édition
2025

Tables Informatique & Libertés

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

Version du 26/02/2025 – V 2.1

(CJUE – 2003-2025 ; CEDH –2017-2025 ; CC – 1978-2025 ; Cass – 1998-2025 ; CE – 1978-2025 ; CNIL – 2021-2025 ; CEPD – 2018-2025)

Avant-propos

Les Tables Informatique et Libertés de la CNIL ont pour objectif de rassembler, sous forme de résumés, l'essentiel de la jurisprudence et des décisions pertinentes de la CNIL en matière de protection des données à caractère personnel. Les résumés des principaux points tranchés par ces décisions sont ordonnés dans un plan de classement.

Ce document répond à un manque, non pas tant s'agissant de la jurisprudence, qui est déjà disponible et classée sous de nombreuses formes, mais pour la diffusion de la pratique décisionnelle de la CNIL. Si les décisions de la formation restreinte sont en partie publiques, ainsi que certaines rares mises en demeure, la CNIL est confrontée chaque jour à un très grand nombre de questions d'application pratique du règlement général sur la protection des données (RGPD) et de la loi Informatique et Libertés. À travers les mesures correctrices qu'elle prend (rappels aux obligations légales, mises en demeure, sanctions de la formation restreinte, etc.) ou les décisions par lesquelles elle rejette les plaintes portées devant elle, elle prend position sur un grand nombre de questions pratiques pour les responsables de traitement. Une partie est bien connue et, en consultant ces tables, les professionnels n'y trouveront que la confirmation de ce qu'ils savent déjà. Ainsi, s'agissant des obligations de sécurité, les grands principes appliqués par la Commission dans des milliers de dossiers chaque année sont déjà clairement exposés dans des recommandations officielles adoptées par le collège des commissaires de la CNIL ou dans des décisions de sa formation restreinte. Pour d'autres questions, à l'inverse, la doctrine reste purement interne, fixée par des décisions prises dans des affaires ponctuelles, sans aucune publicité extérieure.

Il en résulte un double inconvénient : d'une part, le risque que cette doctrine soit insuffisamment connue en interne ; d'autre part, l'absence de communication de celle-ci aux professionnels de la protection des données à caractère personnel que sont les délégués à la protection des données, les avocats, les cabinets de conseil, et tous les juristes ou ingénieurs qui doivent s'assurer du respect de ces règles. Ces prises de position sont également inconnues des universitaires, alors que, dans une matière aussi vaste que la protection des données, la doctrine est essentielle, tant pour les acteurs que pour le régulateur.

À ce double inconvénient répondent les deux objectifs poursuivis par ces tables, qui s'inspirent des documents du même type publiés par d'autres autorités administratives, comme l'Autorité des marchés financiers. Le premier objectif est de contribuer à la bonne appropriation de la doctrine à l'intérieur de la CNIL. Cela est essentiel pour continuer d'assurer le respect de l'égalité de traitement, exigence fondamentale du service public, dans une institution dont les effectifs ont fortement crû ces dernières années. Les tables fournissent, en outre, des rédactions-types, issues de décisions de justice, de décisions de la formation restreinte ou de la présidente, qui peuvent ensuite être reprises dans les autres décisions et assurer une unité de rédaction. C'est l'occasion de souligner la variété et la multitude des dossiers que traitent les quelques 300 agents de la CNIL : près de 20 000 demandes d'information qui reçoivent une réponse écrite, environ 1 500 demandes de consultation juridique complexes de responsables de traitement ou de fédérations professionnelles, un canal spécifique d'information et de conseil pour les délégués à la protection des données personnelles, près d'une centaine d'avis sur des textes réglementaires, près de 500 autorisations de traitements de données de santé, 14 000 plaintes, ainsi que plus de 300 contrôles, qui nourrissent l'ensemble des mesures correctrices instruites et édictées chaque année. Cette présentation ne rend d'ailleurs que partiellement compte de l'activité de la CNIL, mais elle illustre le défi qu'il y a à répondre de façon

assurée et homogène à l'ensemble des questions d'application du RGPD qui sont posées par ces dizaines de milliers de dossiers.

Le second objectif est tourné vers l'extérieur : faire connaître les points de droit sur lesquels la CNIL, avant la jurisprudence ou en la précisant, a dû prendre position. L'administration est en effet dans l'obligation de prendre position sur certaines questions délicates d'application des textes avant que le juge ne les tranche. La CNIL doit éclairer l'application du RGPD et de la loi Informatique et Libertés pour les personnes physiques et les responsables de traitement, ce qu'elle fait par l'adoption de lignes directrices, de recommandations, de référentiels etc. ; elle doit aussi le faire pour décider des plaintes et réclamations dont elle est saisie, ou pour prendre position sur la légalité d'un traitement qu'elle a contrôlé. La publication des premiers est assurée de longue date, au Journal officiel et sur le site internet de la CNIL ; celle des secondes l'était à travers des publications générales, le plus souvent sur le site internet. Malgré la richesse de ce site, souvent saluée par nos interlocuteurs, un certain nombre de positions doctrinales demeuraient non publiées et pourront figurer dans les tables. En outre, les tables permettront de publier le raisonnement et les formules juridiques utilisées dans les décisions, ce qui n'est pas la vocation du site internet. Leur publication participe à une volonté de plus grande transparence et ouverture vers l'extérieur, en réponse à certaines remontées des professionnels du droit des données personnelles ou d'associations de défense des droits individuels.

L'élaboration d'un document de ce type avec les moyens limités de la CNIL est forcément imparfait : il est probable que des décisions importantes de jurisprudence manquent ; que des coquilles ou des erreurs de classement demeurent ; que des éléments structurants et publics de la doctrine de la CNIL ne trouvent aucune expression dans les tables. Nous avons préféré prendre le risque de ces imperfections plutôt que de ne pas publier le document. Nous avons créé une adresse fonctionnelle tablesIL@cnil.fr, où vous pouvez nous écrire pour nous signaler une erreur ou un manque, en vue des prochaines mises à jour.

Je remercie tout spécialement M. Gaëtan Goldberg qui, durant plus d'une année, a progressivement repris l'ensemble du document existant en interne pour le relire, le compléter et le mettre en forme en collaboration avec Mme Léa Divo. Ils ont été aidés par Mme Flora Sanchez.

Enfin, je remercie chaleureusement, au nom de la présidente, toutes les personnes des services de la CNIL qui ont contribué à ce document et à sa publication.

Louis Dutheillet de Lamothe

Secrétaire général de la CNIL

Navigation

Les tables peuvent être utilisées selon différentes modalités de navigation.

La **table des matières** constitue le premier et principal point d'entrée du document et permet d'effectuer une recherche thématique par notion de droit. Le plan de classement est structuré sur la base de neuf grands chapitres :
– Les dispositions générales,
– Les règles principales,
– Les autres règles incombant aux responsables du traitement et aux sous-traitants,
– Les droits des personnes,
– Les transferts,
– Les règles spéciales et les applications du RGPD selon les secteurs d'activité,
– Les actes administratifs encadrant les traitements publics,
– Les règles applicables aux décisions de la CNIL,
– La coopération européenne.

Pour chacun de ces chapitres et de leurs sous-chapitres, il est possible de développer le plan de classement sous la forme de signets en utilisant le menu de navigation, accessible via l'icône en haut à gauche du document.

Par exemple, pour une recherche de décisions relatives aux données biométriques :
1. Dispositions générales > 1.3 Notions générales > 1.3.3 Données sensibles > 1.3.3.7 Données biométriques

Le document étant volumineux, il est possible d'accéder directement à un chapitre, ou à une entrée spécifique, en cliquant sur le titre dans la table des matières ou dans le menu de navigation.

Il est également possible d'**effectuer une recherche dans l'ensemble du document par mot ou expression (Ctrl+F) ou d'extraire l'ensemble des pages d'un titre ou d'un chapitre à cette fin.**

Utilisation et références

Pour simplifier le document, les textes de droit cités à plusieurs reprises ont été abrégés. Par exemple, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est régulièrement désignée comme "loi Informatique et Libertés" ou "loi du 6 janvier 1978".

Les autres abréviations mobilisées sont les suivantes :

- « RGPD » correspond au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;
- « Directive « Police-Justice » » correspond à la Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ;
- « Directive ePrivacy » ou « Directive vie privée et communications électroniques » correspond à la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet

2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ; ,

- « Directive 95/46/CE » correspond à la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
- « Directive 2016/680 » correspond à la Directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil,
- « Directive PNR » correspond à la Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière,
- « Conv. EDH » pour la Convention de sauvegarde des droits de l'homme et libertés fondamentales.

Chaque décision est référencée à la suite du résumé.

Pour les décisions de la CNIL, les abréviations suivantes sont utilisées :

- SP pour Séance plénière,
- FR pour Formation restreinte,
- MED pour mise en demeure du président,
- ROL pour rappel aux obligations légales,
- P pour les autres décisions du président.

Les références aux décisions de la CNIL précisent le statut de publication des documents : « publié » pour toutes les décisions publiées par la CNIL elle-même (sanction publique, mise en demeure publique, référentiel, etc.), et « non publié » pour les décisions n'ayant pas vocation à l'être (mise en demeure non publique, décision de rejet ou clôture d'une plainte, etc.).

Les décisions non publiées ont été pseudonymisées, y compris pour les personnes morales, et la rédaction générale du résumé est généralement de nature à rendre difficile la réidentification. Lorsque celle-ci s'avère trop aisée, la CNIL apprécie si l'intérêt public qui s'attache à la diffusion de sa doctrine l'emporte ou non sur l'intérêt de la personne concernée par la décision.

Table des matières

1. Dispositions générales

1.1 Principes constitutionnels et conventionnels

1.1.1 Sources constitutionnelles

Aucune norme constitutionnelle ne s'oppose par principe à ce qu'un traitement automatisé poursuive plusieurs finalités.

CC, 2019-797 QPC, 26 juillet 2019, Unicef France et autres, point 8

Constitution du 4 octobre 1958

Article 34

L'article 34 de la Constitution dispose que la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ainsi que la procédure pénale.

Il appartient au législateur, dans le cadre de sa compétence, d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect des autres droits et libertés constitutionnellement protégés. Il lui est à tout moment loisible d'adopter des dispositions nouvelles dont il lui appartient d'apprécier l'opportunité et de modifier des textes antérieurs ou d'abroger ceux-ci en leur substituant, le cas échéant, d'autres dispositions, dès lors que, dans l'exercice de ce pouvoir, il ne prive pas de garanties légales des exigences constitutionnelles.

La liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

CC, 2012-652 DC, 22 mars 2012, Loi relative à la protection de l'identité, points 7, 8

Dispositions autorisant la communication des informations relatives à la circulation et à l'état des véhicules aux fonctionnaires des douanes – Caractère législatif - Existence

L'article 64 B du code des douanes autorise la communication de l'ensemble des informations relatives à la circulation et à l'état des véhicules aux fonctionnaires des douanes, sur leur demande. D'une part, eu égard à la nature des données auxquelles ces agents peuvent ainsi accéder et à l'ampleur des traitements dont elles peuvent faire l'objet, ces dispositions mettent en cause les règles relatives aux « garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques », placées par l'article 34 de la Constitution dans le domaine de la loi. D'autre part, en instituant un droit de communication en vue de faciliter la recherche et la constatation d'infractions, ces dispositions figurent au nombre des règles concernant « la procédure pénale ». Par suite, elles ont un caractère législatif.

CC, 2024-308 L, 4 juillet 2024, 04 juillet 2024, points 25, 26

Déclaration des droits de l'homme et du citoyen

Article 2

Hadopi – 1) Droit d'obtenir communication des données de connexion – Trafic et localisation – Objectif de sauvegarde de la propriété intellectuelle – Inclusion – 2) Garanties propres à assurer une conciliation qui ne soit pas manifestement déséquilibrée entre le droit au respect de la vie privée et l'objectif visé – Absence

Dispositions conférant aux agents de la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi) le droit d'obtenir communication et copie des données de connexion détenues par les opérateurs de communication électronique.

En adoptant ces dispositions, le législateur a entendu renforcer la lutte contre les pratiques de contrefaçon sur internet, qui répond à l'objectif de sauvegarde de la propriété intellectuelle. En outre, ce droit de communication, qui n'est pas assorti d'un pouvoir d'exécution forcée, n'est ouvert qu'aux agents publics de la Haute autorité, dûment habilités et assermentés, qui sont soumis, dans l'utilisation de ces données, au secret professionnel. Enfin, le troisième alinéa de l'article L. 331-21 du code de la propriété intellectuelle subordonne son exercice aux nécessités de la procédure mise en œuvre par la commission de protection des droits.

Toutefois, ce droit de communication peut s'exercer sur toutes les données de connexion détenues par les opérateurs de communication électronique. Or, compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, de telles données fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée. Elles ne présentent pas non plus nécessairement de lien direct avec le manquement à l'obligation de respect du droit d'auteur et des droits voisins énoncée à l'article L. 336-3 du code de la propriété intellectuelle.

Il résulte de ce qui précède que, dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation qui ne soit pas manifestement déséquilibrée entre le droit au respect de la vie privée et l'objectif de sauvegarde de la propriété intellectuelle.

CC, 2020-841 QPC, 20 mai 2020, La Quadrature du Net et autres, points 9, 10, 14-18

Accès, enregistrement, conservation et transmission de données informatiques – Enquête

En autorisant, pour les nécessités d'une enquête ou d'une information relative à une infraction relevant de la criminalité ou de la délinquance organisée, le recours à des dispositifs techniques permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre telles qu'elles sont reçues et émises par des périphériques, y compris non audiovisuels, le législateur n'a pas méconnu le droit au respect de la vie privée.

CC, 2019-778 DC, 21 mars 2019, Loi de programmation 2018-2022 et de réforme pour la justice, point 167

Transmission des informations nominatives à caractère médical

La liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. Ce droit requiert que soit observée une particulière vigilance dans la transmission des informations nominatives à caractère médical entre les médecins prescripteurs, les professionnels de

santé et les organismes de sécurité sociale. Il appartient toutefois au législateur de concilier, d'une part, le droit au respect de la vie privée et, d'autre part, les exigences de valeur constitutionnelle qui s'attachent tant à la protection de la santé qu'à l'équilibre financier de la sécurité sociale.

CC, 2017-756 DC, 21 décembre 2017, Loi de financement de la sécurité sociale pour 2018, point 63

Accès en temps réel aux données de trafic et de localisation – Conciliation entre la prévention des atteintes à l'ordre public et des infractions et le droit au respect de la vie privée – Existence

Les dispositions contestées permettent à l'autorité administrative, pour la prévention du terrorisme, d'obtenir le recueil en temps réel des données de connexion relatives, d'une part, à une personne préalablement identifiée susceptible d'être en lien avec une menace et, d'autre part, aux personnes appartenant à l'entourage de la personne concernée par l'autorisation lorsqu'il y a des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation. Cette technique de recueil de renseignement est autorisée pour une durée de quatre mois renouvelable, conformément à l'article L. 821-4 du code de la sécurité intérieure.

D'une part, le recueil des données de connexion en temps réel ne peut être mis en œuvre que pour les besoins de la prévention du terrorisme. Ne peuvent, par ailleurs, être recueillis que les informations ou documents traités ou conservés par les opérateurs de télécommunication, les fournisseurs d'accès à un service de communication au public en ligne ou les hébergeurs de contenu sur un tel service.

D'autre part, cette technique de recueil de renseignement s'exerce dans les conditions prévues au chapitre Ier du titre II du livre VIII du code de la sécurité intérieure. En vertu de l'article L. 821-4 de ce code, elle est autorisée par le Premier ministre ou les collaborateurs directs auxquels il a délégué cette compétence, sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, après avis préalable de la Commission nationale de contrôle des techniques de renseignement. Elle est autorisée pour une durée de quatre mois renouvelable. En vertu du paragraphe II de l'article L. 851-2, la procédure d'urgence absolue prévue à l'article L. 821-5 de ce code n'est pas applicable. En application de l'article L. 871-6 du même code, les opérations matérielles nécessaires à la mise en place de la technique mentionnée à l'article L. 851-2 ne peuvent être exécutées, dans leurs réseaux respectifs, que par des agents qualifiés des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications.

Enfin, cette technique de renseignement est réalisée sous le contrôle de la Commission nationale de contrôle des techniques de renseignement. La composition et l'organisation de cette autorité administrative indépendante sont définies aux articles L. 831-1 à L. 832-5 du code de la sécurité intérieure dans des conditions qui assurent son indépendance. Ses missions sont définies aux articles L. 833-1 à L. 833-11 du même code dans des conditions qui assurent l'effectivité de son contrôle. Conformément aux dispositions de l'article L. 841-1 du même code, le Conseil d'État peut être saisi par toute personne souhaitant vérifier qu'aucune technique de recueil de renseignement n'est irrégulièrement mise en œuvre à son égard ou par la Commission nationale de contrôle des techniques de renseignement.

Il résulte de ce qui précède que le législateur a assorti la procédure de réquisition des données de connexion, lorsqu'elle s'applique à une personne préalablement identifiée susceptible d'être en lien avec une menace, de garanties propres à assurer une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public et celle des infractions et, d'autre part, le droit au respect de la vie privée.

CC, 2017-648 QPC, 4 août 2017, La Quadrature du Net et autres, points 5-10

Etat d'urgence (loi du 3 avril 1955) – Conciliation entre la sauvegarde des atteintes à l'ordre public et le respect des droits et libertés

La Constitution n'exclut pas la possibilité pour le législateur de prévoir un régime d'état d'urgence. Il lui appartient, dans ce cadre, d'assurer la conciliation entre, d'une part, la sauvegarde des atteintes à l'ordre public et, d'autre part, le respect des droits et libertés reconnus à tous ceux qui résident sur le territoire de la République. Parmi ces droits et libertés figure le droit au respect de la vie privée, en particulier de l'inviolabilité du domicile, protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

CC, 2016-600 QPC, 2 décembre 2016, M. Raïme A., point 6

Secret des correspondances – Réquisition administrative

Des dispositions instituant une procédure de réquisition administrative de données de connexion excluant l'accès au contenu des correspondances ne sauraient méconnaître le droit au secret des correspondances.

CC, 2015-478 QPC, 24 juillet 2015, Association French Data Network et autres, point 17

Registre national des crédits aux particuliers

Par la création d'un traitement de données à caractère personnel recensant les crédits à la consommation accordés aux personnes physiques n'agissant pas pour des besoins professionnels, le législateur a poursuivi un motif d'intérêt général de prévention du surendettement.

Toutefois, ce registre est destiné à comprendre des données à caractère personnel d'un très grand nombre de personnes (plus de 12 millions), la durée de conservation est de plusieurs années (toute la durée du crédit ou du plan de surendettement), les motifs de consultation sont très nombreux (octroi d'un crédit à la consommation ou d'un prêt sur gage corporel, reconduction d'un contrat de crédit renouvelable, vérification triennale de solvabilité de l'emprunteur, vérification relative aux personnes se portant caution d'un prêt à la consommation…) et plusieurs dizaines de milliers d'agents des établissements de crédit seront habilités à consulter le registre.

Compte tenu de la nature des données enregistrées, de l'ampleur du traitement de données, de la fréquence de son utilisation, du grand nombre de personnes susceptibles d'y avoir accès et de l'insuffisance des garanties relatives à l'accès au registre, la création du registre national des crédits aux particuliers porte une atteinte au droit au respect de la vie privée qui ne peut être regardée comme proportionnée au but poursuivi.

CC, 2014-690 DC, 13 mars 2014, Loi relative à la consommation, points 51-57

Justification de la collecte, l'enregistrement, la conservation, la consultation et la communication de données par un motif d'intérêt général – Mise en œuvre adéquate et proportionnée à cet objectif

La liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

CC, 2013-681 DC, 5 décembre 2013, Loi organique portant application de l'article 11 de la Constitution, point 27

Utilisation de données nominatives recueillies dans le cadre d'activités de police judiciaire à des fins administratives

Aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire. Toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées.

CC, 2003-467 DC, 13 mars 2003, Loi pour la sécurité intérieure, point 32

1.1.2 Sources de droit de l'Union européenne

Principe de non-discrimination

Traité instituant la communauté européenne – Traitement de données spécifique aux citoyens de l'Union non-ressortissants d'un État membre dans l'objectif de lutte contre la criminalité – Principe de non-discrimination – Illicéité

L'article 12, paragraphe 1, du Traité instituant la communauté européenne (TCE) s'oppose à l'instauration par un État membre d'un système de traitement de données à caractère personnel spécifique aux citoyens de l'Union non-ressortissants de cet État membre dans l'objectif de lutter contre la criminalité. Un tel traitement méconnaît le principe de non-discrimination.

CJUE, grande chambre, 16 décembre 2008, Huber, C-524/06

Principe non bis in idem

Charte des droits fondamentaux de l'Union européenne – Application du principe non bis in idem en droit de l'Union – Droit de la concurrence – Amende pour infraction au droit de la concurrence dans un État membre et poursuite par une autorité dans un autre État membre pour un même comportement

L'article 50 de la Charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'une entreprise soit poursuivie, par l'autorité de concurrence d'un État membre, et se voit, le cas échéant, infliger une amende pour une infraction à l'article 101 TFUE et aux dispositions correspondantes du droit national de la concurrence, en raison d'un comportement qui a eu un objet ou un effet anticoncurrentiel sur le territoire de cet État membre. Ceci alors que ce comportement a déjà été mentionné, par une autorité de concurrence d'un autre État membre, dans une décision définitive que celle-ci a adoptée, à l'égard de cette entreprise, au terme d'une procédure d'infraction à l'article 101 TFUE et aux dispositions correspondantes du droit de la concurrence de cet autre État membre, pour autant que cette décision ne repose pas sur le constat d'un objet ou d'un effet anticoncurrentiel sur le territoire du premier État membre.

CJUE, grande chambre, 22 mars 2022, Nordzucker e.a, C-151/20

1.1.3 Convention de sauvegarde des droits de l'homme et des libertés fondamentales

1) Législation nationale prévoyant une obligation extrêmement large de conservation de toutes les communications Internet de tous les utilisateurs – Violation de l'article 8 CEDH – 2) Accès direct aux communications sans présentation d'une autorisation d'interception aux fournisseurs de services – Absence de garanties adéquates et suffisantes contre les abus liés à l'accès des autorités répressives aux communications Internet et aux données de communication connexes stockées – 3) Obligation légale de déchiffrer les communications cryptées de bout en bout – Disproportion

1) La législation contestée exige la conservation et le stockage automatiques et continus du contenu de toutes les communications Internet (communications vocales, textuelles, visuelles, sonores, vidéo ou d'autres communications électroniques) pendant une durée de six mois et des données de connexion correspondantes pendant une durée d'un an. Elle concerne tous les utilisateurs, même en

l'absence de soupçon raisonnable de participation à des activités criminelles ou à des activités mettant en danger la sécurité nationale, ou de toute autre raison de penser que la conservation des données peut contribuer à la lutte contre les formes graves de criminalité ou à la protection de la sécurité nationale. Il n'y a aucune limitation du champ d'application de la mesure en termes d'application territoriale ou temporelle ou de catégories de personnes susceptibles de voir leurs données à caractère personnel conservées. La Cour conclut que l'ingérence est exceptionnellement étendue et grave. La législation ne peut être considérée comme nécessaire dans une société démocratique et porte atteinte à l'essence même du droit au respect de la vie privée garanti par l'article 8 de la Convention. L'État défendeur a donc outrepassé toute marge d'appréciation acceptable à cet égard.

2) Contrairement à la législation en cause qui prévoit un accès direct aux communications Internet par les services de sécurité sans autorisation judiciaire préalable, la Cour recommande une obligation de présenter une autorisation au fournisseur de services de communication avant d'obtenir l'accès aux communications d'une personne en ce qu'elle constitue une garantie importante contre les abus des autorités répressives, en veillant à ce qu'une autorisation en bonne et due forme soit obtenue dans tous les cas de surveillance secrète.

3) L'obligation légale de déchiffrer les communications chiffrées de bout en bout risque d'équivaloir à une obligation pour les fournisseurs de tels services d'affaiblir le mécanisme de chiffrement pour tous les utilisateurs et n'est donc pas proportionnée aux buts légitimes poursuivis.

CEDH, 13 février 2024, Podchasov c. Russie, n°33696/19, points 70, 73 et 79

Conservation de photographies par la police – Application de techniques de reconnaissance faciale – Ingérence dans l'exercice du droit au respect de la vie privée

Dans une jurisprudence constante, la Cour EDH juge que la conservation de photographies par la police, combinée à la possibilité de leur appliquer des techniques de reconnaissance faciale, constitue une ingérence dans l'exercice du droit à la vie privée. La Cour rappelle également qu'il est essentiel, dans le cadre de la mise en œuvre de la technologie de reconnaissance faciale, de disposer de règles détaillées régissant la portée et l'application des mesures ainsi que de garanties solides contre le risque d'abus et d'arbitraire. La nécessité de disposer de garanties est d'autant plus grande lorsque la technologie de reconnaissance faciale est utilisée en temps réel.

De telles mesures, particulièrement intrusives, requièrent un niveau élevé de justification pour qu'elles puissent être considérées comme « nécessaires dans une société démocratique », le niveau de justification le plus élevé étant requis pour l'utilisation de cette technologie.

CEDH,4 octobre 2023, Glukhin c.Russie, n°11519/20

Droit au respect de la vie privée – Article 8 CEDH – Consécration d'un droit à l'auto-détermination informationnelle

Il ressort de la jurisprudence établie que les considérations liées à la vie privée entrent en jeu dans les situations où des informations ont été recueillies sur une personne bien précise, où des données à caractère personnel ont été traitées ou utilisées et où les éléments en question avaient été rendus publics d'une manière ou dans une mesure excédant ce à quoi les intéressés pouvaient raisonnablement s'attendre (Uzun c. Allemagne, n° 35623/05 §§ 44–46, CEDH 2010 ; voir également Rotaru c. Roumanie, précité, §§ 43–44, P.G. et J.H. c. Royaume-Uni, précité, § 57, Amann, précité, §§ 65–67, et M.N. et autres c. Saint-Marin, n° 28005/12 §§ 52-53, 7 juillet 2015).

La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (S. et Marper, précité, §

103). L'article 8 de la Convention consacre donc le droit à une forme d'auto-détermination informationnelle, qui autorise les personnes à invoquer leur droit à la vie privée en ce qui concerne des données qui, bien que neutres, sont collectées, traitées et diffusées à la collectivité, selon des formes ou modalités telles que leurs droits au titre de l'article 8 peuvent être mis en jeu.

CEDH, grande chambre, 27 juin 2017, Satakunnan Markkinapörssi OY et Satamedia OY c/ Finlande, n°931/13, points 136-137

Mémorisation de données relatives à la privée – Ingérence dans le droit au respect de la vie privée – Prise en compte du contexte particulier pour les autorités

Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 de la Convention européenne des droits de l'homme qui garantit le droit au respect de la vie privée et familiale, du domicile et de la correspondance [...]. Peu importe que les informations mémorisées soient ou non utilisées par la suite [...]. Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu un aspect de la vie privée [...], la Cour européenne des droits de l'homme tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés.

CEDH, grande chambre, 4 décembre 2008, S. et Marper c. Royaume-Uni, n°30562/04, 305666/04, point 67

1.1.4 Convention pour la protection des données à caractère personnel (n° 108)

Application article 5 – Données pertinentes au regard de la finalité du traitement – Conditions

Considérant qu'aux termes de l'article 5 de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel signée à Strasbourg le 28 janvier 1981, ratifiée en vertu de la loi du 19 octobre 1982 et publiée au Journal officiel en vertu du décret du 15 novembre 1985 : « les données à caractère personnel faisant l'objet d'un traitement automatisé sont : « adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ».

Considérant que, pour l'application de ces stipulations, les données pertinentes au regard de la finalité d'un traitement automatisé d'informations nominatives sont celles qui sont en adéquation avec la finalité du traitement et qui sont proportionnées à cette finalité.

CE, Section, 30 octobre 2001, Association française des sociétés financières et autres, n°204909, Rec., points 3-4

Articles 6 et 9 – Traitement de données nominatives – Données sensibles – Conditions d'autorisation

Considérant, en deuxième lieu, que les articles 6 et 9 de la convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel signée à Strasbourg le 28 janvier 1981, ratifiée en vertu de la loi du 19 octobre 1982 et publiée au Journal Officiel en vertu du décret du 15 novembre 1985, n'autorisent le traitement des données nominatives qui font apparaître les origines raciales ou les opinions politiques, les convictions religieuses ou autres convictions, les données à caractère personnel relatives à la santé ou à la vie sexuelle que si ce traitement dérogatoire prévu « par la loi de la partie, constitue une mesure nécessaire, dans une société démocratique : a) à la protection de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales... ».

CE, 10ème/7ème SSR, 18 novembre 1992, Ligue internationale contre le racisme et l'antisémitisme, n°115367, Rec., point 7

1.2 Droit applicable

Traitements non automatisés de données à caractère personnel soumis à la loi du 6 janvier 1978 – 1) Notion – 2) Collecte, conservation et consultation des empreintes digitales relevées lors d'une demande de carte nationale d'identité – Inclusion

1) Il résulte des dispositions de l'article 2 de la loi n° 78-17 du 6 janvier 1978, dans sa rédaction issue de la loi n° 2004-801 du 6 août 2004, que cette loi s'applique y compris aux traitements non automatisés de données à caractère personnel, entendus comme toute opération ou ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

2) Par suite, la collecte, la conservation et la consultation des empreintes digitales effectuées sur le fondement de l'article 5 du décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité, sous la responsabilité du ministre de l'intérieur, entrent dans le champ d'application de la loi du 6 janvier 1978, nonobstant la circonstance que ces fichiers ne sont pas numérisés et qu'ils ne sont constitués et conservés qu'au seul niveau des préfectures, pour l'arrondissement du chef-lieu d'un département, ou des sous-préfectures, et des consulats.

CE, 10ème/9ème SSR, 18 novembre 2015, Mme X et Mme Y, n° 372111, T., point 3

1.2.1 RGPD (titre II Loi Informatique et Libertés)

Champ d'application matériel

Activités relevant du champ d'application du droit de l'Union

Activités d'une commission d'enquête mise en place par le parlement d'un État membre dans l'exercice de son pouvoir de contrôle du pouvoir exécutif, ayant pour objet d'enquêter sur les activités d'une autorité policière de protection de l'État en raison d'un soupçon d'influence politique sur cette autorité – Inclusion

L'article 16, paragraphe 2, première phrase, TFUE et l'article 2 paragraphe 2 sous a) du RGPD doivent être interprétés en ce qu'une activité ne saurait être considérée comme située en dehors du champ d'application du droit de l'Union et comme échappant dès lors à l'application de ce règlement pour la seule raison qu'elle est exercée par une commission d'enquête mise en place par le parlement d'un État membre dans l'exercice de son pouvoir de contrôle du pouvoir exécutif.

L'article 2 paragraphe 2 sous a) du RGPD, lu à la lumière du considérant 16 de ce règlement, doit être interprété en ce que ne sauraient être considérées, en tant que telles, comme des activités relatives à la sécurité nationale situées en dehors du champ d'application du droit de l'Union, au sens de cette disposition, les activités d'une commission d'enquête mise en place par le parlement d'un État membre dans l'exercice de son pouvoir de contrôle du pouvoir exécutif, ayant pour objet d'enquêter sur les activités d'une autorité policière de protection de l'État en raison d'un soupçon d'influence politique sur cette autorité.

CJUE, 16 janvier 2024, Österreichische Datenschutzbehörde, C-33/22

Traitement de données à caractère personnel dans le contexte de l'organisation d'élections dans un État membre – Application du RGPD

Les activités ayant pour but de préserver la sécurité nationale au sens de l'article 2, paragraphe 2, sous a), du RGPD couvrent, en particulier, celles ayant pour objet de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société.

Or, les activités relatives à l'organisation d'élections dans un État membre ne poursuivent pas un tel objectif et ne sauraient, en conséquence, être rangées dans la catégorie des activités ayant pour but la préservation de la sécurité nationale, visées à l'article 2, paragraphe 2, sous a), du RGPD. Eu égard à ces considérations, l'article 2, paragraphe 2, sous a), du RGPD doit être interprété en ce sens que n'est pas exclu du champ d'application de ce règlement le traitement de données à caractère personnel dans le contexte de l'organisation d'élections dans un État membre.

CJUE, 20 octobre 2022, Koalitsia « Demokratichna Bulgaria – Obedinenie », C-306/21, points 40-42

Voir aussi : CJUE, grande chambre, 22 juin 2021, Latvijas Republikas Saeima, C-439/19, points 66 -67

Traitement de données à caractère personnel à des fins fiscales – Demande de communication d'informations à des fins de lutte contre la fraude fiscale – Application du RGPD, en l'absence d'objectif spécifique d'exercer des poursuites pénales

L'accès aux numéros de châssis des véhicules faisant l'objet d'une annonce publiée sur le portail Internet d'un opérateur économique par l'administration fiscale d'un État membre en vue de se voir fournir des informations sur les annonces publiées sur ce portail aux fins de la perception de l'impôt et de la lutte contre la fraude fiscale relève du champ d'application du RGPD dans la mesure où, dans ces circonstances, l'administration n'agit pas en tant qu'« autorité compétente », au sens de l'article 3, point 7, de la directive 2016/680 dite « Police-Justice » et que ces données à caractère personnel ne sont pas collectées dans l'objectif spécifique d'exercer des poursuites pénales ou dans le cadre des activités de l'État relatives à des domaines du droit pénal.

CJUE,24 février 2022, Valsts ieņēmumu dienests, C-175/20, points 42-47

Transferts de données à caractère personnel effectués à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur établi dans un pays tiers – Inclusion – Données susceptibles d'être traitées par les autorités du pays tiers concerné à des fins de sécurité nationale – Absence d'incidence

L'article 2, paragraphes 1 et 2, du RGPD doit être interprété en ce sens que relève du champ d'application de ce règlement un transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, nonobstant le fait que, au cours ou à la suite de ce transfert, ces données sont susceptibles d'être traitées par les autorités du pays tiers concerné à des fins de sécurité publique, de défense et de sûreté de l'État.

CJUE, grande chambre, 16 juillet 2020, Facebook Ireland et Schrems, C-311/18

Notion de « responsable du traitement » – Commission des pétitions du parlement d'un État fédéré d'un État membre – Inclusion – Article 15 – Droit d'accès de la personne concernée – Application

Aucune exception n'est prévue dans le RGPD en ce qui concerne les activités parlementaires. Par conséquent, dans la mesure où la Commission des pétitions du Parlement du Land de Hesse détermine, seule ou avec d'autres, les finalités et les moyens du traitement, cette commission doit être qualifiée de « responsable du traitement », au sens de l'article 4, point 7, du règlement. Le traitement de données à caractère personnel effectué par une telle commission relève du champ d'application de ce règlement, notamment de l'article 15 de celui-ci (droit d'accès).

CJUE, 9 juillet 2020, Land Hessen, C-272/19, points 72-74

Collecte de données à caractère personnel par les membres d'une communauté religieuse dans le cadre de leur activité de prédication de porte-à-porte – Notion de « fichier de données à caractère personnel » – Notion de « responsable du traitement » – Article 10, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne

La collecte de données à caractère personnel effectuée par des membres d'une communauté religieuse dans le cadre d'une activité de prédication de porte-à-porte et les traitements ultérieurs de ces données relèvent de la directive 95/46/CE. En particulier, il ne s'agit ni de traitements de données à caractère personnel mis en œuvre pour l'exercice d'activités visées à l'article 3, paragraphe 2, premier tiret (traitements ne relevant pas du champ du droit de l'UE ou ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives au droit pénal), de la directive, ni de traitements de données à caractère personnel effectués par des personnes physiques pour l'exercice d'activités exclusivement personnelles ou domestiques, au sens de l'article 3, paragraphe 2, second tiret (traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques), de ladite directive. La communauté religieuse doit être regardée comme étant responsable, conjointement avec ses membres prédicateurs, de ces traitements.

CJUE, grande chambre, 10 juillet 2018, Jehovan Todistajat, C-25/17

Administration fiscale – Traitement aux fins d'obtenir le droit de procéder à une mesure d'enquête – Fraude fiscale – Champ d'application matériel du RGPD

Le traitement de données à caractère personnel mis en œuvre par l'administration fiscale aux fins d'obtenir l'autorisation de procéder à des opérations de visite et saisies sur le fondement de l'article L. 16 B du livre des procédures fiscales, qui a pour finalité d'obtenir le droit de procéder à une mesure d'enquête pouvant donner lieu à la constatation d'une infraction ou d'un manquement à la législation fiscale, dans le but de percevoir l'impôt et de lutter contre la fraude fiscale, entre dans le champ d'application matériel du RGPD.

Cass, com., 1er juin 2023, n°21-18.558, B., point 10

Application de gestion des dossiers des ressortissants étrangers en France – Adoption d'un téléservice visant à recenser les données relatives au droit au séjour de l'étranger titulaire d'un visa de long séjour valant titre de séjour –RGPD

Un projet de décret relatif à la validation du visa de long séjour valant titre de séjour complète notamment les objectifs du traitement de données à caractère personnel dénommé « Application de gestion des dossiers des ressortissants étrangers en France » (AGDREF 2), pour y ajouter la possibilité, pour le titulaire d'un visa de long séjour valant titre de séjour, de procéder, par voie électronique au moyen d'un téléservice adossé au traitement de données AGDREF 2, aux formalités prévues à l'article R. 311-3 du code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA) qui prévoyaient que certains titulaires de visa puissent déclarer la date de leur entrée en France et leur domicile au moyen d'un téléservice afin de séjourner au-delà d'une période de trois mois (dispositions abrogées en 2021).

Le Conseil d'État (section de l'intérieur) estime que cette nouvelle fonctionnalité du traitement de données, dont l'objet est de recenser les données relatives au droit au séjour de l'étranger titulaire d'un visa de long séjour valant titre de séjour, n'a pas pour finalité première la prévention et la détection d'infractions pénales, la conduite d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et ne relève pas de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 mais du règlement 2016/679 du Parlement européen et du Conseil (règlement général sur la protection des données).

CE, Section de l'intérieur, 27 novembre 2018, Avis n°396212, Projet de décret relatif à la validation du visa long séjour valant titre de séjour

---

Traitements mis en œuvre par le CESE dans le cadre des saisines par voie de pétition

Si certains traitements mettant en œuvre des dispositions constitutionnelles françaises et n'intéressant ni la défense nationale, ni la sûreté de l'État relèvent du seul titre Ier de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés(v. CNIL, SP, 14 janvier 2021, Avis sur projet de décret, Répertoire électoral unique, n° 2021-008, publié), le RGPD est applicable aux traitements mis en œuvre par le Conseil économique, social et environnemental dans le cadre des saisines par voie de pétition. En effet, la Cour de justice de l'Union européenne a estimé que le RGPD était applicable aux traitements de données à caractère personnel effectués par la Commission des pétitions du parlement d'un État fédéré d'un État membre dans le cadre de ses activités.

CNIL, P, 17 février 2022, Avis sur projet de décret, CESE, n°2022-023, publié, point 6

Voir aussi : CJUE, 9 juillet 2020, Land Hessen, C-272/19

Activités ne relevant pas du champ d'application du droit de l'Union

Activités ne relevant pas du droit de l'Union – 1) Portée – Activités qui vise à préserver la sécurité nationale ou activité pouvant être rangée dans la même catégorie – Exclusion du champ d'application du RGPD – 2) Application – Cas de traitement de données à caractère personnel dans le contexte de l'organisation d'élections dans un État membre – Application du RGPD

L'article 2, paragraphe 2, sous a) du RGPD, lu à la lumière du considérant 16 de ce règlement, a pour seul objet d'exclure du champ d'application dudit règlement les traitements de données à caractère personnel effectués par les autorités étatiques dans le cadre d'une activité qui vise à préserver la sécurité nationale ou d'une activité pouvant être rangée dans la même catégorie, de telle sorte que le seul fait qu'une activité soit propre à l'État ou à une autorité publique ne suffit pas pour que cette exception soit automatiquement applicable à une telle activité.

Les activités ayant pour but de préserver la sécurité nationale au sens de l'article 2, paragraphe 2, sous a), du RGPD couvrent, en particulier, celles ayant pour objet de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société.

Or, les activités relatives à l'organisation d'élections dans un État membre ne poursuivent pas un tel objectif et ne sauraient, en conséquence, être rangées dans la catégorie des activités ayant pour but la préservation de la sécurité nationale, visées à l'article 2, paragraphe 2, sous a), du RGPD. Eu égard à ces considérations, l'article 2, paragraphe 2, sous a), du RGPD doit être interprété en ce sens que n'est pas exclu du champ d'application de ce règlement le traitement de données à caractère personnel dans le contexte de l'organisation d'élections dans un État membre.

CJUE, 20 octobre 2022, Koalitsia « Demokratichna Bulgaria – Obedinenie », C-306/21, points 39-42

Activités visant à préserver la sécurité nationale ou relevant de cette catégorie – Notion – Activité visant à améliorer la sécurité routière – Exclusion

L'exception relative à la non-application du RGPD à un traitement effectué dans le cadre d'une activité ne relevant pas du droit de l'Union est à considérer comme ayant pour seul objet d'exclure du champ d'application de ce règlement les traitements de données à caractère personnel effectués par les autorités étatiques dans le cadre d'une activité visant à préserver la sécurité nationale ou d'une activité pouvant être rangée dans la même catégorie. Ces activités couvrent, en particulier, celles visant à protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société.

Les activités relatives à la sécurité routière ne poursuivent pas cet objectif et ne sauraient donc être rangées dans la catégorie des activités ayant pour but la préservation de la sécurité nationale.

CJUE, grande chambre, 22 juin 2021, Latvijas Republikas Saeima, C-439/19, points 64-68

Directive 95/46 – Dérogations – Traitement de données ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal – Interprétation stricte

En tant qu'elle rend inapplicable le régime de protection des données à caractère personnel prévu par la directive 95/46 et s'écarte ainsi de l'objectif sous-jacent à celle-ci, consistant à assurer la protection des libertés et des droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel, l'exception prévue à l'article 3, paragraphe 2, premier tiret (traitements mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire et, en tout état de cause, traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État - y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État - et les activités de l'État relatives à des domaines du droit pénal), de cette directive doit faire l'objet d'une interprétation stricte.

À cet égard, il convient de rappeler que les activités mentionnées à titre d'exemples par ladite disposition sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers.

Par ailleurs, les activités mentionnées en tant qu'exemples à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 sont destinées à définir la portée de l'exception qui y est prévue, de telle sorte que cette exception ne s'applique qu'aux activités qui y sont ainsi expressément mentionnées ou qui peuvent être rangées dans la même catégorie.

CJUE, 27 septembre 2017, Puškár, C-73/16, points 36-38

Voir aussi : CJUE, 6 novembre 2003, Lindqvist, C-101/01, points 43-44 ; CJUE, grande chambre, 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, point 41

Activités ne relevant pas du champ de la protection des données personnelles

Protection des données des personnes morales

Réglementation nationale renvoyant aux dispositions du droit de l'Union – Droit national différant substantiellement de la finalité et du contexte du droit de l'Union – Données fiscales concernant une personne morale – Incompétence de la Cour

Cas d'une législation nationale renvoyant au RGPD pour ce qui est de la protection des données des personnes morales. La Cour estime qu'une interprétation de dispositions du RGPD ne saurait être effectuée de la même manière selon qu'il s'agit de personnes physiques, seules entrant dans le champ du RGPD, ou de personnes morales, le droit à la protection des données de ces dernières n'ayant pas été défini par le RGPD.

Le droit national ne se borne donc pas à rendre applicables les dispositions du RGPD en dehors du champ d'application de ce règlement, mais en modifie l'objet et la portée. Par suite, ces dispositions ne peuvent être regardées comme ayant été rendues applicables en dehors du champ du droit de l'Union et la Cour est incompétente.

CJUE, 10 décembre 2021, J & S Service, C-620/19, points 47-52

Collecte de données à caractère personnel effectuée par des membres d'une communauté religieuse dans le cadre d'une activité de prédication de porte-à-porte et traitements ultérieurs de ces données – Traitements de données à caractère personnel effectués par des personnes physiques pour l'exercice d'activités exclusivement personnelles ou domestiques – Exclusion

La collecte de données à caractère personnel effectuée par des membres d'une communauté religieuse dans le cadre d'une activité de prédication de porte-à-porte et les traitements ultérieurs de ces données relèvent de la directive 95/46/CE. En particulier, il ne s'agit ni de traitements de données à caractère personnel mis en œuvre pour l'exercice d'activités visées à l'article 3, paragraphe 2, premier tiret (traitements ne relevant pas du champ du droit de l'UE ou ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives au droit pénal), de la directive, ni de traitements de données à caractère personnel effectués par des personnes physiques pour l'exercice d'activités exclusivement personnelles ou domestiques, au sens de l'article 3, paragraphe 2, second tiret (traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques), de ladite directive. La communauté religieuse doit être regardée comme étant responsable, conjointement avec ses membres prédicateurs, de ces traitements.

CJUE, grande chambre, 10 juillet 2018, Jehovan Todistajat, C-25/17

Caméra de surveillance à l'intérieur d'une maison familiale – Surveillance partielle de l'espace public – Exception domestique – Absence

L'exploitation d'un système de caméra, donnant lieu à un enregistrement vidéo des personnes stocké dans un disque dur, installé par une personne physique dans sa maison familiale afin de protéger les biens, la santé et la vie des propriétaires de la maison ne constitue pas un traitement de données effectué pour l'exercice d'activités exclusivement personnelles ou domestiques, dès lors que ce système surveille également, même partiellement, l'espace public.

CJUE, 11 décembre 2014, Ryneš, C-212/13

Solution logicielle d'un tiers disponible sur internet ou une application sur un terminal mobile – Traitement effectué à la demande de l'utilisateur, sous son contrôle et sans intervention possible du tiers sur ces données – Exception domestique – Inclusion

Lorsqu'une personne physique recourt, pour traiter des données à caractère personnel à des fins propres et non professionnelles, relevant de la sphère domestique au sens du c du 2 de l'article 2 du RGPD, à la solution logicielle d'un tiers à laquelle cette personne accède sur internet ou une application sur un terminal mobile, un tel traitement relève en principe de l'exemption domestique s'il est initié à la discrétion de cette personne, opéré sous son contrôle et pour son seul compte, et réalisé dans un environnement cloisonné, c'est à dire sans intervention possible du tiers sur ces données. Dans les autres cas, le tiers qui traite les données à la demande de la personne assume une forme de responsabilité de traitement pour l'application du RGPD, soit comme responsable de traitement, soit comme sous-traitant.

En l'espèce, le traitement étant effectué localement, sur le poste de l'utilisateur, aucune donnée à caractère personnel des personnes concernées n'est transmise à la société X. Par conséquent, le traitement, effectué à la demande de l'utilisateur et sous son contrôle, doit être considéré comme relevant de l'exemption domestique prévue par l'article 2, paragraphe 2, c), du RGPD, qui ne lui est ainsi pas applicable.

CNIL, P, 28 février 2024, Mise en demeure, société X, n° MED 2024-032, non publié

Champ d'application territorial

Succursale ou filiale de l'exploitant d'un moteur de recherche installée dans un État membre destinée à assurer la promotion et la vente d'espaces publicitaires – Activités visant les habitants de cet État membre – Traitement de données effectué dans ce cadre

L'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre.

CJUE, 13 mai 2014, Google Spain, C-131/12

Collecte systématique et généralisée d'images sur des sites web – Base à des fins d'identification biométrique par reconnaissance faciale – Suivi du comportement des personnes en ligne

Cas d'un responsable du traitement ne disposant d'aucun établissement sur le territoire d'un État membre de l'Union européenne, qui procède à la collecte systématique et généralisée, à partir de millions de sites web à travers le monde, d'images contenant des visages, afin de constituer une base de données et de permettre la recherche des photographies dans cette base à partir d'une autre image, et ainsi procéder à l'identification biométrique des personnes concernées par reconnaissance faciale.

Le résultat de recherche qui est associé à une photographie doit être qualifié, au moins en partie, de profil comportemental de la personne concernée dans la mesure où il contient de nombreuses informations relatives à cette personne et en particulier à son comportement. La mise en relation des photographies et du contexte dans lequel elles sont présentées sur un site web permet en effet de recueillir de nombreuses informations sur une personne, ses habitudes ou ses préférences. La recherche peut par ailleurs être renouvelée dans le temps, ce qui permet de constater une évolution des informations relatives à une personne ; la base de données étant mise à jour régulièrement, des recherches successives permettent de suivre l'évolution d'un profil dans le temps.

Ce traitement doit être considéré comme une activité de traitement liée au suivi du comportement des personnes en ligne et il est donc soumis au RGPD.

Par ailleurs, dans ce contexte, la mise en ligne de photographies peut être considérée en soi comme un comportement de la personne concernée, reflétant des choix sur le niveau d'exposition qu'elle souhaite donner à des éléments de sa vie privée ou professionnelle.

CNIL, P, 26 novembre 2021, Mise en demeure, Société X, n° MED 2021-134, publié, points 27, 24, 30-31, 26

Voir aussi : CNIL, FR, 17 octobre 2022, Sanction, Société X, n°SAN-2022-019, publié

Collecte et traitement de données de personnes physiques en France impliquées dans le débat sur le renouvellement de l'autorisation d'utilisation d'une substance phytopharmaceutique dans l'Union européenne – Traitement de données procédant du suivi de comportement au sens de l'article 3-2)-b) du RGPD

La collecte et le traitement des données à caractère personnel de personnes physiques en France impliquées dans le débat sur le renouvellement de l'autorisation d'utilisation d'une substance phytopharmaceutique dans l'Union européenne procède du suivi du comportement des personnes concernées qui se trouve sur le territoire de l'Union au sens des dispositions de l'article 3-2)-b) du RGPD et relève en conséquence du champ d'application territorial du RGPD et des dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés , indépendamment du lieu d'établissement du responsable de traitement.

CNIL, FR, 26 juillet 2021, Sanction, Société X, n°SAN-2021-012, publié, point 55

1.2.2 Directive « Police-Justice » (titre III loi Informatique et Libertés)

Champ d'application matériel

Perception de l'impôt et lutte contre la fraude fiscale – Collecte de données personnelles par l'administration fiscale d'un opérateur économique – Champ d'application de la directive « Police-Justice » – Absence

Lorsqu'elle demande à un opérateur économique de lui communiquer des données à caractère personnel relatives à certains contribuables aux fins de la perception de l'impôt et de la lutte contre la fraude fiscale, il n'apparaît pas que l'administration fiscale d'un État membre puisse être considérée comme une « autorité compétente », au sens de l'article 3, point 7, de la directive 2016/680, ni, partant, que de telles demandes d'informations puissent relever de l'exception prévue à l'article 2, paragraphe 2, sous d), du RGPD. En outre, même s'il n'est pas exclu que les données à caractère personnel en cause au principal puissent être utilisées dans le cadre de poursuites pénales qui pourraient être exercées, en cas d'infraction dans le domaine fiscal, contre certaines des personnes concernées, il n'apparaît pas que ces données soient collectées dans l'objectif spécifique d'exercer de telles poursuites pénales ou dans le cadre des activités de l'État relatives à des domaines du droit pénal.

CJUE, 24 février 2022, Valsts ieņēmumu dienests, C-175/20, points 44-45

1.2.3 Sûreté de l'État et défense (titre IV loi Informatique et Libertés)

1) Traitement mettant en relation les traitements HOPSYWEB et FSPRT – Finalité – Prévention de la radicalisation à caractère terroriste – 2) Conséquences – a) Application des dispositions relatives aux traitements intéressant la sûreté de l'État et la défense – Existence – b) Application du RGPD – Absence

1) Le traitement créé par le décret n° 2019-412 du 6 mai 2019 qui met partiellement en relation les traitements dénommés HOPSYWEB relatifs au suivi des personnes en soins psychiatriques sans consentement, qui relève du RGPD, et le traitement dénommé fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) a pour finalité la prévention de la radicalisation à caractère terroriste.

2) a) Il s'ensuit qu'il relève, au même titre que ce dernier, des seules dispositions applicables aux traitements intéressant la sûreté de l'État et la défense aujourd'hui regroupées au sein du titre IV de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés ainsi que des dispositions communes à l'ensemble des traitements figurant aujourd'hui au titre I.

b) Il ne relève dès lors pas du champ d'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD), ni du titre II de la loi Informatique et Libertés relatif aux traitements relevant du régime de protection prévu par ce règlement désormais applicable.

CE, 10ème-9ème chambres réunies, 27 mars 2020, Cercle de réflexion et de proposition d'actions sur la psychiatrie et autres, n°431350, T., point 10

Traitement des données collectées via des techniques de recueil de renseignement à des fins de recherche et de développement – Titres I et IV de la loi Informatique et Libertés – Inclusion

Le traitement des données collectées par le biais de techniques de recueil de renseignement à des fins de recherche et de développement en matière de capacités techniques de recueil et d'exploitation des renseignements relève, compte tenu de ces finalités, des titres I et IV de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Il n'est pas pour autant soumis à une autorisation par arrêté ministériel ou décret en Conseil d'État pris après avis de la Commission, dès lors que des dispositions spéciales prévoient un mécanisme spécifique d'autorisation de mise en œuvre.

CNIL, SP, 8 avril 2021, Avis sur projet de loi, PJL Renseignement, n° 2021-040, publié, point 40

1.2.4 Personnes décédées (chapitre V du titre II loi Informatique et Libertés)

Conditions de réalisation des expertises génétiques sur une personne décédée à des fins d'actions en matière de filiation

En interdisant l'identification par les empreintes génétiques d'une personne décédée qui n'y avait pas expressément consenti de son vivant, la dernière phrase du cinquième alinéa de l'article 16-11 du code civil n'a pas porté atteinte au respect dû à la vie privée.

CC, 2011-173 QPC, 30 septembre 2011, M. Louis C. et autres, point 6

Qualité d'ayant droit d'un père décédé dont les données figurent dans un fichier intéressant la sûreté de l'État ou la défense – Qualité de personne concernée dudit ayant droit – Absence

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés n'ouvre la possibilité de demander la communication de données à caractère personnel figurant dans un traitement automatisé ou de solliciter un accès indirect à de telles données qu'à la personne concernée par celles-ci. La seule qualité d'ayant droit de son père décédé dont se prévaut une personne ne lui confère pas la qualité de personne concernée par les données susceptibles de concerner son père dans un fichier intéressant la sûreté de l'État ou la défense.

CE, Formation spécialisée, 2 décembre 2019, M. B... A..., n° 420917, Inédit., point 4

Ayant-droit d'une personne à laquelle se rapportent des données à caractère personnel – 1) Personne concernée (art.2 et 39 de la loi du 6 janvier 1978) – Absence en principe – 2) Exception – Héritiers de la victime d'un dommage ayant engagé une

action en réparation avant son décès ou ayant eux-mêmes engagé ultérieurement une telle action

1) Il résulte des dispositions des articles 2 et 39 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, que la communication de données à caractère personnel n'est possible qu'à la personne concernée par ces données. Par suite, la seule qualité d'ayant droit d'une personne à laquelle se rapportent des données ne confère pas la qualité de « personne concernée » par leur traitement au sens de ces dispositions.

2) Toutefois, lorsque la victime d'un dommage décède, son droit à la réparation de ce dommage, entré dans son patrimoine, est transmis à ses héritiers, saisis de plein droit des biens, droits et actions du défunt en application du premier alinéa de l'article 724 du code civil. Par suite, lorsque la victime a engagé une action en réparation avant son décès ou lorsque ses héritiers ont ultérieurement eux-mêmes engagé une telle action, ces derniers doivent être regardés comme des « personnes concernées » au sens des articles 2 et 39 de la loi du 6 janvier 1978 pour l'exercice de leur droit d'accès aux données à caractère personnel concernant le défunt, dans la mesure nécessaire à l'établissement du préjudice que ce dernier a subi en vue de sa réparation et pour les seuls besoins de l'instance engagée.

CE, 10ème-9ème chambres réunies, 7 juin 2017, M. X, n° 399446, T., points 2-3

1.2.5 Les traitements mixtes

Généralités

1) RGPD et directive (UE) 2016/680 – Champs d'application respectifs – a) Principe – Appréciation en fonction de la finalité du traitement – b) Application – Traitement ayant pour finalité le transfert de données fiscales vers l'administration fiscale américaine – Finalité d'amélioration du respect par les contribuables de leurs obligations fiscales – Conséquence – Traitement relevant du RGPD – 2) Appréciation de cette finalité sans incidence sur le champ des traitements soumis, en raison de leur objet, à des modalités procédurales particulières définies en droit interne

1) a) Un traitement de données à caractère personnel relève du champ d'application du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD) ou de la directive (UE) n° 2016/680 du même jour selon sa finalité.

b) Accord conclu le 14 novembre 2013 entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et de mettre en œuvre la loi relative au respect des obligations fiscales concernant les comptes étrangers (dite « loi FATCA »). Traitement d'échange automatique d'informations organisant notamment la collecte et le transfert de données à caractère personnel aux autorités fiscales américaines créé pour la mise en œuvre de cet accord.

Alors même que le traitement litigieux a plusieurs objets au nombre desquels figurent la prévention, la détection et la répression des infractions pénales, sa finalité est de permettre, en luttant contre la fraude et l'évasion fiscales, l'amélioration du respect de leurs obligations fiscales par les contribuables franco-américains. Il s'ensuit qu'il relève du champ d'application du RGPD et non de celui de la directive (UE) n°2016/680.

2) Un traitement ayant pour finalité de lutter contre la fraude et l'évasion fiscales est au nombre des traitements visés à l'article 31 de la loi n° 78-17 du 6 janvier 1978 dès lors qu'il a parmi ses objets la prévention, la recherche, la constatation ou la poursuite des infractions pénales.

CE, Assemblée, 19 juillet 2019, Association des Américains accidentels, n° 424216, Rec., points 8, 18

Traitements de données relevant à la fois du champ de la directive et de celui du règlement ou du droit interne – 1) Finalités mixtes – Mise en œuvre par un acte législatif ou réglementaire – 2) Double régime et droits des personnes concernées – a) Traitements directive – Règlement – Conditions – Diminution de la portée du droit à l'oubli et droit à la portabilité des données prévue par l'acte – b) Traitements directive – Droit interne – Condition – Restriction limitée des droits

Le Conseil d'État constate qu'existent des traitements de données à caractère personnel qui relèvent à la fois du champ de la directive, en raison de certaines de leurs finalités, et du champ du règlement (UE) 2016/679 ou du droit interne, en raison de leurs autres finalités. Cette situation est traitée par l'article 9 de la directive (UE) 2016/680, qui dispose que le traitement à d'autres fins de données collectées dans le champ de la directive n'est possible que si un tel traitement est autorisé par le droit de l'Union ou le droit de l'État-membre et que, dès lors que les données sont traitées à d'autres fins, le règlement s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.

1) D'une part, le Conseil d'État en conclut que, lorsqu'un traitement de données répond à des finalités mixtes, il convient que sa mise en œuvre soit prévue par un acte législatif ou règlementaire ou un acte répondant aux exigences de clarté, de précision et de prévisibilité rappelées au considérant 33 de la directive. Le Conseil d'État relève d'ailleurs que l'existence d'un tel acte est également nécessaire, lorsqu'il est envisagé d'apporter des restrictions aux droits des personnes concernées en application des articles 13, 15 et 16 de la directive, transposés à l'article 70-21 de la loi du 6 janvier 1978.

2) D'autre part, le Conseil d'État estime que l'article 9 de la directive impose un double régime aux traitements de données à finalités mixtes.

S'agissant des traitements relevant à la fois du champ de la directive et de celui du règlement, ce double régime paraît complexe à mettre en œuvre pour les droits des personnes concernées. Le Conseil d'État relève en effet qu'existent deux droits prévus par le règlement et absents de la directive : le droit à l'oubli et le droit à la portabilité des données. Dans les deux cas, le règlement prévoit que ces droits ne sont pas applicables, lorsque le traitement est nécessaire « à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ». Ces droits devraient donc être inapplicables aux traitements de données dont les finalités sont mixtes. Les autres droits des personnes concernées (information, accès, opposition…) sont plus ouverts dans le règlement que dans la directive. Le Conseil d'État estime que, dès lors que les données sur lesquelles la personne concernée demande à exercer ses droits ne pourront pas être exclusivement rattachées soit aux finalités prévues par la directive, soit aux autres finalités du traitement de données, il convient que l'acte ayant autorisé le traitement de données à finalités mixtes s'appuie sur l'article 23 du règlement, qui permet une diminution de la portée des droits de la personne concernée sous plusieurs conditions, dont la sécurité publique et la préservation des procédures pénales, afin de déterminer un régime des droits des personnes concernées cohérent pour l'ensemble des données traitées pour les diverses finalités. Pour être conforme aux exigences du second paragraphe de l'article 23 du règlement, les dispositions apportant de telles limitations doivent être précises et ne sauraient prendre la forme d'habilitations générales.

S'agissant des traitements relevant à la fois du champ de la directive et de celui du droit interne, dès lors que les données sur lesquelles la personne concernée demande à exercer ses droits ne peuvent être exclusivement rattachées à l'un ou l'autre de ces deux champs, les restrictions apportées à ces droits ne pourront excéder celles prévues par la directive.

CE, Assemblée générale (section de l'intérieur), 7 décembre 2017, Avis n°393836, Projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Traitements automatisés de données à caractère personnel provenant de dispositifs de vidéosurveillance installés dans les emprises des locaux et centres de rétention administrative et des zones d'attente

Dans la mesure où des dispositifs vidéo sont installés dans les emprises des locaux et centres de rétention administrative ainsi que des zones d'attente relevant de la compétence de la police et de la gendarmerie nationales, il s'agit de dispositifs de « vidéosurveillance » car ces derniers filment des lieux non ouverts au public. À ce titre, le code de la sécurité intérieure, qui régit les dispositifs de « vidéoprotection » filmant la voie publique ou des lieux ouverts au public, n'est pas applicable et seules les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et du RGPD encadrent la mise en œuvre de tels traitements.

Le placement en centre ou en lieu de rétention est indépendant de toute qualification pénale. Le contrôle du respect des règles de sécurité du règlement intérieur de chaque local de rétention administrative et des règles de contrôle d'accès ne relève pas non plus d'une finalité pénale. Il en va de même de la finalité relative à la collecte de preuves dans le cadre des procédures administratives et disciplinaires.

En revanche, les missions de maintien de la sécurité publique par les forces de l'ordre au sein des centres et lieux de rétention sont susceptibles de relever de la directive « Police-Justice ». Les traitements automatisés de données à caractère personnel provenant de dispositifs de vidéosurveillance installés dans les emprises des locaux et centres de rétention administrative ainsi que des zones d'attente devraient donc relever d'un régime mixte (RGPD et directive « Police-Justice » tel que transposée au titre III de la loi du 6 janvier 1978 dite « Informatique et Libertés ») en fonction des finalités poursuivies.

CNIL, P, 31 mars 2022, Avis sur projet d'arrêté, VidéoCRA, n° 2022-045, publié, points 5, 7

Crise sanitaire – Traitement mis en œuvre dans le cadre du suivi de mesures individuelles de quarantaine et d'isolement et à l'accompagnement des personnes – Régime mixte

Les finalités d'un traitement, mis en œuvre dans un contexte de crise sanitaire, liées au suivi du respect de mesures individuelles de quarantaine et d'isolement et à l'accompagnement des personnes en faisant l'objet relèvent du RGPD par leur visée sanitaire. Lorsque le contrôle de ces mesures individuelles, entendu notamment par la constatation des infractions pénales associées, apparait également au titre des finalités du même traitement, que celui-ci est placé sous la responsabilité conjointe du ministre chargé de la santé et du ministre de l'intérieur et que plusieurs services du ministère de l'intérieur accèdent ou sont rendus destinataires des données qui y sont enregistrées, il y a lieu de considérer que la prévention, la recherche et la constatation d'infractions pénales constituent une des finalités dudit traitement, et non un objet de ce traitement sans incidence sur son régime juridique.

Dans ces conditions, et dès lors que le critère de l'autorité compétente prévue par la Directive « Police-Justice » est rempli, un tel traitement relève d'un régime mixte, à savoir le RGPD pour la finalité de suivi des mesures individuelles et le titre III de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée, pour la finalité de contrôle du respect de ces mesures par la constatation des infractions pénales associées, ce qui doit notamment apparaitre dans les dispositions réglementaires encadrant le traitement en cause.

CNIL, SP, 12 mai 2021, Avis sur projet de décret, n° 2021-055, non publié

Voir aussi : CE, Assemblée, 19 juillet 2019, Association des Américains accidentels, n°424216, Rec.

Juridictions compétentes pour le contentieux portant sur les traitements mixtes

Il résulte des articles L. 841-2 et R. 841-2 du code de la sécurité intérieur que la formation spécialisée du Conseil d'État statuant au contentieux n'est compétente, en ce qui concerne les litiges relatifs à l'accès indirect aux données recueillies dans le fichier STARTRAC, que pour celles de ces données qui intéressent la sûreté de l'État. Le tribunal administratif et la cour administrative d'appel restent compétents en première instance et en appel pour connaître des litiges relatifs à l'accès indirect aux données recueillies dans ce même fichier n'intéressant pas la sûreté de l'État.

CE, 10ème–9ème chambres réunies, 10 novembre 2021, M. M... B..., n° 444992, Inédit., point 7

Traitement de données à caractère personnel – Fichier mixte – Traitements dont la finalité relève pour partie de la sécurité publique et pour partie de la sûreté de l'État – Nécessité de définir les données intéressant la sûreté de l'État

Le Conseil d'État (section de l'intérieur) a donné un avis favorable à trois projets de décret modifiant les dispositions du code de la sécurité intérieure relatives aux traitements de données à caractère personnel dénommés « Enquêtes administratives liées à la sécurité publique » (EASP), « Prévention des atteintes à la sécurité publique » (PASP) et « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP).

En premier lieu ces projets ajoutent à la finalité de « sécurité publique » des trois traitements, celle de « sûreté de l'État ». Par suite, les trois traitements deviennent des fichiers mixtes, les données intéressant la sécurité publique relevant du titre III de la loi n° 78-17 du 6 janvier 1978 et de la directive 2016/680, et celles intéressant la sûreté de l'État du titre IV de la loi du 6 janvier 1978 dite « Informatique et Libertés », et du RGPD.

Ces deux groupes de données étant ainsi soumis à des régimes juridiques distincts, notamment quant aux droits d'accès, de rectification et d'effacement des personnes concernées, le Conseil d'État a considéré nécessaire que les trois projets de décret comportent une définition des données intéressant la sûreté de l'État, la notion de sûreté de l'État n'ayant jamais été définie par une disposition législative ou réglementaire, ni par la jurisprudence. S'inspirant des dispositions de l'article 410-1 du code pénal et de l'article L. 811-1 du code de la sécurité intérieure qui traitent des intérêts fondamentaux de la Nation, et aux seules fins de préciser les finalités des traitements concernés, le Conseil d'État propose que les articles 1ers des trois projets de décret soient complétés afin de prévoir que « Les données intéressant la sûreté de l'État sont celles qui révèlent des activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste portant atteinte à ces mêmes intérêts (...) » .

En second lieu le Conseil d'État a considéré que l'indication de l'enregistrement ou non d'une personne dans les traitements de données énumérées par les articles modifiés R. 236-2, R. 236-12 et R. 236-22 du code de la sécurité intérieure, ainsi que l'enregistrement de données à caractère personnel issues d'autres traitements, constituaient une mise en relation de fichier et non une interconnexion. En effet, ces enregistrements ne procèdent ni d'une consultation automatique d'un des traitements énumérés, aux fins de vérifier si l'identité d'une personne y est enregistrée, ni d'une inscription automatique de cette information ou d'autres informations la concernant au nombre des données pouvant être enregistrées dans l'un des trois traitements examinés.

CE, Section de l'intérieur, 3 mars 2020, Avis n° 401352, 401354, 401355, Projets de décrets modifiant les dispositions du code de la sécurité intérieure relatives aux traitements de données à caractère personnel dénommés « Prévention des atteintes à la sécurité publique » (PASP), « Enquêtes administratives liées à la sécurité publiques » (EASP) , « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP)

1.2.6 Traitements mis en œuvre dans des circonstances exceptionnelles

Covid-19

Extension de l'accès aux données des personnes atteintes de la covid-19 – Respect du droit à la vie privée – Conditions

Les données relatives à la santé des personnes atteintes par le virus responsable de la covid-19 et des personnes en contact avec elles sont, le cas échéant sans leur consentement, traitées et partagées à travers un système d'information ad hoc. Ne méconnaît pas le droit au respect de la vie privée l'extension de l'accès à ces données à certains professionnels de santé qui participent à l'établissement du diagnostic et à l'identification des chaines de contamination, sans consentement préalable, dès lors que ces professionnels ne peuvent avoir accès qu'aux seules données nécessaires à leur intervention et dans la stricte mesure où leur intervention sert les finalités poursuivies par le système d'information ; aux organismes assurant l'accompagnement social des personnes infectées ou susceptibles de l'être, lorsque cet accès est subordonné au recueil préalable du consentement des intéressés et ne peut porter que sur les données strictement nécessaires à l'exercice de la mission de ces organismes (voir à ce sujet la censure sous DC 2020-800).

CC, 2020-808 DC, 13 novembre 2020, Loi autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise sanitaire, points 16-24

Traitement des données relatives à la santé des personnes atteintes par la covid-19 et des personnes en contact avec elles sans consentement préalable – OVC de protection de la santé – Contrôle de la proportionnalité du traitement StopCovid

L'article 11 contesté prévoit que, par dérogation à l'exigence fixée à l'article L. 1110-4 du code de la santé publique, les données à caractère personnel relatives à la santé des personnes atteintes par la covid-19 et des personnes en contact avec elles peuvent être traitées et partagées, sans le consentement des intéressés, dans le cadre d'un système d'information ad hoc ainsi que dans le cadre d'une adaptation des systèmes d'information relatifs aux données de santé déjà existants. La collecte, le traitement et le partage d'informations portent donc non seulement sur les données médicales personnelles des intéressés, mais aussi sur certains éléments d'identification et sur les contacts qu'ils ont noués avec d'autres personnes. Ce faisant, les dispositions contestées portent atteinte au droit au respect de la vie privée. Toutefois ce dispositif n'est pas contraire à la Constitution dès lors que :

- le législateur a entendu renforcer les moyens de lutte contre l'épidémie et poursuit l'objectif de valeur constitutionnelle (OVC) de protection de la santé ;
- le traitement des données ne peut être mis en œuvre que dans la mesure strictement nécessaire à quatre finalités précisément définies en lien avec cet objectif de valeur constitutionnelle ;
- le champ des données susceptibles de faire l'objet du traitement en cause est circonscrit aux seules données relatives à la covid-19 et strictement nécessaires à la poursuite de ces finalités ;
- le champ des personnes pouvant accéder aux données collectées, bien que large, est proportionné compte tenu de l'étendue des démarches à entreprendre pour organiser la

collecte des informations nécessaires à la lutte contre le développement de l'épidémie. Par ailleurs, diverses garanties sont prévues par la loi (secret professionnel, encadrement de l'accès aux données pour les seules finalités dont relèvent les organismes concernés…) ;
- le traitement de ces données reste soumis aux règles issues du RGPD et de la loi du 6 janvier 1978 dite « Informatique et Libertés » ;
- ce dispositif ne peut s'appliquer au-delà du temps strictement nécessaire à la lutte contre la propagation de l'épidémie de covid-19 et les données à caractère personnel collectées, qu'elles soient ou non médicales, doivent, quant à elles, être supprimées trois mois après leur collecte ;
- le décret d'application de la loi est pris après avis public de la Commission nationale de l'informatique et des libertés.

Le Conseil constitutionnel émet néanmoins des réserves :

- l'anonymisation prévue des données nominatives pour ce qui concerne la finalité de surveillance épidémiologique et de recherche contre le virus doit s'étendre aux coordonnées de contact électronique et téléphonique ;
- le recueil de ces données sans consentement préalable par des organismes d'accompagnement social méconnaît le droit au respect de la vie privée dans la mesure où l'accompagnement ne relève pas directement de la lutte contre l'épidémie ;
- il appartiendra au pouvoir réglementaire de définir des modalités de collecte, de traitement et de partage des informations assurant leur stricte confidentialité et, notamment l'habilitation spécifique des agents chargés, au sein de chaque organisme, de participer à la mise en œuvre du système d'information ainsi que la traçabilité des accès à ce système d'information ;
- le recours à des sous-traitants, qui agissent pour leur compte et sous leur responsabilité, doit s'effectuer en conformité avec les exigences de nécessité et de confidentialité des données.

CC, 2020-800 DC, 11 mai 2020, Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, points 62-78

1.3 Notions principales

1.3.1 Donnée à caractère personnel

Signature manuscrite – Inclusion

L'article 4, point 1, du règlement 2016/679 du 27 avril 2016 (RGPD) doit être interprété en ce sens que la signature manuscrite d'une personne physique relève de la notion de « données à caractère personnel » au sens de cette disposition.

CJUE, 4 octobre 2024, Agentsia po vpisvaniyata, C 200/23

VIN (Vehicule Identification Number) – Inclusion sous conditions – Moyens raisonnables de rattacher un VIN à une personne physique ou identifiable

Le VIN (Vehicule Identification Number), code alphanumérique attribué au véhicule par son constructeur afin d'assurer l'identification adéquate de ce véhicule et qui, en tant que tel, est dépourvu de caractère « personnel », acquiert ce caractère à l'égard de quiconque dispose raisonnablement de moyens permettant de l'associer à une personne déterminée.

Or, il résulte de l'annexe I, point II.5, de la directive 1999/37 que le VIN doit figurer dans le certificat d'immatriculation d'un véhicule, tout comme le nom et l'adresse du titulaire de ce certificat. En outre, en vertu des points II.5 et II.6 de cette annexe, une personne physique peut être désignée dans ledit

certificat comme propriétaire du véhicule ou comme une personne pouvant disposer du véhicule à un titre juridique autre que celui de propriétaire. Dans ces conditions, le VIN constitue une donnée à caractère personnel, au sens de l'article 4, point 1, du RGPD, de la personne physique mentionnée dans le même certificat, dans la mesure où celui qui y a accès pourrait disposer de moyens lui permettant de l'utiliser pour identifier le propriétaire du véhicule auquel il se rapporte ou la personne pouvant disposer de ce véhicule à un titre juridique autre que celui de propriétaire.

Lorsque les opérateurs indépendants [personnes physiques ou morales, autres qu'un concessionnaire ou réparateur agréé, qui sont directement ou indirectement engagées dans la réparation et l'entretien de véhicules] peuvent raisonnablement disposer des moyens leur permettant de rattacher un VIN à une personne physique identifiée ou identifiable, ce VIN constitue pour eux une donnée à caractère personnel, au sens de l'article 4, point 1, du RGPD, ainsi que, indirectement, pour les constructeurs automobiles qui le mettent à disposition, même si le VIN n'est pas, en soi, pour ces derniers une donnée à caractère personnel et ne l'est pas, en particulier, lorsque le véhicule auquel ce VIN a été attribué n'appartient pas à une personne physique.

CJUE, 9 novembre 2023, Gesamtverband Autoteile-Handel, C-319/22, points 46-50

Enregistrement, par un titulaire de droits de propriété intellectuelle ou par un tiers, d'adresses IP d'utilisateurs d'un réseau de pair à pair aux fins d'une action en indemnisation – Inclusion – Condition de licéité – Demande justifiée, proportionnée et non abusive formulée sur le fondement d'une mesure législative nationale qui limite la portée de certains droits et obligations au sens de l'article 15§1 de la directive ePrivacy

L'article 6, paragraphe 1, premier alinéa, sous f), du RGPD, lu en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002 (directive vie privée et communications électroniques), doit être interprété en ce sens qu'il ne s'oppose, en principe, ni à l'enregistrement systématique, par le titulaire de droits de propriété intellectuelle ainsi que par un tiers pour son compte, d'adresses IP d'utilisateurs de réseaux de pair à pair (peer-to-peer) dont les connexions internet ont été prétendument utilisées dans des activités contrefaisantes ni à la communication des noms et des adresses postales de ces utilisateurs à ce titulaire ou à un tiers afin de lui permettre d'introduire un recours en indemnisation devant une juridiction civile pour un dommage prétendument causé par lesdits utilisateurs, à condition toutefois que les initiatives et les demandes en ce sens dudit titulaire ou d'un tel tiers soient justifiées, proportionnées et non abusives et trouvent leur fondement juridique dans une mesure législative nationale, au sens de l'article 15, paragraphe 1, de la directive 2002/58, qui limite la portée des règles énoncées aux articles 5 et 6 de cette directive.

CJUE, 17 juin 2021, M.I.C.M., C-597/19

Image d'une personne enregistrée par une caméra – Donnée à caractère personnel – Inclusion

L'image d'une personne enregistrée par une caméra constitue une « donnée à caractère personnel », au sens de l'article 2, sous a), de la directive 95/46, dans la mesure où elle permet d'identifier la personne concernée.

CJUE, 14 février 2019, Buivids, C-345/17, point 31

Voir aussi : CJUE, 11 décembre 2014, Ryneš, C-212/13, point 22

Réponses écrites fournies par le candidat à un examen professionnel – Annotations de l'examinateur relatives à ces réponses – Inclusion

Les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examinateur relatives à ces réponses constituent des données à caractère personnel. Le candidat a, en principe, un droit d'accès à ces données.

CJUE, 20 décembre 2017, Nowak, C-434/16

Adresse de protocole internet dynamique – Inclusion

Une adresse de protocole internet dynamique dite « adresse IP », enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site internet que ce fournisseur rend accessible au public, constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de l'article 2, sous a), de la directive 95/46, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à internet de cette personne.

CJUE, 19 octobre 2016, Breyer, C-582/14

Voir aussi : CJUE, 17 juin 2021, M.I.C.M., C-597/19, point 102

Opinions exprimées par des experts à titre professionnel dans le cadre des travaux d'une agence de l'Union – Inclusion

La notion de données à caractère personnel ne se confond pas avec celle de données relatives à la vie privée. Ainsi, les opinions exprimées par des experts à titre professionnel, dans le cadre des travaux d'une agence de l'Union, ne relèvent pas de leur vie privée, mais n'en sont pas moins des données à caractère personnel.

CJUE, 16 juillet 2015, ClientEarth et PAN Europe /EFSA, C-615/13 P, point 32

Données relatives à une personne physique contenues dans un document administratif préparatoire – Données figurant dans l'analyse juridique de la décision – Inclusion

Les données relatives au demandeur d'un titre de séjour figurant dans un document administratif, telle que la « minute » en cause au principal, exposant les motifs que l'agent instructeur avance à l'appui du projet de décision qu'il est chargé de rédiger dans le cadre de la procédure préalable à l'adoption d'une décision relative à la demande d'un tel titre, et, le cas échéant, celles figurant dans l'analyse juridique que contient ce document constituent des « données à caractère personnel », au sens de la directive 95/46/CE du 24 octobre 1995. Tel n'est pas le cas en revanche de ladite analyse juridique : si celle-ci peut certes contenir des données à caractère personnel, elle ne constitue pas pour autant en elle-même une telle donnée.

CJUE, 17 juillet 2014, YS, C-141/12,C-372/12

Registre de temps de travail – Conditions – Inclusion

Un registre du temps de travail qui comporte l'indication pour chaque travailleur des heures de début et de fin du travail, ainsi que des interruptions ou des pauses correspondantes, relève de la notion de « données à caractère personnel », au sens de l'article 2 de la directive 95/46/CE.

CJUE, 30 mai 2013, Worten, C-342/12

Adresse IP – Inclusion

Les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, au sens de l'article 2 de la loi du 6 janvier 1978 dite « Informatique et Libertés », de sorte que leur collecte constitue un traitement de données à caractère personnel.

Cass, 1ère civ., 3 novembre 2016, n° 15-22.595, B., point 5

Résultats d'un sondage portant sur une personne représentant l'état statistique de l'opinion de la population à un moment donné – Exclusion

Les résultats d'un sondage portant sur une personne, qui représentent l'état statistique, à un moment donné, de l'opinion de la population sur celle-ci, ne constituent pas une information nominative au sens de l'article 4 de la loi du 6 janvier 1978 dite « Informatique et Libertés ». Il s'en déduit que, dès lors que les résultats ne lui sont pas opposés, cette personne ne saurait bénéficier du droit d'accès et des prérogatives qui en découlent, prévus par les articles 34 et suivants de ladite loi, ni exiger la communication du nom du commanditaire de l'opération.

Cass, crim., 12 mai 1998, n° 96-85.900, B., point 5

Entrepreneur individuel pris en cette qualité – Personne physique – Exclusion

Il résulte des termes mêmes des dispositions des articles 4 et 5 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, éclairées au surplus par leurs travaux préparatoires, que les informations nominatives qu'elles mentionnent sont celles qui permettent d'identifier des personnes physiques. Les entrepreneurs individuels, pris en cette qualité, ne sont pas des personnes physiques pour l'application de ces dispositions.

CE, Section, 3 juillet 2002, Ministre de l'équipement, des transports et du tourisme, n° 157402, T., point 2

Résultats d'un sondage portant sur l'image d'une personnalité – Absence d'informations nominatives concernant cette personnalité – Exclusion

Les résultats d'un sondage comportant des questions qui demandent aux personnes interrogées ce qu'elles pensent d'une personnalité ne constituent pas des informations nominatives concernant cette personnalité. Celle-ci ne saurait, par suite, être titulaire du droit d'accès organisé par l'article 34 de la loi du 6 janvier 1978, ni des droits de communication, de rectification et d'effacement qui en découlent.

CE, Section, 9 juillet 1997, Chambre syndicale Syntec Conseil, n° 148975, Rec., point 4

Combinaison de traces laissées par un témoin de connexion ou une adresse IP à des identifiants uniques ou à d'autres informations – Caractère identifiant ou non d'une donnée – Nécessaire prise en considération de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne – Espèce

Le considérant 30 du RGPD, qui s'inscrit dans une jurisprudence bien établie de la Cour de justice de l'Union européenne (CJUE, 24 nov. 2011, Scarlet Extended SAC 70/10, pt. 51 et 19 oct. 2016, Breyer, C-582/14) prévoit qu'un identifiant en ligne associé à une personne physique, tel qu'une adresse IP ou un témoin de connexion, peut « laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes ».

Dans son arrêt Breyer précité, la CJUE a souligné l'importance d'une approche casuistique du caractère identifiant ou non d'une donnée plutôt qu'une position générale et de principe. Elle a indiqué que, pour déterminer si une personne est identifiable, il convenait de prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne.

En l'espèce, l'identifiant attribué par la société au moyen des cookies qu'elle dépose, a pour but de distinguer chaque individu dont elle collecte les données et de très nombreuses informations destinées à enrichir le profil publicitaire de l'internaute sont associées à cet identifiant, parmi lesquelles : des données liées à l'identification de la personne (emplacement géographique à partir d'adresse IP, identifiant utilisateur, identifiant de terminal, identifiants fournis par des partenaires, adresse de courrier électronique sous forme hachée fournie par les partenaires), des données liées à l'activité de la personne (suivi de l'historique de navigation de l'internaute à travers les sites visités, les produits consultés, ceux ajoutés au panier ainsi que l'acte d'achat, les éventuelles interactions de l'utilisateur avec les publicités qui lui sont présentées : l'utilisateur a-t-il cliqué sur la bannière ? a-t-il procédé à un achat ?), ou encore des données dérivées ou inférées à partir des informations précédentes afin de pouvoir proposer à l'utilisateur les produits les plus pertinents, compte tenu de ses centres d'intérêt.

Pour la CNIL, si la société ne dispose pas directement de l'identité des personnes physiques auxquelles sont liés les terminaux sur lesquels des cookies sont inscrits, la réidentification peut être facilitée par le fait que, dans certaines hypothèses, la société collecte, outre les données liées aux évènements de navigation, d'autres données qui facilitent la réidentification telles que les adresses électroniques des personnes ayant fait leur parcours de navigation depuis un environnement authentifié (ou « logué ») sous forme hachée, des identifiants leur correspondant générés par d'autres acteurs, l'adresse IP sous forme hachée ou encore l'agent utilisateur du terminal utilisé. Par conséquent, dès lors que la société est en mesure de réidentifier des personnes par des moyens raisonnables, les données traitées conservent un caractère personnel, au sens de l'article 4, 1) du RGPD.

CNIL, FR, 15 juin 2023, Sanction, Société X, n°SAN-2023-009, publié, points 32-33, 39-41

Adresse postale – Identification indirecte – Inclusion

La formation restreinte considère que l'adresse postale peut constituer une donnée à caractère personnel indirectement identifiante dans la mesure où, notamment combinée à d'autres informations, elle peut, dans certaines conditions, permettre l'identification d'une personne. C'est par exemple le cas lorsqu'une seule personne habitue à cette adresse ou lorsque l'adresse est combinée à un numéro de téléphone ou à des données de réseaux telles que l'identifiant Wi-Fi ou l'adresse MAC d'un routeur.

CNIL, FR, 3 juin 2021, Sanction, Société X, n° SAN-2021-007, non publié

Propos tenus dans le cadre d'une conversation téléphonique – Inclusion

L'ensemble des propos tenus dans la cadre d'une conversation téléphonique enregistrée sont susceptibles de constituer des données à caractère personnel concernant les deux parties à cette conversation.

CNIL, P, 10 décembre 2020, Mise en demeure, Société X, n° MED-2020-043, non publié

1.3.2 Personne concernée

Principe – Ayant droit d'une personne décédée à laquelle se rapportent des données à caractère personnel – Qualité de personne concernée – Exclusion

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés n'ouvre la possibilité de demander la communication de données à caractère personnel figurant dans un traitement automatisé ou de solliciter un accès indirect à de telles données qu'à la personne concernée par celles-ci. La seule qualité d'ayant droit de son père décédé dont se prévaut une personne ne lui confère pas la qualité de personne concernée par les données susceptibles de concerner son père dans un fichier intéressant la sûreté de l'État ou la défense.

CE, Formation spécialisée, 2 décembre 2019, M. B... A..., n° 420917, Inédit., point 4

Exception – Héritiers de la victime d'un dommage ayant engagé une action en réparation avant son décès ou ayant eux-mêmes engagé ultérieurement une telle action – Qualification

1) Il résulte des dispositions des articles 2 et 39de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, que la communication de données à caractère personnel n'est possible qu'à la personne concernée par ces données. Par suite, la seule qualité d'ayant droit d'une personne à laquelle se rapportent des données ne confère pas la qualité de « personne concernée » par leur traitement au sens de ces dispositions.

2) Toutefois, lorsque la victime d'un dommage décède, son droit à la réparation de ce dommage, entré dans son patrimoine, est transmis à ses héritiers, saisis de plein droit des biens, droits et actions du défunt en application du premier alinéa de l'article 724 du code civil. Par suite, lorsque la victime a engagé une action en réparation avant son décès ou lorsque ses héritiers ont ultérieurement eux-mêmes engagé une telle action, ces derniers doivent être regardés comme des « personnes concernées » au sens des articles 2 et 39 de la loi n°78-17 du 6 janvier 1978 pour l'exercice de leur droit d'accès aux données à caractère personnel concernant le défunt, dans la mesure nécessaire à l'établissement du préjudice que ce dernier a subi en vue de sa réparation et pour les seuls besoins de l'instance engagée.

CE, 10ème – 9ème chambres réunies, 7 juin 2017, M. X, n° 399446, T., points 2-3

1.3.3 Données sensibles

Article 9 RGPD – Données dévoilant indirectement des informations sensibles – Application

L'article 9 RGPD s'applique à des traitements portant non seulement sur les données intrinsèquement sensibles auxquelles a trait celle-ci, mais également sur des données dévoilant indirectement, au

terme d'une opération intellectuelle de déduction ou de recoupement, des informations de cette nature.

Une interprétation large de la notion de « données sensibles » est confortée par l'objectif du RGPD qui est de garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel les concernant. Une telle interprétation est également conforme à la finalité de l'article 9, paragraphe 1, du RGPD, consistant à assurer une protection accrue à l'encontre de traitements qui, en raison de la sensibilité particulière des données qui en sont l'objet, sont susceptibles de constituer, comme il ressort du considérant 51 de ce règlement, une ingérence particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, garantis aux articles 7 et 8 de la Charte.

CJUE, grande chambre, 5 juin 2023, Commission c/ Pologne, C-204/21, points 344-345

Voir aussi : CJUE, grande chambre, 1er août 2022, Vyriausioji tarnybines etikos komisija, C-184/20

Données nominatives relatives au conjoint, concubin ou partenaire publiées en ligne dans la déclaration d'intérêts privés susceptibles de divulguer indirectement l'orientation sexuelle – Inclusion

Un traitement de données à caractère personnel susceptible de dévoiler, de manière indirecte, des informations sensibles concernant une personne physique peut relever de la protection renforcée du régime des catégories particulières de données au sens de l'article 9, paragraphe 1, du RGPD.

Tel est le cas de la publication, sur le site internet de l'autorité publique chargée de collecter et de contrôler la teneur des déclarations d'intérêts privés, de données à caractère personnel susceptibles de divulguer indirectement l'orientation sexuelle d'une personne physique.

CJUE, grande chambre, 1er août 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, points 127-128

Enregistrement de vidéosurveillance susceptible de contenir des données sensibles ou des données d'infraction – Absence de qualification automatique

Un enregistrement vidéo, quoiqu'il puisse contenir des images révélant des données sensibles ou des données d'infraction, n'est pas considéré en soi comme relevant de ces catégories particulières de données à caractère personnel. En revanche, si les images font l'objet d'un traitement spécifique sur des données sensibles ou d'infraction, l'article 6 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ou l'article 10 du RGPD seraient susceptibles de s'appliquer.

CNIL, P, 31 mars 2022, Avis sur projet d'arrêté, VidéoCRA, n° 2022-045, publié, point 12

Voir aussi : CNIL, SP, 25 juin 2020, Avis sur projet de décret, PASP, n° 2020-064, publié

Conditions applicables aux traitements de données sensibles relevant du seul titre Ier – Application des exceptions prévues à l'article 9 du RGPD aux traitements relevant du RGPD mais aussi aux traitements relevant du seul titre Ier de la loi Informatique et Libertés

En vertu de l'article 6 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés (ci-après LIL), le traitement des données sensibles n'est

possible, sauf disposition législative spéciale l'autorisant, que s'il s'inscrit dans le cadre de l'une des exceptions prévues à l'article 9 du RGPD ou, s'agissant de traitements relevant du champ d'application des articles 31 et 32 de la loi Informatique et Libertés (en particulier le champ d'application de la directive « Police-Justice » et les traitements intéressant la sûreté et la défense nationale), s'il est autorisé selon les modalités prévues à ces articles, à savoir un décret en Conseil d'État après avis de la CNIL.

Il y a lieu d'interpréter le titre Ier de la LIL de façon à ce que ses dispositions ne portent pas une atteinte disproportionnée à des droits ou objectifs de valeur constitutionnelle. Dès lors, il est nécessaire de lire la loi de sorte que les traitements ne relevant que du titre Ier puissent bénéficier de certaines exceptions à l'interdiction de traiter des données sensibles, notamment pour les données manifestement rendues publiques, pour les traitements d'intérêt public, ou en cas de consentement de la personne. Le renvoi aux exceptions de l'article 9 du RGPD opéré par l'article 6 de la LIL doit être entendu comme ayant vocation à s'appliquer non seulement aux traitements relevant du RGPD mais aussi aux traitements relevant des autres titres, et notamment ceux relevant du seul titre Ier.

Cette question ne se pose que pour le titre Ier dès lors que, pour les traitements du titre III (directive « Police-Justice »), la loi a prévu des dispositions spéciales, transposant la directive sur ce point et que, pour ceux du titre IV, tous les traitements relèveront du champ des articles 31 et 32 et seront autorisés par décret en Conseil d'État.

CNIL, P, 17 février 2022, Avis sur projet de décret, n° 2022-021, non publié

Données révélant l'origine raciale ou ethnique

Données révélant les opinions politiques

Les données relatives à l'abstention électorale ne sont pas de nature à faire apparaître les opinions politiques.

Les informations individuelles détenues par l'Institut national de la statistique et des études économiques (INSEE), collectées à partir des listes d'émargement de scrutins électoraux et relatives à la participation électorale ou aux abstentions constatées lors de ces scrutins, ne peuvent être regardées comme de nature à faire apparaître, même indirectement, les opinions politiques ou philosophiques des individus concernés, au sens et pour l'application de l'article 31 de la loi du 6 janvier 1978relative à l'informatique, aux fichiers et aux libertés.. Par suite, la création d'un traitement automatisé de ces informations ne figure pas au nombre des mesures qui, en vertu de cet article, ne peuvent être prises qu'avec le consentement exprès des intéressés ou par décret en Conseil d'État pris sur proposition ou avis conforme de la Commission nationale de l'informatique et des libertés.

CE, Section, 10 mars 2004, M.C, n° 252691, T., point 3

Données révélant les convictions religieuses

Enregistrement et traitement automatisé de données nominatives sensibles [article 31 de la loi n° 78-17 du 6 janvier 1978] – Fichier informatique contenant des données nominatives faisant apparaître les origines raciales, les opinions politiques,

philosophiques ou religieuses ou les appartenances syndicales des personnes – Existence

Le fichier créé par l'arrêté du 28 février 1984 du secrétaire d'Etat auprès du ministre des affaires sociales et de la solidarité nationale chargé des rapatriés concerne exclusivement des personnes visées à l'article 2 de l'ordonnance du 21 juillet 1962 qui définit les conditions dans lesquelles les « personnes de statut civil de droit local originaires d'Algérie » peuvent se faire reconnaître la nationalité française. Ce fichier fait ainsi apparaître indirectement les opinions religieuses des personnes intéressées.

CE, Section, 5 juin 1987, M.X, n° 59674, Rec., point 3

Voir aussi : CJUE, grande chambre, 1er août 2022, Vyriausioji tarnybinės etikos komisija, C-184/20

Données révélant les convictions philosophiques

Données révélant l'appartenance syndicale

Données génétiques

Données biométriques

Passeport biométrique – Empreintes digitales – Règlement (CE) n° 2252/2004 – Article 1er, paragraphe 2 – Validité – Fondement juridique – Procédure d'adoption – Articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne – Droit au respect de la vie privée – Droit à la protection des données à caractère personnel – Proportionnalité

Il n'a pas été porté à la connaissance de la Cour l'existence de mesures susceptibles de contribuer, de manière suffisamment efficace, au but tenant à la protection des passeports contre leur utilisation frauduleuse, tout en portant des atteintes moins importantes aux droits reconnus par les articles 7 et 8 de la Charte que celles entraînées par la méthode fondée sur les empreintes digitales. Ce recueil est donc proportionné.

CJUE, 17 octobre 2013, Schwarz, C-291/12, point 53

Voir aussi : CE, Assemblée, 26 août 2011, Association pour la promotion de l'image & autres, n°317827

Donnée faisant état d'un handicap sans donner d'information sur sa nature – Exclusion

La mention du taux d'incapacité permanente ou du taux d'invalidité du « conjoint ou partenaire » et des personnes à la charge de l'agent n'est pas une donnée « relative à la santé » au sens des dispositions précitées de l'article 8 la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dès lors qu'il n'est pas même allégué qu'elle donnerait une information sur la nature du handicap.

CE, 10ème/9ème SSR, 28 mars 2014, Syndicat National des Enseignements de Second Degré (SNES), n° 361042, T., point 15

Catégorie de classe d'intégration scolaire (CLIS) – Inclusion – Structure de soins accueillant des élèves – Exclusion

La mention exacte, dans la « Base élèves 1er degré », de la catégorie de classe d'intégration scolaire (CLIS) dont relève l'élève, identifiée par l'un des quatre chiffres codant le type de handicap ou de déficience de l'élève, ce qui permet d'identifier la nature de l'affection ou du handicap dont il souffre, est une donnée relative à la santé au sens de l'article 8 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Tel n'est pas le cas, en revanche, de la structure de soins qui l'accueille, celle-ci ne permettant que dans de très rares cas, où sa dénomination est explicite, d'identifier directement la pathologie de l'élève.

CE, 10ème/9ème SSR, 19 juillet 2010, M. A et Mme B, n° 317182, Rec., point 18

Code d'identification d'un établissement scolaire accueillant des enfants handicapés – Absence

Les codes d'identification propres aux établissements dans lesquels sont scolarisés les enfants, y compris dans les cas où l'enfant est scolarisé dans une structure hospitalière ou dans un établissement de santé, permettent de savoir que l'élève a été souffrant mais ne fournissent par eux-mêmes aucune information sur la nature, la durée ou la gravité de l'affection de l'élève, information qui ne peut être obtenue qu'en accédant à un autre fichier mettant en correspondance les codes et la dénomination de l'établissement. Ce n'est que dans de très rares cas que la dénomination de l'établissement est explicite quant à la nature des pathologies qu'il soigne. Par conséquent, ces données ne sont pas relatives à la santé au sens de l'article 8 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés.

CE, 10ème/9ème SSR, 19 juillet 2010, M. F et Mme C, n° 334014, T., point 10

Traitement impliquant nécessairement des données de santé – Information explicite de l'utilisateur – Obligation

Lorsque le service demandé par l'utilisateur implique nécessairement le traitement de données de santé, il est cependant nécessaire que l'utilisateur ait pleinement conscience de ce que ses données de santé seront traitées et parfois conservés par le responsable de traitement, ce qui implique en principe une information explicite sur ce point lors du recueil du consentement.

CNIL, FR, 11 mai 2023, Sanction, Société X, n°SAN-2023-006, publié, point 56

Données concernant la santé

Droit d'accès aux documents administratifs - Communication à un tiers d'un registre de contention et d'isolement avec occultation des éléments permettant d'identifier les patients et les soignants, mais sans occultation des identifiants " anonymisés " des patients – Atteinte à la protection de la vie privée et du secret médical – Illicéité

Demande de communication d'un registre de contentieux et d'isolement au titre du droit d'accès aux documents administratifs. Dans le cas où l'identité des patients a fait l'objet d'une pseudonymisation, laquelle ne permet l'identification des personnes en cause qu'après recoupement d'informations, il appartient au juge administratif d'apprécier si, eu égard à la sensibilité des informations en cause et aux efforts nécessaires pour identifier les personnes concernées, leur communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. En l'espèce, compte tenu de la nature des informations en cause, qui touchent à la santé mentale des patients, et du nombre restreint

de personnes pouvant faire l'objet d'une mesure de contention et d'isolement, facilitant ainsi leur identification, alors au demeurant que les autorités énumérées à la dernière phrase du deuxième alinéa de l'article L. 3222-5-1 du code de la santé publique peuvent accéder à l'ensemble des informations figurant sur les registres et contrôler l'activité des établissements concernés, l'identifiant dit " anonymisé " figurant dans ces registres, qu'il s'agisse, selon la pratique du centre hospitalier, de " l'identifiant permanent du patient " (IPP) ou d'un identifiant spécialement défini, doit être regardé comme une information dont la communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. Cet identifiant n'est donc communicable qu'au seul intéressé en vertu des dispositions de l'article L. 311-6 du code des relations entre le public et l'administration.

CE, 10ème chambre, 22 mars 2024, Centre hospitalier Le Vinatier, n°471369, Inédit, point 6

Données concernant la vie sexuelle

Données relatives au choix d'un abonné d'un service de télévision de recevoir certains programmes – Exclusion

Les données relatives au choix d'un abonné d'un service de télévision de recevoir des programmes définis comme « œuvres cinématographiques interdites aux mineurs de moins de dix-huit ans ainsi que les programmes pornographiques ou de très grande violence, réservés à un public adulte averti et susceptibles de nuire à l'épanouissement physique, mental ou moral des mineurs de moins de dix-huit ans » ne peuvent être regardées comme étant relatives à la vie sexuelle des personnes concernées ou comme étant de nature à faire apparaître, même indirectement, leurs mœurs au sens des dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

CE, 5ème/4ème SSR, 17 mai 2006, Association Comité télévision et libertés et autres, n° 263081, Inédit., point 9

1.3.4 Données relatives aux infractions, aux condamnations pénales et aux mesures de sécurité

1) Notion – Donnée relative aux infractions de nature pénale – Notion autonome du droit de l'Union européenne – 2) Données relatives à des points de pénalité infligés à la suite d'un manquement à la réglementation routière – Inclusion

1) Afin de déterminer si l'accès aux données à caractère personnel relatives aux infractions routières, telles que les points de pénalité imposés aux conducteurs de véhicules qui ont commis une infraction routière et auxquels une sanction, pécuniaire ou autre, a été infligée, constitue un traitement de données à caractère personnel relatives à des « infractions », qui jouissent d'une protection accrue, la Cour juge que cette notion renvoie exclusivement aux infractions pénales. Toutefois, le fait que, dans le système juridique d'un État membre, les infractions routières sont qualifiées d'administratives n'est pas déterminant pour apprécier si ces infractions relèvent de la notion d'« infraction pénale » dans la mesure où il s'agit d'une notion autonome du droit de l'Union qui requiert, dans toute l'Union, une interprétation autonome et uniforme.

2) Ainsi, après avoir rappelé les trois critères pertinents pour apprécier le caractère pénal d'une infraction, à savoir la qualification juridique de l'infraction en droit interne, la nature de l'infraction et le degré de sévérité de la sanction encourue, la Cour juge que les infractions routières en cause relèvent de la notion d'« infraction » au sens du RGPD. S'agissant des deux premiers critères, la Cour

constate que, même si les infractions ne sont pas qualifiées de « pénales » en droit national, un tel caractère peut découler de la nature de l'infraction, et notamment de la finalité répressive poursuivie par la sanction que l'infraction est susceptible d'entraîner. Or, en l'espèce, l'attribution de points de pénalité pour des infractions routières, tout comme les autres sanctions que leur commission peut entraîner, poursuivent, entre autres, une telle finalité répressive. Quant au troisième critère, la Cour observe que seules des infractions routières d'une certaine gravité comportent l'imposition de points de pénalité, et que, partant, celles-ci sont susceptibles d'entraîner des sanctions d'une certaine sévérité. De plus, l'imposition de tels points se rajoute généralement à la sanction infligée, et la cumulation de ces points entraîne des conséquences juridiques pouvant même aller jusqu'à l'interdiction de conduire.

CJUE, grande chambre, 22 juin 2021, Latvijas Republikas Saeima, C-439/19, points 54-94

Données collectées dans le seul but d'assurer la sécurité des manifestations sportives – Exclusion

Seuls relèvent du champ de l'article 25 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans sa rédaction applicable (dispositions abrogées) et sont par conséquent soumis au régime d'autorisation prévu par cet article mais au régime de déclaration de l'article 22 (dispositions abrogées), les données collectées dans le but d'établir l'existence ou de prévenir la commission d'infractions.

Par conséquent, n'en relèvent pas les traitements créés par le décret du 28 décembre 2016, qui sont, ainsi que le prévoit le 2° de l'article R. 332-15 du code du sport créé par ce dernier, relatives à des manquements « aux dispositions des conditions générales de vente ou du règlement intérieur concernant la sécurité des manifestations sportives », qui exploitent des données collectées dans le seul but d'assurer la sécurité des manifestations sportives en permettant aux organisateurs de telles manifestations d'empêcher certaines personnes d'accéder à leurs enceintes sportives, en raison de comportements dangereux correspondant à des manquements à des obligations de nature contractuelle, quand bien même certains faits ou comportements susceptibles d'être enregistrés dans ces traitements sont pénalement réprimés.

CE, 10ème–9ème chambres réunies, 6 avril 2018, Association nationale des supporters et autres, n°406664, T., point 6

---

1) Champ d'application – Données collectées dans le but d'établir ou de prévenir une infraction – Inclusion – 2) Possibilité pour les victimes d'infractions de traiter ces données – Existence

Limitation des autorités susceptibles de mettre en œuvre des traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté par l'article 9 de la loi n° 78-17 du 6 janvier 1978.

1) Doivent être regardées comme entrant dans le champ d'application de cet article, non seulement les données relatives aux infractions, condamnations ou mesures de sûreté elles-mêmes, mais également les données qui, en raison des finalités du traitement automatisé, ne sont collectées que dans le but d'établir l'existence ou de prévenir la commission d'infractions, y compris par des tiers.

2) En revanche, ces dispositions ne font pas obstacle à la mise en œuvre de traitements de données à caractère personnel relatives à des infractions par les personnes qui en ont été victimes ou sont susceptibles de l'être.

CE, 10ème/9ème SSR, 11 mai 2015, Société Renault Trucks, n° 375669, Rec., point 6

1.3.5 Notion de traitement

Traitement

Communication orale de données à caractère personnel – Traitement de connées à caractère personnel – Inclusion si ces données sont contenues dans un fichier.

L'article 2, paragraphe 1, et l'article 4, point 2, du règlement général sur la protection des données, doivent être interprétés en ce sens que la communication orale d'informations relatives à d'éventuelles condamnations pénales en cours ou déjà purgées dont une personne physique a fait l'objet constitue un traitement de données à caractère personnel, au sens de l'article 4, point 2, de ce règlement, qui relève du champ d'application matériel de ce règlement dès lors que ces informations sont contenues ou appelées à figurer dans un fichier.

CJUE, 7 mars 2024, Endemol Shine Finland, C-740/22, point 59

Enregistrement vidéo publié sur internet et que les utilisateurs peuvent envoyer, regarder et partager – Inclusion

L'article 3 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 doit être interprété en ce sens que relèvent du champ d'application de cette directive l'enregistrement vidéo de membres de la police dans un commissariat, lors d'une prise de déposition, et la publication de la vidéo ainsi enregistrée sur un site internet de vidéos sur lequel les utilisateurs peuvent envoyer, regarder et partager celles-ci.

CJUE, 14 février 2019, Buivids, C-345/17

Registre des sociétés– Inclusion

En transcrivant et en conservant les indications relatives à l'identité des personnes qui, en tant que membres d'organe légalement prévu ou membres de tel organe, ont le pouvoir d'engager la société concernée à l'égard des tiers et de la représenter en justice ou participent à l'administration, à la surveillance ou au contrôle de cette société dans le registre et en communiquant celles-ci, le cas échéant, sur demande à des tiers, l'autorité chargée de la tenue de ce registre effectue un « traitement de données à caractère personnel », pour lequel elle est le « responsable », au sens des définitions fournies à l'article 2, sous b) et d), de la directive 95/46.

CJUE, 9 mars 2017, Manni, C-398/15, point 35

Surveillance par enregistrement vidéo stocké dans un disque dur – Inclusion

Une surveillance effectuée par un enregistrement vidéo des personnes, stocké dans un dispositif d'enregistrement continu, à savoir un disque dur, constitue, conformément à l'article 3, paragraphe 1, de la directive 95/46, un traitement de données à caractère personnel automatisé.

CJUE,11 décembre 2014, Ryneš, C-212/13, point 25

Collecte, publication, cession ou traitement dans un service de SMS des documents publics d'une administration fiscale contenant des données relatives aux revenus du travail et du capital et au patrimoine de personne physiques – Inclusion

Constitue un traitement de données à caractère personnel relevant du champ de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 l'activité consistant à :

- collecter dans les documents publics de l'administration fiscale des données relatives aux revenus du travail et du capital ainsi qu'au patrimoine de personnes physiques et à les traiter en vue de leur publication, y compris lorsque ces documents ne contiennent que des informations préalablement publiées dans les médias,
- les publier dans l'ordre alphabétique et par classe de revenus, sous la forme de listes détaillées établies commune par commune,
- les céder sous la forme de disques CD-ROM, pour qu'elles soient utilisées à des fins commerciales,
- les traiter dans un service de SMS qui permet aux utilisateurs de téléphones mobiles, en envoyant le nom et la commune de résidence d'une personne, de recevoir des informations concernant les revenus du travail et du capital ainsi que le patrimoine de cette personne.

CJUE, grande chambre, 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, point 37

Publication sur un site internet de données à caractère personnel – Inclusion

La seule publication sur un site internet de données à caractère personnel constitue un traitement de ces données au sens des règles nationales et européennes.

CE, 10ème–9ème chambres réunies, 10 juin 2021, M. B... A...-C..., n° 431875, T., point 3

Dispositif de surveillance par drone transmettant, après floutage, des images au centre de commandement de la préfecture de police pour un visionnage en temps réel – Traitement de données à caractère personnel au sens de la directive (UE) 2016/680 – Existence, sans qu'ait d'incidence la circonstance que seules les images floutées parviennent au centre de commandement

Il résulte de l'article 3 de la directive (UE) 2016/680 du 27 avril 2016 qu'un dispositif de surveillance qui consiste à collecter des données, grâce à la captation d'images par drone, afin de les transmettre, après application d'un procédé de floutage, au centre de commandement de la préfecture de police pour un visionnage en temps réel, constitue un traitement au sens de cette directive. Si ce dispositif permet de ne renvoyer à la direction opérationnelle que des images ayant fait l'objet d'un floutage, il ne constitue que l'une des opérations d'un traitement d'ensemble des données, qui va de la collecte des images par le drone à leur envoi vers la salle de commandement, après transmission des flux vers le serveur de floutage, décomposition de ces flux image par image aux fins d'identifier celles qui correspondent à des données à caractère personnel pour procéder à l'opération de floutage, puis à la recomposition du flux vidéo comportant les éléments floutés. Dès lors que les images collectées par les appareils sont susceptibles de comporter des données identifiantes, la circonstance que seules les données traitées par le logiciel de floutage parviennent au centre de commandement n'est pas de nature à modifier la nature des données faisant l'objet du traitement, qui doivent être regardées comme des données à caractère personnel.

CE, 10ème–9ème chambres réunies, 22 décembre 2020, La Quadrature du Net, n°446155, T., points 6-7

Traitement de données à caractère personnel (art.2 de la loi du 6 janvier 1978) – Mise en relation de traitements existants en vue de leur utilisation au regard de la finalité poursuivie par l'un d'entre eux ou d'une finalité propre – 1) Inclusion – 2) Cadre juridique applicable dépendant de la finalité poursuivie

1) Une mise en relation de deux traitements existants qui consiste à rapprocher des données conservées dans l'un et l'autre en vue de leur utilisation au regard de la finalité poursuivie par l'un d'entre eux ou d'une finalité propre constitue en elle-même un traitement au sens de l'article 2 de la loi n°78-17 du 6 janvier 1978.

2) Le cadre juridique applicable à un tel traitement dépend de la finalité ainsi poursuivie.

CE, 10ème–9ème chambres réunies, 27 mars 2020, Cercle de réflexion et de proposition d'actions sur la psychiatrie, n°431350, T., point 9

Utilisation de témoins de connexion (« cookies ») répondant aux caractéristiques définies au II de l'article 32 de la loi du 6 janvier 1978 – Inclusion

L'utilisation de « cookies » répondant aux caractéristiques définies au II de l'article 32 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés constitue un traitement de données qui doit respecter les prescriptions de l'article 6 de cette même loi.

CE, 10ème–9ème chambres réunies, 6 juin 2018, Société Editions Croque Futur, n° 412589, Rec., point 11

Traitement automatisé

Activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et à les mettre à disposition des internautes selon un ordre de préférence donné – Traitement de données à caractère personnel – Inclusion

L'article 2, sous b), de la directive 95/46, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doit être interprété en ce sens que, d'une part, l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de traitement de données à caractère personnel lorsque ces informations contiennent des données à caractère personnel.

Par ailleurs, l'exploitant d'un moteur de recherche doit être considéré comme le responsable dudit traitement des données à caractère personnel au sens dudit article 2, sous d), de ladite directive. En effet, dans la mesure où l'activité d'un moteur de recherche est susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites web les droits fondamentaux de la vie privée et de la protection des données à caractère personnel, l'exploitant de ce moteur en tant que personne qui détermine les finalités et les moyens de cette activité doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que celle-ci satisfait aux exigences de la

directive 95/46 pour que les garanties prévues par celle-ci puissent développer leur plein effet et qu'une protection efficace et complète des personnes concernées, notamment de leur droit au respect de leur vie privée, puisse effectivement être réalisée.

CJUE, 13 mai 2014, Google Spain et Google, C-131/12, points 29, 30, 38, 41

Référence, sur une page Internet, à diverses personnes identifiées par leur nom ou d'autres moyens – Inclusion

L'opération consistant à faire référence, sur une page Internet, à diverses personnes, à les identifier soit par leur nom, soit par d'autres moyens (numéro de téléphone ou informations relatives à leurs conditions de travail et à leurs loisirs) constitue un « traitement de données à caractère personnel, automatisé en tout ou en partie » au sens de la directive 95/46.

CJUE, 6 novembre 2003, Lindqvist, C-101/01, point 27

Traitement ultérieur

1) Aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire. Toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées.

L'article 25 du projet de loi ne permet la consultation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire que pour des finalités déterminées. Il s'agit, en premier lieu, « des décisions de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux ». En pareil cas, la consultation a pour but exclusif de vérifier que le comportement des intéressés n'est pas incompatible avec l'exercice des fonctions ou missions envisagées Elle s'effectue dans la stricte mesure exigée par la protection de la sécurité des personnes et par la défense des intérêts fondamentaux de la Nation. Elle donne lieu à information des intéressés. Un décret en Conseil d'Etat doit fixer la liste des enquêtes administratives qui, en application de l'article 25 de la loi déférée, pourront donner lieu à la consultation des traitements automatisés d'informations personnelles mentionnés à son article 21. La consultation est également prévue « pour l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de

renouvellement des titres relatifs à l'entrée et au séjour des étrangers ainsi que pour la nomination et la promotion dans les ordres nationaux ». En pareil cas, la consultation est faite par des agents de la police et de la gendarmerie spécialement habilités à cet effet ou, dans des conditions déterminées par décret en Conseil d'Etat, par des personnels investis de missions de police administrative désignés selon les mêmes procédures. La consultation est enfin permise pour « l'exercice de missions ou d'interventions lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et des biens, ainsi qu'au titre des mesures de protection ou de défense prises dans les secteurs de sécurité des installations prioritaires de défense visés à l'article 17 de l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense ». En pareil cas, la consultation est effectuée par des agents de la police et de la gendarmerie nationale spécialement habilités à cet effet.

Eu égard aux motifs qu'elle fixe pour ces consultations, comme aux restrictions et précautions dont elle les assortit, la loi pour la sécurité intérieure ne méconnaît par elle-même aucune de ces exigences constitutionnelles.

2) L'ensemble des garanties prévues par les articles 21 à 23 de la loi pour la sécurité intérieure, ainsi que celles de la loi du 6 janvier 1978, qui, comme il ressort des débats parlementaires, s'appliqueront aux traitements automatisés de données nominatives mis en oeuvre par les services de la police nationale et de la gendarmerie nationale dans le cadre de leurs missions, sont de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée.

CC, 13 mars 2003, Loi pour la sécurité intérieure, 2003-467 DC

1.3.6 Anonymisation

Conditions d'anonymisation d'une donnée à caractère personnel

Il résulte de la définition de la donnée personnelle donnée par les dispositions de l'article 2 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans sa version applicable au litige, qu'une telle donnée ne peut être regardée comme rendue anonyme que lorsque l'identification de la personne concernée, directement ou indirectement, devient impossible que ce soit par le responsable du traitement ou par un tiers. Tel n'est pas le cas lorsqu'il demeure possible d'individualiser une personne ou de relier entre elles des données résultant de deux enregistrements qui la concernent.

CE, 10ème–9ème chambres réunies, 8 février 2017, Société JCDecaux France, n° 393714, T., point 7

Mesures permettant d'assurer une anonymisation effective

Constitue une mesure de nature à ne plus permettre la réidentification des personnes la mise en place d'une procédure d'anonymisation automatique des données clients à l'issue de la période d'archivage intermédiaire, par laquelle les données – nom, prénom, numéro de téléphone, adresse électronique, adresse postale et coordonnées bancaires – sont remplacées par des données non identifiantes qui correspondent à une série de « X », d'autres données sont supprimées, et ne sont conservées que les données clients correspondant à la civilité, au code postal et à la ville. Ces dernières données, seules ou en lien avec d'autres données accessibles par le responsable de traitement ou des tiers, ne permettent pas, en l'espèce, de réidentifier la personne concernée.

CNIL, FR, 23 juin 2022, Clôture d'injonction, Société X, n° SAN-2022-012, non publié

Distinction anonymisation et pseudonymisation – Sens restrictif du terme anonymisation pour le RGPD

Il y a lieu, lorsque des dispositions législatives ou réglementaires font référence à la notion d'anonymisation, de rechercher quelle est l'intention de l'auteur du texte pour comprendre la portée de ses exigences, et notamment si les dispositions en cause exigent une anonymisation au sens du RGPD ou une pseudonymisation, par occultation des données directement identifiantes. La Commission invite le législateur et le pouvoir réglementaire à tenir systématiquement compte de la distinction posée par le RGPD et à employer le mot d'anonymisation dans le seul sens restrictif que lui donne le RGPD.

CNIL, SP, 11 juin 2020, Avis sur projet de décret, n° 2020-062, non publié

1.3.7 Acteurs du traitement

Responsable du traitement

Accès aux données personnelles et consignes écrites relatives aux traitements – Conditions non nécessaires pour retenir la responsabilité

L'article 2, sous d), de la directive 95/46/CE, lu à la lumière de l'article 10, paragraphe 1, de la Charte des droits fondamentaux, doit être interprété en ce sens qu'il permet de considérer une communauté religieuse comme étant responsable, conjointement avec ses membres prédicateurs, des traitements de données à caractère personnel effectués par ces derniers dans le cadre d'une activité de prédication de porte-à-porte organisée, coordonnée et encouragée par cette communauté, sans qu'il soit nécessaire que ladite communauté ait accès aux données ni qu'il doive être établi qu'elle a donné à ses membres des lignes directrices écrites ou des consignes relativement à ces traitements.

CJUE, grande chambre, 10 juillet 2018, Jehovan Todistajat, C-25/17

La notion de « responsable du traitement » au sens de la directive 95/46/CE du 24 octobre 1995 englobe l'administrateur d'une page fan hébergée sur un réseau social.

Une société offrant des services par l'intermédiaire d'une page fan hébergée sur Facebook peut obtenir des données statistiques anonymes sur les visiteurs de ces pages, à l'aide d'une fonction « Facebook Insight » mise gratuitement à sa disposition par Facebook, selon des conditions d'utilisation non modifiables. Ces données sont collectées grâce à des cookies comportant chacun un code utilisateur unique, actifs pendant 2 ans et sauvegardés par Facebook sur le disque dur de l'utilisateur des visiteurs. Ce code peut être mis en relation avec les données de connexion des utilisateurs enregistrés sur Facebook et être collecté et traité au moment de l'ouverture des pages fans.

Si la Cour relève que le réseau social et sa filiale irlandaise doivent être regardés comme responsables du traitement des données à caractère personnel des utilisateurs ainsi que des personnes ayant visité les pages fan hébergées, elle considère que l'administrateur de cette page, eu égard à ces caractéristiques, doit être regardé comme conjointement responsable de ces données.

Pour qualifier l'administrateur de responsable de traitement, la Cour relève qu'il participe, par son action de paramétrage, en fonction d'une audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page. En particulier, l'administrateur peut demander l'obtention, et, par construction, le traitement :

- de données démographiques concernant son audience cible (tendances en matière d'âge, de sexe, de situation amoureuse et de profession) ;
- d'informations sur le style de vie et les centres d'intérêt de cette audience (informations sur les achats et le comportement d'achat en ligne ainsi que sur les catégories de produits ou de services qui l'intéressent le plus) ;
- de données géographiques lui permettant d'effectuer des promotions spéciales ou organiser des événements et de cibler son offre d'informations.

En outre, les pages fan peuvent être visitées par des personnes qui ne sont pas utilisateurs de Facebook. Dans ce cas, la responsabilité de l'administrateur est encore plus marquée puisque la simple consultation de sa page déclenche le traitement de ses données à caractère personnel.

Enfin, si les données ne sont transmises à l'administrateur que sous une forme anonymisée, l'établissement de ces statistiques repose sur la collecte préalable de données personnelles. Or, la directive n'exige pas, lorsqu'il y a une responsabilité conjointe de plusieurs opérateurs, que chacun ait accès aux données à caractère personnel concernées.

Dès lors, l'administrateur de la page ne saurait s'exonérer du respect de ses obligations en matière de protection des données, quand bien même il utiliserait la plateforme mise en place par Facebook.

En revanche, la reconnaissance d'une responsabilité conjointe ne se traduit pas par une responsabilité équivalente. Le niveau de responsabilité de chacun doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce.

CJUE, grande chambre, 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, points 25-44

Caméras individuelles des agents de la police municipale – Traitement pour le compte de l'État au sens de l'article 31 de la loi Informatique et Libertés – Existence – Responsabilité de traitement du ministre de l'intérieur – Absence

À l'occasion de l'examen d'un projet de décret relatif à la mise en œuvre de traitements de données à caractère personnel provenant des caméras individuelles des agents de la police municipale, le Conseil d'État (section de l'intérieur) estime qu'il résulte tant des finalités poursuivies par les dispositifs en cause que des missions confiées aux agents de police municipale, que les traitements projetés relèvent des dispositions de la directive (UE) n° 2016/680 du 27 avril 2016 telle que transposée aux articles 70-1 et suivants de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Compte tenu de leurs finalités ils doivent être regardés comme mis en œuvre pour le compte de l'État au sens de l'article 31 de la loi « Informatique et libertés ». Le traitement étant mis en œuvre au niveau des collectivités locales ou des établissements de coopérations intercommunales, le ministre de l'intérieur ne peut être regardé comme le responsable du traitement au sens du premier alinéa de l'article 70-4, alors même que cette mise en œuvre est faite pour le compte de l'État.

CE, Section de l'intérieur, 8 janvier 2019, Avis n° 396340, Projet de décret relatif à la mise en œuvre de traitements provenant des caméras individuelles des agents de la police municipale

Traitement de données consistant en l'utilisation de témoins de connexion (« cookies ») répondant aux caractéristiques définies au II de l'article 32 de la loi du 6 janvier 1978 – 1) « Cookies » déposés par l'éditeur du site ou mis en place pour son compte par un sous-traitant – Responsable de traitement – Éditeur du site – 2) a) « Cookies » déposés par des tiers – Responsables de traitement – b) Cookies déposés par des tiers autorisés par l'éditeur du site – Responsables de traitement – Tiers et éditeur du site – Obligations pesant sur l'éditeur du site

1) Lorsque des « cookies » sont déposés par l'éditeur du site, il doit être considéré comme responsable de traitement au sens de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés. Il en va de même lorsque l'éditeur sous-traite à des tiers la gestion de cookies mis en place pour son compte.

2) a) Les autres tiers qui déposent des cookies à l'occasion de la visite du site d'un éditeur doivent être considérés comme responsables de traitement.

b) Toutefois, les éditeurs de site qui autorisent le dépôt et l'utilisation de tels cookies par des tiers à l'occasion de la visite de leur site doivent également être considérés comme responsables de traitement, alors même qu'ils ne sont pas soumis à l'ensemble des obligations qui s'imposent au tiers qui a émis le « cookie », notamment lorsque ce dernier conserve seul la maîtrise du respect de sa finalité ou de sa durée de conservation. Au titre des obligations qui pèsent sur l'éditeur de site dans une telle hypothèse, figurent celle de s'assurer auprès de ses partenaires qu'ils n'émettent pas, par l'intermédiaire de son site, des cookies qui ne respectent pas la règlementation applicable en France et celle d'effectuer toute démarche utile auprès d'eux pour mettre fin à des manquements.

CE, 10ème–9ème chambres réunies, 6 juin 2018, Société Éditions Croque Futur, n° 412589412589, Rec., point 11412589, Rec., point 11

1) Société déterminant la nature des données collectées, les droits d'accès des entités qui lui sont liées ainsi que la durée de conservation des données – Inclusion – 2) Entités liées ayant désigné un correspondant à la protection des données – Exclusion

Société ayant mis un traitement de données à caractère personnel à disposition des entités qui lui sont liées, décidé de la nature des données collectées et déterminé les droits d'accès à celles-ci puis, après le contrôle de la Commission nationale de l'informatique et des libertés (CNIL), ayant fixé la durée de conservation des données et apporté des correctifs à leur traitement.

Ainsi, cette société, qui détermine les finalités et les moyens du traitement, doit être regardée comme le responsable du traitement, la désignation d'un correspondant à la protection des données par les autres entités n'ayant pas, par elle-même, pour effet de rendre celles-ci responsables des traitements.

CE, 10ème/9ème SSR, 12 mars 2014, Société Foncia Groupe, n° 354629, T., point 5

Identification – Méthode du faisceau d'indices

Cas d'une filiale d'une société X qui exerce son activité sous la marque X.

Afin de déterminer si cette filiale doit être regardée comme le responsable de traitement, et non la société X, plusieurs éléments sont pris en compte : l'exploitation par ses propres soins des fichiers, pour l'exercice de sa propre activité commerciale ; la détermination effective du champ des données renseignées ; l'indication au cours de la procédure devant la CNIL de la volonté de renoncer à la collecte de différentes données ou encore

Sont sans incidence d'une part, l'indication, sous le timbre de la société X, qu'après la sanction, des instructions correctives ont été données la circonstance que d'autres filiales ou franchises utilisent lesdites données et d'autre part, l'indication au juge d'avoir accompli les nécessaires à la régularisation de l'exploitation des fichiers au regard des dispositions de la loi.

CE, 10ème/9ème SSR, 27 juillet 2012, Société AIS 2, n° 340026, T., point 7

Responsabilité du traitement dans la mise en œuvre de traitements à des fins de mesure d'audience en ligne

Une société gestionnaire du site web qui, d'une part, décide de mettre en œuvre une fonctionnalité d'un prestataire de service, laquelle conduit à traiter des données à caractère personnel, à des fins de mesure d'audience, de performance des campagnes médias de la société, d'évaluation et d'optimisation du site web (détermination de la finalité), et qui, d'autre part, a déterminé les moyens de la collecte et du traitement des données collectées dans le cadre de l'intégration de cette fonctionnalité sur son site web (détermination des moyens), est responsable de traitement au sens de l'article 4.7 du RGPD.

CNIL, P, 3 février 2022, Mise en demeure, Société X, n° MED-2022-005, non publié

Fichier de gestion de la crise sanitaire – Agences régionales de santé – Traitement de suivi des patients zéro et des cas contact

Si le décret n° 2020-551 du 12 mai 2020 modifié réglemente des traitements placés sous la responsabilité du traitement de la caisse nationale de l'assurance maladie, il se borne, s'agissant des agences régionales de santé, à autoriser la mise en œuvre d'autres traitements de données personnelles par celles-ci, pour la mise en place d'un système d'information aux fins d'enquêtes sanitaires.

Les logiciels de suivi des patients utilisés dans ce cadre le sont sous la seule responsabilité des agences régionales de santé, ces dernières devant être considérées comme responsables du traitement de suivi des patients zéro et des cas contacts qu'elle mettent en œuvre. Ce traitement est soumis aux dispositions du RGPD et de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

CNIL, P, 12 janvier 2021, Mise en demeure, Agence régionale de santé X, n° MED-2021-003, non publié

Personne mettant à disposition du public un logiciel – Exclusion sous conditions

La seule mise à disposition d'un logiciel au public, dès lors que les données à caractère personnel sont stockées et traitées uniquement localement, sur le terminal de l'utilisateur, à la discrétion et pour le seul compte de ce dernier, n'implique pas la mise en œuvre d'un traitement de données dont la responsabilité incomberait à celui qui le met à disposition.

CNIL, SP, 17 décembre 2020, Avis sur projet de décret, TousAntiCovid, n° 2020-135, publié, point 38

Concession de service public – Qualification du concessionnaire – Qualification de l'autorité publique concédante

La qualification de responsable de traitement est reconnue au concessionnaire dès lors qu'il agit pour son propre compte avec une autonomie certaine sur les traitements des données d'usagers qu'il met en œuvre dans l'exécution de ses missions, en déterminant les finalités et les moyens essentiels du traitement.

Cependant, l'autorité publique concédante est également qualifiée de responsable des traitements des données à caractère personnel des usagers mis en œuvre par le concessionnaire dans le cadre de l'exécution du service, dès lors que le traitement de ces données est nécessaire à la satisfaction des finalités poursuivies par la collectivité et que cette dernière a substantiellement défini les traitements de données en cause et leurs conditions de réalisation par le concessionnaire, notamment à travers des clauses contractuelles ou des instructions précises quant à leur mise en œuvre durant l'exécution du contrat.

CNIL, P, 24 novembre 2020, Mise en demeure, LAPI Commune X, n° MED-2020-040, non publié

Responsable conjoint

Le gestionnaire d'un site internet équipé du bouton « j'aime » de Facebook peut être regardé comme conjointement responsable avec Facebook de la collecte et de la transmission à Facebook des données à caractère personnel des visiteurs de son site. En revanche, il n'est, en principe, pas responsable du traitement ultérieur de ces données par Facebook seul.

Le gestionnaire d'un site Internet qui insère sur ledit site un module social permettant au navigateur du visiteur de ce site de solliciter des contenus du fournisseur dudit module et de transmettre à cet effet à ce fournisseur des données à caractère personnel du visiteur (bouton « j'aime » de Facebook), peut être considéré comme étant conjointement responsable du traitement, au sens de l'article 2, sous d), de la directive 95/46. Cette responsabilité est cependant limitée à l'opération ou à l'ensemble des opérations de traitement des données à caractère personnel dont il détermine effectivement les finalités et les moyens, à savoir la collecte et la communication par transmission des données en cause.

Ainsi, le gestionnaire du site insérant un bouton « j'aime » peut être considéré comme étant responsable, conjointement avec Facebook, des opérations de collecte et de communication à Facebook de ces données, dès lors qu'il peut être considéré que le gestionnaire et Facebook déterminent, conjointement, les finalités et les moyens de cette collecte et de cette transmission. En effet, l'insertion du bouton « j'aime » sur son site permet d'optimiser la publicité pour les produits en les rendant plus visibles sur le réseau social lorsqu'un visiteur clique dessus. Ce faisant, le gestionnaire du site a consenti, implicitement du moins, à la collecte et à la communication de ces données, qui s'opère dans son intérêt économique et dans celui de Facebook. Il en résulte que le coresponsable de ces opérations doit fournir certaines informations à ses visiteurs au moment de la collecte de ces données, comme son identité et les finalités du traitement :

- Lorsque le traitement repose sur le consentement, le gestionnaire du site doit recueillir le consentement au préalable pour les opérations dont il est coresponsable (collecte et transmission des données) ;
- Lorsque le traitement est nécessaire à la réalisation d'un intérêt légitime, chacun des coresponsables doivent poursuivre, avec la collecte et la transmission des données, un intérêt légitime.

CJUE, 29 juillet 2019, Fashion ID, C-40/17

Sous-traitant

Mise à disposition de plateforme en ligne pour la publication d'annonces immobilières – Sous-traitance et sous-traitance de second rang – Formalisation des relations entre responsable du traitement et sous-traitants

Un organisme de représentation professionnel qui met à disposition des entités indépendantes qu'il représente une plateforme de publication d'annonces immobilières et d'hébergement des documents annexés à ces annonces via un site web - en tant qu'activité accessoire et non réglementée de cette profession - doit être considéré comme sous-traitant de ces entités, considérées comme responsables du traitement, dès lors que ces dernières conservent dans ce cadre une entière liberté de choix quant aux moyens mis en œuvre pour exercer cette activité et publier des annonces immobilières, et dans la mesure où elles déterminent seules les finalités et les moyens du traitement.

En outre, lorsque les entités responsables du traitement confient à l'organisme sous-traitant la charge de publier leurs annonces immobilières et d'héberger les documents annexés à ces annonces sur un site web dont l'organisme sous-traitant se déclare éditeur, et lorsque que l'hébergement, l'exploitation, la maintenance et l'évolution de ce site, qui impliquent le traitement des données personnelles contenues dans les documents annexés aux annonces, ont été confiés par l'organisme sous-traitant à une autre société, cette dernière intervient dès lors en qualité de sous-traitant de second rang recruté par l'organisme sous-traitant.

Dès lors que, d'une part, aucun acte juridique ne formalise ni les relations entre les responsables du traitement de publication d'annonces immobilières et l'organisme sous-traitant, ni les relations entre l'organisme sous-traitant et la société intervenant en tant que sous-traitant de second rang, et que, d'autre part, aucune autorisation écrite préalable des responsables de traitement ne prévoit le recrutement, par l'organisme sous-traitant, de la société intervenant en tant que sous-traitant de second rang, ces faits constituent un manquement à l'article 28 du RGPD.

CNIL, P, 4 mars 2021, Mise en demeure, n° MED-2021-009, non publié

Répartition des responsabilités entre responsable de traitement et sous-traitant – Solutions techniques et organisationnelles adéquates – Responsabilité du sous-traitant – Existence

Si aux termes de l'article 32 du RGPD, les obligations en matière de sécurité des traitements de données à caractère personnel s'adressent tant au responsable de traitement qu'au sous-traitant, la répartition des responsabilités entre ces deux acteurs résulte également du contrat de sous-traitance qu'ils doivent conclure au titre de l'article 28 du RGPD. En ce sens, l'article 28-3-f impose que ce contrat prévoit que le sous-traitant « aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ». La CNIL déduit de la combinaison de ces dispositions qu'il revient au sous-traitant de proposer au responsable de traitement les solutions techniques et organisationnelles adéquates, notamment en ce qui concerne la sécurité des traitements, et ce, indépendamment des obligations qui pèsent en propre sur le responsable du traitement.

CNIL, FR, 8 janvier 2021, Sanction, Société X, n°SAN-2021-002, non publié

Destinataire et accédant

Droit d'obtenir communication des informations relatives aux « destinataires ou catégories de destinataires » – Connaissance de l'identité des agents publics ou des salariés ayant consulté les données – Exclusion

Les dispositions du c) du paragraphe 1 de l'article 15 du RGPD, qui prévoient le droit pour la personne concernée d'obtenir communication des informations relatives aux « destinataires ou catégories de destinataires » auxquels les données à caractère personnel la concernant ont été communiquées, n'ont ni pour objet, ni pour effet d'autoriser une personne à connaître l'identité des agents publics ou des salariés ayant consulté les données à caractère personnel la concernant dans l'exercice de leurs fonctions au sein de la personne morale ou du service destinataire.

CE, 10ème chambre, 24 février 2022, M. A... B..., n° 447495, Inédit., point 6

Distinction entre interconnexion et mise en relation – Inclusion des services autorisés à mettre en œuvre le traitement dans les destinataires des données du traitement – Limitation de la consultation des traitements relevant du titre II de l'article 26 de la loi Informatique et Libertés

Le Conseil d'État a donné un avis favorable à un projet de décret portant création d'un traitement automatisé de données à caractère personnel, dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD).

Le projet crée un traitement automatisé de données à caractère personnel permettant, à l'occasion de la réalisation d'enquêtes administratives sur le fondement des articles L. 114-1, L. 114-2 et L. 211-11-1 du code de la sécurité intérieure, de consulter automatiquement d'autres traitements automatisés de données à caractère personnel ou d'entrer en relation avec eux. Cette consultation peut prendre la forme d'une consultation automatique ou d'une mise en relation.

Le Conseil d'État relève que la consultation automatique d'un traitement aux fins de vérifier si l'identité d'une personne y est enregistrée, suivie de l'inscription automatique de cette information au nombre des données qui peuvent être enregistrées dans le nouveau traitement, constitue une interconnexion.

En revanche, l'interrogation, par les services autorisés à mettre en œuvre le nouveau traitement, des services autorisés à mettre en œuvre d'autres traitements, dont la réponse prend la forme d'un courriel, n'est pas une interconnexion, mais une mise en relation, alors même que le contenu de cette réponse peut consister en des données enregistrées dans ces autres traitements et pourra figurer au nombre des données enregistrées dans le nouveau traitement.

Le Conseil d'État estime que les services autorisés à mettre en œuvre le nouveau traitement doivent figurer au nombre des destinataires des données du traitement au sens des dispositions du 4° de l'article 29 de la loi n°78-17 du 6 janvier 1978, dans l'acte autorisant chacun des traitements qui fait l'objet d'une consultation automatique ou avec lequel le nouveau traitement est mis en relation. La consultation de traitements automatisés de données à caractère personnel relevant du III de l'article 26 de la même loi, qu'elle prenne la forme d'une consultation automatique ou d'une mise en relation, doit être limitée à certaines des enquêtes administratives réalisées sur le fondement de l'article L. 114 - 1. Est à cet égard légitime une consultation opérée dans le cadre d'enquêtes administratives relatives à des emplois ou activités comportant l'exercice de prérogatives de puissance publique ou pour lesquels le port d'une arme est prescrit ou autorisé, ou encore comportant des risques au regard de l'interdiction du blanchiment.

CE, Section de l'intérieur, 4 juillet 2017, Avis n° 393336, Projet de décret portant création d'un traitement automatisé dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD)

Personnes accédants au traitement ou destinataires de données de santé – Secret médical et droit d'en connaître

Dans le cadre d'un traitement mis en œuvre pour le compte de l'État et contenant des données recueillies par des professionnels de santé et couvertes par le secret médical, il revient au responsable du traitement de s'assurer que les personnes accédant au traitement ou destinataires des données qui pourraient avoir connaissance des données couvertes par le secret médical ont bien le droit d'en connaître.

Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne portée à la connaissance d'un professionnel de santé, de tout membre du personnel d'un établissement, service ou organisme concourant à la prévention ou aux soins et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. La Commission rappelle que ce secret s'impose à tous les professionnels intervenant dans le système de santé qui pourraient être amenés à transmettre des informations afin qu'elles soient enregistrées dans le traitement

CNIL, P, 21 avril 2022, Avis sur projet de décret, n° 2022-051, non publié

Notions d'accédants et de destinataires – Habilitations des accédants

Le terme « accédant », que n'utilise ni le RGPD, ni la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés mais qui a été créé par la doctrine, désigne, s'agissant d'un traitement automatisé de données mis en œuvre par une administration et encadré par un acte réglementaire, les personnes qui, au sein du responsable de traitement, seront appelées à effectuer les diverses opérations de traitement et, à ce titre, à accéder au système informatique en cause.

Les habilitations des différents accédants peuvent être définies par l'acte réglementaire, et ne se limitent généralement pas à la seule consultation des données mais incluent aussi l'enregistrement, la correction ou l'effacement des données. Par ailleurs, au sens de la réglementation, et notamment du RGPD, les « destinataires » sont les personnes à qui le responsable de traitement peut être amené à communiquer les données et sur lesquelles il doit fournir une information aux personnes concernées. En pratique, cette communication peut prendre plusieurs formes, qu'il s'agisse d'une transmission d'un extrait des données ou d'une simple faculté de consultation par un accès sécurisé au système informatique. Lorsqu'un projet de décret mentionne des personnes comme « accédants aux données » alors qu'elles ne seront pas seulement chargées de consulter les données mais également de décider de leur recueil, ce point doit être précisé pour éviter toute ambiguïté.

CNIL, P, 13 janvier 2022, Avis sur projet de décret, Caméras installées sur des aéronefs circulant sans personne à bord, n° 2022-006, publié

Voir aussi : CNIL, P, 20 janvier 2022, Avis sur projet de décret, Titre IV du livre II du code de la sécurité intérieure, n° 2022-005, publié

1.3.8 Établissement principal

Traitement transfrontalier – 1) a) Autorité de contrôle compétente – b) Conditions – 2) a) Modalités de détermination de l'autorité chef de file – Lieu de l'établissement principal – b) Administration centrale du responsable du traitement sauf compétence d'un autre établissement pour prendre les décisions relatives aux finalités et aux moyens du traitement

1) a) Il résulte clairement des 7, 16 et 23 de l'article 4 du RGPD et de ses articles 51, 55 et 56 que, lorsqu'est en cause un traitement transfrontalier de données à caractère personnel opéré au sein de l'Union européenne, l'autorité de contrôle de l'établissement principal dans l'Union du responsable

de ce traitement est en principe compétente, en tant qu'autorité chef de file, pour contrôler le respect des exigences du RGPD, b) sous réserve du cas, prévu au paragraphe 2 de l'article 56 de ce règlement, dans lequel l'objet de la réclamation concerne uniquement un établissement de l'État membre dont relève une autre autorité de contrôle ou affecte sensiblement des personnes concernées dans cet État membre uniquement.

2) a) Pour la détermination de l'autorité chef de file, l'administration centrale du responsable du traitement, c'est-à-dire le lieu de son siège réel, doit en principe être regardée comme son établissement principal.

b) Il en va autrement si un autre de ses établissements est compétent pour prendre les décisions relatives aux finalités et aux moyens du traitement et dispose du pouvoir de les faire appliquer à l'échelle de l'Union.

CE, 10ème-9ème chambres réunies, 4 mai 2023, Mme E...D..., n° 464445, T., point 4

Traitement transfrontalier – 1) Autorité de contrôle compétente – Conditions – a) Modalités de détermination de l'autorité chef de file – Lieu de l'établissement principal – b) Administration centrale du responsable du traitement sauf compétence d'un autre établissement pour prendre les décisions relatives aux finalités et aux moyens du traitement – 2) Responsable de traitement hors UE sans administration centrale et établissement doté d'un pouvoir décisionnel – Compétence de chaque autorité de contrôle nationale

1) Il résulte clairement du 7) de l'article 4 et des articles 16, 55 et 56 du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD) que lorsqu'est en cause un traitement transfrontalier de données à caractère personnel opéré au sein de l'Union européenne, l'autorité de contrôle de l'établissement principal dans l'Union du responsable de ce traitement est, en tant qu'autorité chef de file, compétente pour contrôler le respect des exigences du RGPD.

a) Pour la détermination de l'autorité de contrôle compétente, l'administration centrale du responsable du traitement, c'est-à-dire le lieu de son siège réel, doit en principe être regardée comme son établissement principal.

b) Il en va autrement si un autre de ses établissements est compétent pour prendre les décisions relatives aux finalités et aux moyens du traitement et dispose du pouvoir de les faire appliquer à l'échelle de l'Union.

2) Dans l'hypothèse où un responsable de traitement implanté en dehors de l'Union européenne met en œuvre un traitement transfrontalier sur le territoire de l'Union, mais qu'il n'y dispose ni d'administration centrale, ni d'établissement doté d'un pouvoir décisionnel quant à ses finalités et à ses moyens, le mécanisme de l'autorité chef de file prévu à l'article 56 du RGPD ne peut être mis en œuvre. Dans pareil cas, chaque autorité de contrôle nationale est compétente pour contrôler le respect du RGPD sur le territoire de l'État membre dont elle relève, conformément à l'article 55 précité.

CE, 10ème-9ème chambres réunies, 19 juin 2020, Google LLC, n° 430810, Rec., point 4

« Guichet unique » applicable aux traitements transfrontaliers (art. 56 RGPD) – 1) Champ d'application – Absence d'établissement sur le territoire d'un État membre de l'Union européenne – Exclusion – 2) Conséquence – Compétence de la CNIL pour le contrôle de la conformité au RGPD des traitements visant des personnes résidant sur le territoire national

1) Le mécanisme du « guichet unique » prévu par l'article 56 du RGPD n'a pas vocation à s'appliquer à une société ne disposant pas d'établissement sur le territoire d'un État membre de l'Union

européenne. Dès lors, chaque autorité de contrôle nationale est compétente pour contrôler le respect du RGPD sur le territoire de l'État membre dont elle relève conformément à l'article 55 du RGPD, pour les traitements visant des personnes résidant sur ce territoire.

2) La CNIL est ainsi compétente pour contrôler la conformité au RGPD des traitements mis en œuvre par tout responsable de traitement ou sous-traitant ne disposant pas d'établissement dans l'UE dont les opérations de traitement visent des personnes résidant sur le territoire français.

CNIL, FR, 10 novembre 2022, Sanction, Société X, n° SAN-2022-020, publié, point 25

1.3.9 Fichiers

Activité de prédication de porte-à-porte comportant des noms et des adresses – Données structurées selon des critères déterminés – Inclusion

L'article 2, sous c), de la directive 95/46/CE doit être interprété en ce sens que la notion de « fichier », visée par cette disposition, couvre un ensemble de données à caractère personnel collectées dans le cadre d'une activité de prédication de porte-à-porte, comportant des noms et des adresses ainsi que d'autres informations concernant les personnes démarchées, dès lors que ces données sont structurées selon des critères déterminés permettant, en pratique, de les retrouver aisément aux fins d'une utilisation ultérieure. Pour qu'un tel ensemble relève de cette notion, il n'est pas nécessaire qu'il comprenne des fiches, des listes spécifiques ou d'autres systèmes de recherche.

CJUE, grande chambre, 10 juillet 2018, Jehovan Todistajat, C-25/17

1.3.10 Représentation des personnes pour agir

Qualité pour agir – Association de défense des intérêts des consommateurs – Action représentative intentée par cette association en l'absence d'un mandat et indépendamment de la violation de droits concrets d'une personne concernée – Action fondée sur la violation des règles relatives à la protection des consommateurs ou à la lutte contre les pratiques commerciales déloyales – Admissibilité – Condition

En ouvrant la possibilité aux États membres de prévoir un mécanisme d'action représentative contre l'auteur présumé d'une atteinte à la protection des données à caractère personnel, l'article 80, paragraphe 2, du RGPD prévoit un certain nombre d'exigences à respecter.

Ainsi, premièrement, la qualité pour agir est reconnue à un organisme, à une organisation ou à une association qui remplit les critères énumérés par le RGPD. Peut relever de cette notion, une association de défense des intérêts des consommateurs qui poursuit un objectif d'intérêt public consistant à assurer les droits et les libertés des personnes concernées en leur qualité de consommateurs, dès lors que la réalisation d'un tel objectif est susceptible d'être connexe à la protection des données à caractère personnel de ces dernières.

Deuxièmement, l'exercice de ladite action représentative présuppose que l'entité en cause, indépendamment de tout mandat qui lui a été confié, considère que les droits qu'une personne concernée tire du RGPD ont été violés du fait du traitement de ses données à caractère personnel.

Ainsi, d'une part, l'exercice d'une action représentative n'exige pas l'identification individuelle préalable par l'entité en cause de la personne spécifiquement concernée par un traitement de données prétendument contraire aux dispositions du RGPD. À cette fin, la désignation d'une catégorie ou d'un groupe de personnes affectées par un tel traitement peut être également suffisante.

D'autre part, l'exercice d'une telle action n'exige pas l'existence d'une violation concrète des droits qu'une personne tire du RGPD. En effet, afin de reconnaître la qualité pour agir d'une entité, il suffit de faire valoir que le traitement de données concerné est susceptible d'affecter les droits que des personnes physiques identifiées ou identifiables tirent dudit règlement, sans qu'il soit nécessaire de prouver un préjudice réel subi par la personne concernée, dans une situation déterminée, par l'atteinte à ses droits. Ainsi, au vu de l'objectif poursuivi par le RGPD, le fait d'habiliter des associations de défense des intérêts des consommateurs, telle que l'Union fédérale, à introduire, par un mécanisme de recours représentatif, des actions visant à faire cesser des traitements contraires aux dispositions du RGPD, indépendamment de la violation des droits d'une personne individuellement et concrètement affectée par cette violation, contribue incontestablement à renforcer les droits des personnes concernées et à leur assurer un niveau élevé de protection.

La violation d'une règle relative à la protection des données à caractère personnel peut simultanément entraîner la violation de règles relatives à la protection des consommateurs ou aux pratiques commerciales déloyales. En effet, le RGPD permet aux États membres d'exercer leur faculté de prévoir que les associations de défense des intérêts des consommateurs sont habilitées à agir contre des violations des droits prévus par le RGPD par l'intermédiaire de règles ayant pour objet de protéger les consommateurs ou de lutter contre des pratiques commerciales déloyales.

CJUE, 28 avril 2022, Meta Platforms Ireland Limited, C-319/20, points 48-83

2. Règles principales

2.1 Licéité du traitement

Traitements relevant de la directive Police justice - Exigence d'une autorisation du traitement par le droit de l'Etat membre – Circonstance que la disposition légale se réfère également au RGPD - Circonstance sans incidence sur la validité de la base juridique

L'article 10, sous a), de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, lu à la lumière de l'article 52 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que le traitement de données biométriques et génétiques par les autorités de police en vue de leurs activités de recherche, à des fins de lutte contre la criminalité et de maintien de l'ordre public, est autorisé par le droit d'un État membre, au sens de l'article 10, sous a), de cette directive, dès lors que le droit de cet État membre contient une base juridique suffisamment claire et précise pour autoriser ledit traitement. Le fait que l'acte législatif national contenant une telle base juridique se réfère, par ailleurs, au règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et non à la directive 2016/680, n'est pas de nature, en lui-même, à remettre en cause l'existence d'une telle autorisation, pour autant qu'il ressort, de manière suffisamment claire, précise et dénuée d'équivoque de l'interprétation de l'ensemble des dispositions applicables du droit national que le traitement de données biométriques et génétiques en cause relève du champ d'application de cette directive, et non de ce règlement.

CJUE, 26 janvier 2023, Ministerstvo na vatreshnite raboti, C-205/21

Enregistrement dans un traitement de données à caractère personnel en l'absence de procédure contradictoire préalable – Admission

Aucune disposition législative ou réglementaire ni aucun principe n'impose que l'enregistrement, dans un traitement, de données à caractère personnel soit précédé d'une procédure contradictoire menée avec la personne dont les données sont recueillies.

CE, 10ème-9ème chambres réunies, 6 avril 2018, Association française des sociétés financières, n° 406664, T., point 4

Utilisation par un employeur d'un système de géolocalisation pour le contrôle de la durée du travail de ses salariés – Caractère excessif – Existence, sauf lorsque ce contrôle ne peut pas être fait par un autre moyen, même moins efficace

Il résulte des articles 6 de la loi n° 78-17 du 6 janvier 1978 et L. 1121-1 du code du travail que l'utilisation par un employeur d'un système de géolocalisation pour assurer le contrôle de la durée du travail de ses salariés n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, fût-il moins efficace que la géolocalisation. En dehors de cette hypothèse, la collecte et le traitement de telles données à des fins de contrôle du temps de travail doivent être regardés comme excessifs au sens du 3° de l'article 6 de la loi du 6 janvier 1978.

CE, 10ème – 9ème chambres réunies, 15 décembre 2017, Société Odeolis, n° 403776, Rec., point 7

Données à caractère personnel pouvant faire l'objet d'un traitement automatisé – Nationalité d'un demandeur de prêt bancaire – a) Donnée pertinente au sens de l'article 5 de la convention du 28 janvier 1981 – Notion – Existence – b) Donnée dont la prise en compte constitue une discrimination au sens des stipulations du traité instituant la Communauté européenne ou au sens des articles 225-1 et 225-2 du code pénal – Absence

a) Au sein d'un traitement automatisé d'informations nominatives destiné à aider à la prise des décisions d'octroi ou de refus d'un prêt en contribuant à évaluer le risque qu'une demande présente pour l'établissement prêteur et consistant à combiner dans un calcul automatisé divers critères tirés des renseignements que les auteurs de demandes fournissent sur leur situation familiale, professionnelle et bancaire, la référence à la nationalité comme l'un des éléments de pur fait d'un calcul automatisé du risque, dont la mise en œuvre n'entraîne pas le rejet d'une demande sans l'examen individuel de celle-ci, ne constitue pas une discrimination et dès lors n'entre pas dans le champ d'application de l'article 6 du traité instituant la Communauté économique européenne (traité CE) devenu, après modification, l'article 12 du traité CE.

b) Elle ne saurait davantage, en l'absence d'élément intentionnel, être regardée comme tombant sous le coup des articles 225-1 et 225-2 du code pénal.

CE, Section, 30 octobre 2001, Association française des sociétés financières, n° 204909, Rec., points 5-8

1) Disposition limitant expressément les finalités d'un traitement – Traitement mis en œuvre illicite au regard de cette disposition – Article 5-1 – a) RGPD – Compétence de la formation restreinte de la CNIL – 2) Application – Article L. 37 du code électoral

1) Les articles 5-1 a) du RGPD et 4-1° de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés, disposent que tout traitement de données à caractère personnel doit être « licite » et, d'autre part, que l'article 16 de cette loi donne compétence à la formation restreinte de la Commission nationale de l'informatique et des libertés pour sanctionner les responsables de traitement ou sous-traitants qui ne respectent pas les obligations découlant du RGPD et de la loi Informatique et Libertés.

Il en résulte que, lorsqu'une disposition limite expressément les finalités d'un traitement de données à caractère personnel, que celle-ci soit contenue dans un acte réglementaire autorisant et régissant un traitement particulier de données sur le fondement des articles 31 et suivants de la loi Informatique et Libertés ou des dispositions qui y renvoient, ou qu'elle résulte d'une disposition législative ou réglementaire spéciale limitant la ou les finalités d'un traitement ou d'une catégorie de traitement, la formation restreinte de la CNIL est compétente pour sanctionner le traitement illicite que constitue la méconnaissance de cette disposition.

2) La formation restreinte est donc compétente en l'espèce pour examiner le manquement à l'article 5-1-a) du RGPD qui résulterait, selon la rapporteure, de la méconnaissance de l'article L. 37 du code électoral prohibant l'utilisation des listes électorales, qui contiennent des données personnelles, pour des finalités commerciales.

CNIL, FR, 3 juin 2021, Sanction, Société X, n° SAN-2021-007, non publié

2.2 Loyauté du traitement

Caractérisation du délit de collecte de données à caractère personnel par un moyen déloyal dans le cadre de rapports employeur/employés - Données disponibles en accès libre sur internet – Utilisation sans rapport avec l'objet de leur mise en ligne – Collecte à l'insu des personnes concernées – Méconnaissance de l'obligation d'information des personnes et de leur droit d'opposition

Dans le cadre de rapports employeur/employés, le fait d'effectuer des recherches sur des personnes portant sur des données à caractère personnel telles qu'antécédents judiciaires, renseignements bancaires et téléphoniques, véhicules, propriétés, qualité de locataire ou de propriétaire, situation matrimoniale, santé, déplacement à l'étranger est susceptible de constituer un moyen de collecte déloyal dès lors que, issues de la capture et du recoupement d'informations diffusées sur des sites publics tels que sites web, annuaires, forums de discussion, réseaux sociaux, sites de presse régionale, de telles données ont fait l'objet d'une utilisation sans rapport avec l'objet de leur mise en ligne et ont été recueillies à l'insu des personnes concernées, ainsi privées du droit d'opposition institué par la loi informatique et libertés.

En effet, le fait que les données à caractère personnel collectées en l'espèce par le prévenu aient été pour partie en accès libre sur internet ne retire rien au caractère déloyal de cette collecte, dès lors qu'une telle collecte, de surcroît réalisée à des fins dévoyées de profilage des personnes concernées et d'investigation dans leur vie privée, à l'insu de celles-ci, ne pouvait s'effectuer sans qu'elles en soient informées.

Cass, crim., 30 avril 2024, n°23-80.962, B., points 8,10

Collecte d'adresses électroniques personnelles de personnes physiques, à leur insu, sur l'espace public d'internet – Caractère déloyal – Existence

Constitue une collecte de données nominatives le fait d'identifier des adresses électroniques et de les utiliser, même sans les enregistrer dans un fichier, pour adresser à leurs titulaires des messages électroniques.

Est déloyal le fait de recueillir, à leur insu, les adresses électroniques personnelles de personnes physiques sur l'espace public d'internet, ce procédé faisant obstacle à leur droit d'opposition.

Cass, crim., 14 mars 2006, n° 05-83.423, B., points 11-12

Obligation de collecter de manière loyale les données à caractère personnel – Méconnaissance en l'espèce

Une société qui a constitué un traitement à partir de données recueillies sur un site internet concurrent et malgré l'opposition des personnes concernées à l'utilisation de leurs données à des fins de prospection commerciale ne saurait être regardée comme ayant respecté les principes énoncés au 1° de l'article 6 de la loi n°78-17 du 6 janvier 1978, qui imposent à l'auteur d'un traitement de collecter de manière loyale les données à caractère personnel sur lesquelles porte le traitement.

CE, 10ème/9ème SSR, 9 novembre 2015, Société les Éditions Néressis, n° 384673, T., point 7

Primauté des principes du RGPD sur les intérêts économiques de l'entreprise responsable du traitement

Le RGPD rend Meta IE, en tant que responsable de traitement, directement responsable du respect des principes du règlement (licéité, loyauté et transparence du traitement de données à caractère personnel), ainsi que de toutes les obligations qui découlent de ces principes. Cette obligation prévaut même lorsque l'application effective de ces principes n'est pas aisée ou va à l'encontre des intérêts commerciaux de l'entreprise et de son modèle économique. Le responsable du traitement est également tenu de pouvoir démontrer qu'il respecte ces principes ainsi que toutes les obligations qui en découlent comme le respect des conditions spécifiques applicables à chaque base légale de traitement.

CEPD, 5 décembre 2022, Décision Art. 65, Autorité irlandaise concernant Meta Platforms Ireland Limited et sa plateforme Instagram, 4/2022, point 108

Principe de transparence et principe de loyauté – Appréciation

La transparence est une expression du principe de loyauté qui est également intrinsèquement liée au principe de responsabilité, visé à l'article 5 du RGPD.

Une considération centrale pour l'appréciation des principes de transparence et de loyauté est que les personnes concernées doivent être en mesure de déterminer à l'avance ce que l'étendue et les conséquences du traitement impliquent et ne doivent pas être prises par surprise quant aux modalités dans lesquelles leurs données personnelles ont été utilisées.

CEPD, 28 juillet 2021, Décision Art. 65, Autorité irlandaise concernant WhatsApp Ireland, 1/2021

2.3 Finalités du traitement

2.3.1 Caractère déterminé, explicite et légitime

Traitement poursuivant plusieurs finalités – Conformité

Aucune norme constitutionnelle ne s'oppose par principe à ce qu'un traitement automatisé poursuive plusieurs finalités.

CC, 2019-797 QPC,26 juillet 2019, Unicef France et autres, point 8

Collecte de données non utilisées – Manquement au principe de limitation des finalités

La collecte de données à caractère personnel issues de sites internet sans que cette collecte puisse être justifiée par un usage de ces données constitue un traitement dépourvu de finalités, en violation de l'article 5 § 1, b) du RGPD.

CNIL, P, 1er décembre 2021, Mise en demeure, Société X, n° MED-2021-131, non publié

2.3.2 Traitement ultérieur

Analyse de compatibilité des finalités

Courrier méconnaissant la finalité informative du traitement pour laquelle il a été autorisé – Incompatibilité

Un office public de l'habitat exploitant un traitement ayant pour finalité l'information de ses locataires méconnaît l'obligation de respecter les finalités pour lesquelles le traitement a été autorisé lorsqu'il adresse un courrier aux locataires qui n'est pas de nature purement informative et comporte une critique « virulente » d'une réforme en cours, appelant à la mobilisation des locataires contre ce projet.

CE, 10ème–9ème chambres réunies, 5 octobre 2020, Office public de l'habitat de Rennes Métropole-Archipel Habitat, n° 424440, Rec., point 6

Transmission de données – Condition de limitation des données transmises à celles strictement nécessaires aux destinataires pour poursuivre les finalités du traitement

Il résulte des dispositions de l'article 6 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction applicable au litige que, pour être compatible avec les finalités d'un traitement, la transmission des données à caractère personnel doit être strictement limitée à celles qui permettent aux destinataires de poursuivre les finalités du traitement. Par suite, un traitement relatif à la prévention des atteintes à la sécurité publique en marge d'événements sportifs ne peut pas légalement prévoir que les associations et fédérations sportives, qui n'exercent aucune mission relative aux finalités poursuivies, puissent être destinataires des données collectées.

CE, 10ème/9ème SSR, 21 septembre 2015, Association de défense et d'assistance juridique des intérêts des supporters, n° 389815, Inédit., points 16-17

Destinataires des données

Droit d'accès à l'information sur les destinataires et les catégories de destinataires des données – Obligation de fournir l'identité même des destinataires, sauf impossibilité ou demande abusive

Le droit d'accès de la personne concernée aux données à caractère personnel la concernant, prévu par l'article 15, paragraphe 1, sous c) du RGPD, implique, lorsque ces données ont été ou seront communiquées à des destinataires, l'obligation pour le responsable du traitement de fournir à cette personne l'identité même de ces destinataires, à moins qu'il ne soit impossible de les identifier ou que ledit responsable du traitement ne démontre que les demandes d'accès de la personne concernée sont manifestement infondées ou excessives, au sens de l'article 12, paragraphe 5, du RGPD, auxquels cas celui-ci peut indiquer à cette personne uniquement les catégories de destinataires en cause.

CJUE, 12 janvier 2023, Österreichische Post, C-154/21

Information des personnes

Transfert par une administration publique d'un État membre de données fiscales à caractère personnel en vue de leur traitement par une autre administration publique sans information de la personne – Illicéité

Les articles 10, 11 et 13 de la directive 95/46/CE du 24 octobre 1995 doivent être interprétés en ce sens qu'ils s'opposent à des mesures nationales qui permettent à une administration publique d'un État membre de transmettre des données à caractère personnel à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement, alors qu'aucune disposition législative ou réglementaire interne ne prévoit une telle transmission.

CJUE, 1er octobre 2015, Bara e.a., C-201/14

2.4 Base légale

Traitement de données concernant la santé fondé sur l'article 9, paragraphe 2, sous h) du RGPD – Double condition de licéité – Respect des exigences de l'article 9, paragraphe 2, sous h) et de l'article 6, paragraphe 1 du RGPD

L'article 9, paragraphe 2, sous h), et l'article 6, paragraphe 1, du règlement 2016/679 doivent être interprétés en ce sens qu'un traitement de données concernant la santé fondé sur cette première disposition doit, afin d'être licite, non seulement respecter les exigences découlant de celle-ci, mais aussi remplir au moins l'une des conditions de licéité énoncées à cet article 6, paragraphe 1.

CJUE, 21 décembre 2023, Krankenversicherung Nordrhein, C-667/21

Choix de la base légale de traitement – Objectif de protéger les droits et libertés des personnes physiques

Il n'y a pas de hiérarchie entre les bases légales de traitement. Toutefois, cela ne signifie pas qu'un responsable de traitement, comme Meta IE en l'espèce, dispose d'une entière discrétion dans le choix de la base légale qui se révélerait la plus adaptée à ses intérêts économiques. Le responsable du traitement ne peut se fonder sur l'une des bases légales prévues à l'article 6 du RGPD que si elle est appropriée pour le traitement envisagé. Une base légale spécifique ne sera appropriée que si elle peut répondre aux exigences fixées par le RGPD et remplir l'objectif du règlement de protéger les droits et libertés des personnes physiques, et en particulier leur droit à la protection des données. En revanche, la base légale ne sera pas appropriée si son application à un traitement spécifique va à l'encontre de l'effet utile recherché par le RGPD, par l'article 5, paragraphe 1, point a), et l'article 6 de ce même texte. Ces critères découlent du contenu du règlement et de l'interprétation favorable aux droits des personnes concernées qui doit en être donnée.

CEPD, 5 décembre 2022, Décision Art. 65, Autorité irlandaise concernant Meta Platforms Ireland Limited et sa plateforme Instagram, 4/2022, point 107

2.4.1 Consentement

Conditions générales

Circonstances dans lesquelles le consentement n'est pas libre et éclairé – 1) Case pré-cochée par le responsable de traitement – 2) Information susceptible d'induire la personne concernée en erreur – 3) Exigence d'un formulaire faisant état du refus

L'article 4, point 11, et l'article 6, paragraphe 1, sous a) (relatifs au consentement), du RGPD doivent être interprétés en ce sens qu'il appartient au responsable du traitement des données de démontrer que la personne concernée a, par un comportement actif, manifesté son consentement au traitement de ses données à caractère personnel et qu'elle a obtenu, préalablement, une information au regard de toutes les circonstances entourant ce traitement, sous une forme compréhensible et aisément accessible ainsi que formulée en des termes clairs et simples, lui permettant de déterminer facilement les conséquences de ce consentement, de sorte qu'il soit garanti que celui-ci soit donné en pleine connaissance de cause.

Un contrat relatif à la fourniture de services de télécommunications qui contient une clause selon laquelle la personne concernée a été informée et a consenti à la collecte ainsi qu'à la conservation d'une copie de son titre d'identité à des fins d'identification n'est pas de nature à démontrer que cette personne a valablement donné son consentement, au sens de ces dispositions, à cette collecte et à cette conservation, lorsque

- la case se référant à cette clause a été cochée par le responsable du traitement des données avant la signature de ce contrat, ou lorsque ;
- les stipulations contractuelles dudit contrat sont susceptibles d'induire la personne concernée en erreur quant à la possibilité de conclure le contrat en question même si elle refuse de consentir au traitement de ses données, ou lorsque ;
- le libre choix de s'opposer à cette collecte et à cette conservation est affecté indûment par ce responsable, en exigeant que la personne concernée, afin de refuser de donner son consentement, remplisse un formulaire supplémentaire faisant état de ce refus.

CJUE, 11 novembre 2020, Orange Romania, C-61/19

Cookies – Consentement de la personne concernée – Déclaration de consentement au moyen d'une case pré-cochée par défaut – Exclusion, que les informations stockées ou consultées soient des données à caractère personnel ou non

Le consentement à l'utilisation de cookies en ligne obtenu par le biais d'une case pré-cochée n'est pas valablement recueilli, sans qu'ait d'incidence la circonstance que les informations stockées ou consultées par ce biais constituent ou non des données à caractère personnel.

L'article 2, sous f), et l'article 5, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002 dite directive vie privée et communications électroniques, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lus conjointement avec l'article 2, sous h), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, ainsi qu'avec l'article 4, point 11, et l'article 6, paragraphe 1, sous a), du RGPD doivent être interprétés en ce sens que le consentement visé à ces dispositions n'est pas valablement donné lorsque le stockage d'informations ou l'accès à des informations déjà stockées dans l'équipement terminal de l'utilisateur d'un site Internet, par l'intermédiaire de cookies, est autorisé au moyen d'une case cochée par défaut que cet utilisateur doit décocher pour refuser de donner son consentement.

L'article 2, sous f), et l'article 5, paragraphe 3, de la directive 2002/58, telle que modifiée par la directive 2009/136, lus conjointement avec l'article 2, sous h), de la directive 95/46 ainsi qu'avec l'article 4, point 11, et l'article 6, paragraphe 1, sous a), du règlement 2016/679, ne doivent pas être interprétés différemment selon que les informations stockées ou consultées dans l'équipement terminal de l'utilisateur d'un site internet constituent ou non des données à caractère personnel, au sens de la directive 95/46/CE et du RGPD.

CJUE, grande chambre, 1er octobre 2019, Planet49, C-673/17

Gestionnaire d'un site internet équipé du bouton « j'aime » de Facebook – Responsabilité conjointe – Consentement uniquement recueilli par le gestionnaire et obligation d'information pesant sur lui pour le traitement dont il détermine les finalités

L'article 2, sous h), et l'article 7, sous a), de la directive 95/46/CE doivent être interprétés en ce sens que, lorsque le gestionnaire d'un site internet insère sur ledit site un module social permettant au navigateur du visiteur de ce site de solliciter des contenus du fournisseur dudit module et de transmettre à cet effet audit fournisseur des données à caractère personnel du visiteur (bouton « j'aime » de Facebook), ce site, comme le réseau social, doivent être regardés comme co-responsables du traitement consistant dans le recueil et la transmission à Facebook de données à caractère personnel des visiteurs du site. Pour que ce traitement soit licite au titre du consentement, celui-ci doit être recueilli par ce gestionnaire uniquement en ce qui concerne l'opération ou l'ensemble des opérations de traitement des données à caractère personnel dont ledit gestionnaire détermine les finalités et les moyens.

En outre, l'article 10 de cette directive doit être interprété en ce sens que, dans une telle situation, l'obligation d'information prévue par cette disposition pèse également sur ledit gestionnaire, l'information que ce dernier doit fournir à la personne concernée ne devant toutefois porter que sur l'opération ou l'ensemble des opérations de traitement des données à caractère personnel dont il détermine les finalités et les moyens.

CJUE, 29 juillet 2019, Fashion ID, C-40/17

Accord de responsabilité conjointe – Collecte du consentement pour le compte de sociétés partenaires – Obligation du responsable de traitement ne collectant pas le consentement d'être en mesure de démontrer que la personne concernée a donné son consentement

En cas de responsabilité conjointe, l'article 26 du RGPD oblige les responsables de traitement conjoints à s'assurer, par le biais d'un accord, qu'ils respectent mutuellement le RGPD et notamment qu'ils organisent entre eux la meilleure façon de répondre aux droits des personnes concernées, en fonction de la nature du traitement et de leur responsabilité respective vis-à-vis de ce traitement.

En l'espèce, le fait que la collecte du consentement des internautes pour la mise en œuvre du traitement en cause revenait aux partenaires de la société mise en cause n'exonérait pas cette dernière de son obligation, en application de l'article 7 du RGPD, d'être en mesure de démontrer que la personne concernée avait donné son consentement et de procéder à certaines vérifications à cette fin. En effet, la seule clause issue de conditions générales d'utilisation aux termes desquelles la société exigeait de ses partenaires, « lorsque la loi le prévoit », que la politique de confidentialité de leur site inclue « des mentions et des mécanismes de choix conformes aux lois et réglementations applicables » ne permettait pas de garantir l'existence d'un consentement valide et il convenait à tout le moins qu'elle soit complétée pour préciser que l'organisme qui recueille le consentement doit mettre à disposition de l'autre partie la preuve du consentement.

CNIL, FR, 15 juin 2023, Sanction, Société X, n°SAN-2023-009, publié, points 52, 61, 74

Recueil du consentement à des fins de prospection commerciale par voie électronique – Courtiers en données en charge de la collecte du consentement – Mesures mises en place par les prospecteurs pour s'assurer de la validité du consentement donné par les prospects – Insuffisance en l'espèce

Lorsque des courtiers en données sont en charge de la collecte du consentement aux fins de prospection commerciale pour le compte d'un responsable de traitement, un simple engagement

contractuel desdits courtiers visant à « respecter le RGPD et les règles applicables en matière de prospection commerciale » n'est pas une mesure suffisante pour s'assurer que le consentement a été valablement donné par les prospects avant d'être démarchés lorsqu'un tel engagement ne se double pas d'un contrôle des formulaires de recueil utilisés ou d'audits portant sur les sociétés partenaires mobilisées. Une telle insuffisance est susceptible de constituer un manquement du responsable du traitement aux obligations résultant des articles L. 34-5 du code des postes et des communications électroniques et 7, paragraphe 1, du RGPD, tel qu'éclairé par les dispositions de l'article 4, paragraphe 11 de ce même règlement.

CNIL, FR, 24 novembre 2022, Sanction, Société X, n° SAN-2022-021, publié, points 25-27

Recueil du consentement pour la revente de données – Consentement distinct de celui donné pour l'utilisation des données à des fins de prospection commerciale par voie électronique

Pour vendre les données à des partenaires en vue qu'ils les utilisent pour de la prospection commerciale par voie électronique, un responsable du traitement doit recueillir, sur le support de collecte des données, le consentement libre, spécifique, informé et univoque par lequel les personnes concernées acceptent, par une déclaration ou un acte positif clair, une telle transmission de leurs données.

Le consentement à la revente des données ne dispense pas que le consentement des personnes soit également recueilli, en application de l'article L. 34-5 du code des postes et des communications électroniques, pour l'utilisation de leurs données à des fins de prospection commerciale par voie électronique. Ce consentement à la réception de prospection peut soit être recueilli par les opérateurs ayant acheté ou reçu les données et qui les utiliseront concrètement pour envoyer des messages de prospection, soit par le primo-collectant qui souhaite les transmettre à des partenaires. Dans ce dernier cas, ce consentement peut alors être recueilli globalement pour la transmission et la prospection commerciale, mais cela implique que le primo-collectant puisse fournir la liste exhaustive des partenaires ainsi autorisés, comme responsables de traitement, à utiliser les données pour de la prospection électronique.

CNIL, P, 1er décembre 2021, Mise en demeure, Société X, n° MED-2021-131, non publié

Voir aussi : CNIL, SP, 23 septembre 2021, Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales, n°2021-131, publié

Liberté

Système d'identification électronique – Reconnaissance faciale – Conditions de liberté du consentement – Recours au traitement exigé par sa finalité et absence de préjudice en cas de refus de consentement – Légalité du décret en l'espèce

Dans le cadre d'un système d'identification électronique auprès d'organismes publics ou privés, pour apprécier si le consentement à un traitement de données biométriques est libre, il y a lieu de vérifier si le recours à ce traitement est exigé par sa finalité et si l'usager est susceptible de subir un préjudice en l'absence de consentement.

En l'espèce, il ne ressort pas des pièces du dossier qu'il existait, à la date du décret attaqué, d'alternative à la reconnaissance faciale pour authentifier, avec le même niveau de garantie au regard du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014, l'identité d'une personne de manière entièrement dématérialisée. Les usagers refusant de recourir à

l'application Alicem ne subissent pas de préjudice au sens du RGPD dans la mesure où ils peuvent accéder à l'ensemble des téléservices accessibles par le biais de cette application, à travers un identifiant unique, grâce au dispositif FranceConnect, dont l'utilisation ne présuppose pas le consentement à un traitement de reconnaissance faciale. Le décret du 13 mai 2019 a donc pu légalement autoriser le ministre de l'intérieur à mettre en œuvre un traitement d'identification en ligne s'appuyant une application mobile, dont l'usage est conditionné au consentement au recours à un système de reconnaissance faciale.

CE, 10ème–9ème chambres réunies, 4 novembre 2020, La Quadrature du Net, n°432656, Inédit., points 6-10

Conditions de liberté du consentement – Véritable liberté de choix – Possibilité de refuser ou de retirer le consentement sans préjudice – Absence de méconnaissance en l'espèce

Saisi d'un projet de décret autorisant la création d'un moyen d'identification électronique dénommé « Application de Lecture de l'Identité d'un Citoyen En Mobilité », le Conseil d'État (section de l'intérieur) lui donne un avis favorable.

Ce traitement permet aux titulaires d'un passeport comportant un composant électronique, ou d'un titre de séjour comportant un composant électronique, de s'authentifier auprès d'organismes publics ou privés, au moyen d'un équipement terminal de communications électroniques doté d'un dispositif permettant la lecture sans contact du composant électronique de ces titres.

L'article 9 du RGPD interdit le traitement des données biométriques aux fins d'identifier une personne physique de manière unique, sauf si l'intéressé a donné son consentement. Ces dispositions sont éclairées par son considérant 42 selon lequel « le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ».

Le Conseil d'État considère que ces dispositions ne sont pas méconnues par le projet dès lors que le recours à ALICEM pour s'authentifier auprès d'organismes publics ou privés est une faculté, les usagers ou clients ayant la possibilité de recourir à d'autres dispositifs d'authentification électronique ou d'entrer en contact avec ces organismes par des voies autres qu'électroniques. Le projet prévoit également la possibilité pour l'intéressé de désinstaller l'application de son équipement terminal de communications électroniques à tout moment. Les données biométriques sont elles-mêmes supprimées du traitement sitôt l'enrôlement dans le traitement terminé.

Le Conseil d'État ajoute dans le projet la précision selon laquelle l'Agence nationale des titres sécurisés procède, au moment de la demande d'ouverture du compte, au recueil du consentement de l'usager au traitement de ses données biométriques.

CE, Section de l'intérieur, 2 avril 2019, Avis n°397073, Projet de décret autorisant la création d'un moyen d'identification électronique dénommé « Application de Lecture de l'Identité d'un Citoyen en Mobilité » (ALICEM)

Spécificité du consentement

1) Recueil du consentement (art. 4, 6 et 7 du RGPD) – a) Consentement univoque – Recueil au moyen d'une case cochée par défaut – Absence – b) Consentement spécifique – Recueil dans le cadre de l'acceptation globale de conditions générales d'utilisation d'un service – Absence – c) Consentement éclairé – Exigence d'une présentation claire et distincte de l'ensemble des finalités poursuivies par le traitement

1) Il résulte du 11 de l'article 4 et des articles 6 et 7 du RGPD, tels qu'interprétés par la Cour de justice de l'Union européenne dans son arrêt C-673/17 du 1er octobre 2019 que le consentement libre, spécifique, éclairé et univoque ne peut qu'être un consentement exprès de l'utilisateur, donné en toute connaissance de cause et après une information adéquate sur l'usage qui sera fait de ses données personnelles.

a) Un consentement donné au moyen d'une case cochée par défaut n'implique pas un comportement actif de la part de l'utilisateur et ne peut dès lors être considéré comme procédant d'un acte positif clair permettant valablement le recueil du consentement.

b) En outre, un consentement recueilli dans le cadre de l'acceptation globale de conditions générales d'utilisation d'un service ne revêt pas un caractère spécifique au sens du RGPD.

c) Enfin, indépendamment des modalités dans lesquelles il est recueilli, le consentement n'est valide que s'il est précédé d'une présentation claire et distincte de l'ensemble des finalités poursuivies par le traitement.

CE, 10ème-9ème chambres réunies, 19 juin 2020, Google LLC, n° 430810, Rec., point 21

Voir aussi : CJUE, grande chambre, 1er octobre 2019, Planet49, C-673/17

Prospection commerciale – Collecte indirecte des données des prospects – 1) Modalités et preuve du recueil du consentement – 2) Information des personnes – Liste exhaustive et mise à jour des prestataires et fournisseurs

1) Lorsque les données des prospects n'ont pas été collectées directement auprès d'eux par l'organisme qui prospecte, le consentement peut avoir été recueilli au moment de la collecte initiale des données par le primo-collectant, pour le compte de l'organisme qui réalisera les opérations de prospection ultérieures ou par l'organisme qui prospecte avant de procéder à des actes de prospection. Le prospecteur doit alors être en mesure de prouver qu'il dispose de ce consentement au sens de l'article 7, paragraphe 1 du RGPD.

2) Lorsque le consentement est recueilli par le primo-collectant pour le compte de prospecteurs, celui-là doit clairement informer les personnes de l'identité du ou des prospecteurs pour le compte duquel le consentement est collecté et des finalités pour lesquelles les données seront utilisées. À défaut, il revient à l'organisme qui prospecte de recueillir un tel consentement avant de procéder à des actes de prospection pour que le consentement soit éclairé. Pour ce faire, une liste exhaustive et mise à jour doit être tenue à la disposition des personnes au moment du recueil de leur consentement, par exemple directement sur le support de collecte ou, si celle-ci est trop longue, via un lien hypertexte renvoyant vers ladite liste et les politiques de confidentialité des prestataires et fournisseurs.

CNIL, FR, 24 novembre 2022, Sanction, Société X, n°SAN-2022-021 , publié, point 22

Prospection commerciale – Transmission de données à des tiers – Consentement global aux conditions générales contractuelles régissant un service et à l'ensemble des finalités d'un traitement – Exclusion

Dans le contexte d'une transmission de données à des partenaires afin qu'ils les utilisent pour de la prospection commerciale, le recueil d'un consentement spécifique implique que la personne soit en mesure de marquer son assentiment particulier à la transmission de ses données à des tiers, qui l'utiliseront pour de la prospection commerciale. L'exigence de spécificité du consentement exclut l'obtention d'un consentement global donné à la fois aux conditions générales contractuelles régissant un service et pour l'ensemble des finalités d'un traitement.

CNIL, P, 1er décembre 2021, Mise en demeure, Société X, n°MED-2021-131, non publié

Voir aussi : CJUE, grande chambre, 1er octobre 2019, Planet49, C-673/17

Caractère éclairé

1) Information claire et complète devant être donnée par le fournisseur de services – Durée de fonctionnement des cookies – Inclusion – Possibilité ou non pour des tiers d'avoir accès aux cookies – Inclusion – 2) La liste des informations que doit fournir le responsable du traitement à la personne auprès de laquelle il collecte des données la concernant, dressée à l'article 10 de la directive 95/46, n'est pas exhaustive.

1) L'article 5, paragraphe 3, de la directive 2002/58 doit être interprété en ce sens que les informations que le fournisseur de services doit donner à l'utilisateur d'un site internet incluent la durée de fonctionnement des cookies ainsi que la possibilité ou non pour des tiers d'avoir accès à ces cookies.

L'article 10 de la directive 95/46, à laquelle fait référence l'article 5, paragraphe 3, de la directive 2002/58, ainsi que l'article 13 du RGPD énoncent les informations que le responsable du traitement doit fournir à la personne auprès de laquelle il collecte des données la concernant. Ces informations comprennent notamment, en vertu de l'article 10 de la directive, outre l'identité du responsable du traitement et les finalités du traitement auquel les données sont destinées, toute information supplémentaire telle que les destinataires ou les catégories de destinataires des données, dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

2) Si la durée du traitement des données ne figure pas parmi ces informations, il ressort toutefois de l'expression « au moins » figurant à l'article 10 de la directive 95/46 que celles-ci ne sont pas énumérées de manière exhaustive. Or, l'information sur la durée de fonctionnement des cookies doit être considérée comme répondant à l'exigence d'un traitement loyal des données prévue par ledit article, en ce que, dans une situation telle que celle en cause au principal, une durée longue, voire illimitée, implique la collecte de nombreuses informations sur les habitudes de navigation et la fréquence des visites éventuelles de l'utilisateur sur les sites des partenaires publicitaires de l'organisateur du jeu promotionnel.

Cette interprétation est corroborée par l'article 13, paragraphe 2, sous a), du règlement 2016/679, qui prévoit que le responsable du traitement doit fournir à la personne concernée, pour garantir un traitement équitable et transparent, une information portant, notamment, sur la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée.

Quant à la possibilité ou non pour des tiers d'avoir accès aux cookies, il s'agit d'une information comprise dans les informations mentionnées à l'article 10, sous c), de la directive 95/46, ainsi qu'à l'article 13, paragraphe 1, sous e), du règlement 2016/679, dès lors que ces dispositions mentionnent explicitement les destinataires ou les catégories de destinataires des données.

CJUE, grande chambre, 1er octobre 2019, Planet49, C-673/17, points 76-80

---

1) Obligations d'information et de transparence (art. 12 et 13 du RGPD) – Accessibilité des informations pertinentes relatives aux différentes finalités et à l'ampleur du traitement – 2) Recueil du consentement (art. 4, 6 et 7 du RGPD) –c) Consentement éclairé – Exigence d'une présentation claire et distincte de l'ensemble des finalités poursuivies par le traitement

1) Il résulte clairement des articles 12 et 13 du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD) que l'information fournie aux utilisateurs doit les mettre en mesure de déterminer à l'avance la portée et les conséquences du traitement afin d'éviter qu'ils soient pris au dépourvu quant à la façon dont leurs données à caractère personnel ont vocation à être utilisées. Si les exigences de concision,

d'intelligibilité, de clarté et de simplicité de l'information posées par le RGPD justifient que celle-ci ne soit pas excessivement détaillée afin de ne pas décourager l'utilisateur d'en prendre connaissance, tous les éléments pertinents relatifs aux différentes finalités et à l'ampleur du traitement doivent lui être aisément accessibles.

2) Il résulte du 11 de l'article 4 et des articles 6 et 7 du RGPD, tels qu'interprétés par la Cour de justice de l'Union européenne dans son arrêt C-673/17 du 1er octobre 2019 que le consentement libre, spécifique, éclairé et univoque ne peut qu'être un consentement exprès de l'utilisateur, donné en toute connaissance de cause et après une information adéquate sur l'usage qui sera fait de ses données personnelles. [...]

c) Indépendamment des modalités dans lesquelles il est recueilli, le consentement n'est valide que s'il est précédé d'une présentation claire et distincte de l'ensemble des finalités poursuivies par le traitement.

En l'espèce, l'arborescence choisie par Google apparaît de nature, par l'éparpillement de l'information qu'elle organise, à nuire à l'accessibilité et à la clarté de celle-ci pour les utilisateurs, alors même que les traitements en cause sont particulièrement intrusifs eu égard au nombre et à la nature des données collectées.

CE, 10ème–9ème chambres réunies, 19 juin 2020, Google LLC, n° 430810, Rec., points 15-21

Prospection commerciale – Transmission à des données à des tiers prospecteurs – Information des personnes concernées sur la portée du traitement

Dans le contexte d'une transmission de données à des partenaires en vue qu'ils les utilisent pour de la prospection commerciale, le recueil d'un consentement éclairé requiert en particulier d'informer les personnes concernées de l'étendue de la transmission de leurs données. À cet égard, des indications relatives au nombre et au secteur d'activité des partenaires rendus destinataires des données avant toute transmission, sont de nature à éclairer les personnes concernées quant à l'utilisation ultérieure qui sera faite de leurs données.

CNIL, P, 1er décembre 2021, Mise en demeure, Société X, n° MED-2021-131, non publié

Caractère univoque

Cas particuliers

Consentement pour le compte de sociétés partenaires

Accord de responsabilité conjointe – Collecte du consentement pour le compte de sociétés partenaires – Obligation du responsable de traitement ne collectant pas le consentement d'être en mesure de démontrer que la personne concernée a donné son consentement

En cas de responsabilité conjointe, l'article 26 du RGPD oblige les responsables de traitement conjoints à s'assurer, par le biais d'un accord, qu'ils respectent mutuellement le RGPD et notamment qu'ils organisent entre eux la meilleure façon de répondre aux droits des personnes concernées, en fonction de la nature du traitement et de leur responsabilité respective vis-à-vis de ce traitement.

En l'espèce, le fait que la collecte du consentement des internautes pour la mise en œuvre du traitement en cause revenait aux partenaires de la société mise en cause n'exonérait pas cette dernière

de son obligation, en application de l'article 7 du RGPD, d'être en mesure de démontrer que la personne concernée avait donné son consentement et de procéder à certaines vérifications à cette fin. En effet, la seule clause issue de conditions générales d'utilisation aux termes desquelles la société exigeait de ses partenaires, « lorsque la loi le prévoit », que la politique de confidentialité de leur site inclue « des mentions et des mécanismes de choix conformes aux lois et réglementations applicables » ne permettait pas de garantir l'existence d'un consentement valide et il convenait à tout le moins qu'elle soit complétée pour préciser que l'organisme qui recueille le consentement doit mettre à disposition de l'autre partie la preuve du consentement.

CNIL, FR, 15 juin 2023, Sanction, Société X, n°SAN-2023-009, publié, points 59, 61, 74

Consentement des enfants et offres de service de la société de l'information (article 8 RGPD)

Consentement explicite

Employés

2.4.2 Contrat

Collecte de données des utilisateurs d'un réseau social issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers – Mise en relation de ces données avec le compte du réseau social des utilisateurs – Utilisation des données – Nécessaire à l'exécution du contrat – Condition

L'article 6, paragraphe 1, premier alinéa, sous b), du règlement 2016/679 doit être interprété en ce sens que le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, ne peut être considéré comme étant nécessaire à l'exécution d'un contrat auquel les personnes concernées sont parties, au sens de cette disposition, qu'à la condition que ce traitement soit objectivement indispensable pour réaliser une finalité faisant partie intégrante de la prestation contractuelle destinée à ces mêmes utilisateurs, de telle sorte que l'objet principal du contrat ne pourrait être atteint en l'absence de ce traitement.

CJUE, grande chambre, 4 juillet 2023, Meta Platforms e.a., C-252/21

2.4.3 Obligation légale

L'obligation légale ne peut être retenue comme base légale du traitement que si ledit traitement répond effectivement à une obligation légale qui s'impose au responsable de traitement sans viser d'autre objectif que celui poursuivi par l'auteur de l'obligation et sans qu'il existe de moyen moins intrusif d'atteindre cet objectif, et que la disposition légale en question institue une obligation suffisamment claire, précise et impérative pour le responsable de traitement de traiter des données à caractère personnel.

CNIL, P, 1er août 2024, Rappel aux obligations légales, Société X, n°ROL231090, non publié

2.4.4 Intérêts vitaux

2.4.5 Mission d'intérêt public

1) Condition de licéité d'une demande de communication de données à caractère personnel par l'administration fiscale – Nécessité pour remplir sa mission d'intérêt public – 2) Perception de l'impôt et lutte contre la fraude fiscale – Mission d'intérêt public – Existence – 3) Cas d'une demande qui n'est pas directement fondée sur la disposition légale qui constitue le fondement du traitement mais résulte d'une demande de l'autorité compétente – Conditions

1) Pourvu que les finalités énoncées dans une demande de communication de données à caractère personnel adressée par l'administration d'un État membre à un opérateur économique soient nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investie l'administration fiscale, cette circonstance suffit, ainsi qu'il découle de l'article 6, paragraphe 1, premier alinéa, initio et sous e), du règlement 2016/679, lu conjointement avec l'article 6, paragraphe 3, second alinéa, de ce règlement, pour que lesdits traitements satisfassent également à l'exigence de licéité.

2) La perception de l'impôt et la lutte contre la fraude fiscale doivent être considérées comme étant des missions d'intérêt public, au sens de l'article 6, paragraphe 1, premier alinéa, sous e), du règlement 2016/679 (voir, par analogie, arrêt du 27 septembre 2017, Puškár, C-73/16, EU:C:2017:725, point 108).

3) Dans un cas où la communication des données à caractère personnel en cause n'est pas directement fondée sur la disposition légale qui en constitue le fondement du traitement, mais résulte d'une demande de l'autorité publique compétente, il est nécessaire que cette demande précise quelles sont les finalités spécifiques de cette collecte de données au regard de la mission d'intérêt public ou de l'exercice de l'autorité publique, afin de permettre au destinataire de ladite demande de s'assurer que la transmission des données à caractère personnel en cause est licite et aux juridictions nationales d'opérer un contrôle de la légalité des traitements concernés.

CJUE, 24 février 2022, Valsts ieņēmumu dienests, C-175/20, points 69-71

Demandeur du statut d'opérateur économique agréé – Licéité d'une demande de communication des numéros d'identification fiscale des personnes physiques par les autorités douanières – Condition

L'article 24, paragraphe 1, second alinéa, du règlement d'exécution (UE) 2015/2447 de la Commission, du 24 novembre 2015, établissant les modalités d'application de certaines dispositions du règlement (UE) n° 952/2013 du Parlement européen et du Conseil établissant le code des douanes de l'Union, lu à la lumière de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 et du RGPD, doit être interprété en ce sens que les autorités douanières peuvent exiger du demandeur du statut d'opérateur économique agréé qu'il communique les numéros d'identification fiscale, attribués aux fins du prélèvement de l'impôt sur le revenu, concernant uniquement les personnes physiques qui sont responsables du demandeur ou exercent le contrôle sur la gestion de celui-ci et celles qui sont responsables des questions douanières en son sein, ainsi que les coordonnées des centres des impôts compétents à l'égard de l'ensemble de ces personnes, pour autant que ces données permettent à ces autorités d'obtenir des informations relatives aux infractions graves ou répétées à la législation douanière ou aux dispositions fiscales ou aux infractions pénales graves commises par ces personnes physiques en lien avec leur activité économique.

CJUE, 16 janvier 2019, Deutsche Post, C-496/17

Directive 95/46/CE – Établissement, aux fins de la perception de l'impôt et de la lutte contre la fraude fiscale, d'une liste de personnes sans le consentement des personnes concernées – Admissibilité sous conditions

L'article 7, sous e), de la directive 95/46/CE doit être interprété en ce sens qu'il ne s'oppose pas à un traitement de données à caractère personnel par les autorités d'un État membre aux fins de la perception de l'impôt et de la lutte contre la fraude fiscale tel que celui auquel il est procédé par l'établissement d'une liste de personnes telle que celle en cause dans l'affaire au principal, sans le consentement des personnes concernées, à condition, d'une part, que ces autorités aient été investies par la législation nationale de missions d'intérêt public au sens de cette disposition, que l'établissement de cette liste et l'inscription sur celle-ci du nom des personnes concernées soient effectivement aptes et nécessaires aux fins de la réalisation des objectifs poursuivis et qu'il existe des indices suffisants pour présumer que les personnes concernées figurent à juste titre sur ladite liste et, d'autre part, que toutes les conditions de licéité de ce traitement de données à caractère personnel imposées par la directive 95/46/CE soient satisfaites.

CJUE, 27 septembre 2017, Puškár, C-73/16

Réglementation nationale imposant à l'employeur de mettre à la disposition de l'autorité nationale compétente le registre du temps de travail – Licéité sous conditions

Les articles 6, paragraphe 1, sous b) et c), ainsi que 7, sous c) de la directive 95/46/CE ne s'opposent pas à une réglementation nationale qui impose à l'employeur l'obligation de mettre à la disposition de l'autorité nationale compétente en matière de surveillance des conditions de travail le registre du temps de travail afin d'en permettre la consultation immédiate, pour autant que cette obligation est nécessaire aux fins de l'exercice par cette autorité de ses missions de surveillance de l'application de la réglementation en matière de conditions de travail, notamment, en ce qui concerne le temps de travail.

CJUE, 30 mai 2013, Worten, C-342/12

2.4.6 Intérêt légitime

Collecte, par une entreprise de transport, des données relatives à la civilité et à l'identité de genre de ses clients - 1) Traitement nécessaire à l'exécution d'un contrat liant la personne concernée – Exclusion – Traitement nécessaire aux fins des intérêts légitimes– Conditions – 2) Appréciation de l'intérêt légitime – Prise en compte du droit d'opposition – Exclusion

1) L'article 6, paragraphe 1, premier alinéa, sous b) et f), du règlement général sur la protection des données, lu en combinaison avec l'article 5, paragraphe 1, sous c), de ce règlement doit être interprété en ce sens que :

- le traitement de données à caractère personnel relatives à la civilité des clients d'une entreprise de transport, ayant pour finalité une personnalisation de la communication commerciale fondée sur leur identité de genre, ne paraît ni objectivement indispensable ni essentiel afin de permettre l'exécution correcte d'un contrat et, partant, ne peut pas être considéré comme étant nécessaire à l'exécution de ce contrat ;

- le traitement de données à caractère personnel relatives à la civilité des clients d'une entreprise de transport, ayant pour finalité une personnalisation de la communication commerciale fondée sur leur identité de genre, ne peut pas être considéré comme étant nécessaire aux fins des intérêts légitimes poursuivis par le responsable de ce traitement ou par un tiers, lorsque :
    - l'intérêt légitime poursuivi n'a pas été indiqué à ces clients lors de la collecte de ces données ; ou
    - ledit traitement n'est pas opéré dans les limites du strict nécessaire pour la réalisation de cet intérêt légitime ; ou
    - au regard de l'ensemble des circonstances pertinentes, les libertés et droits fondamentaux desdits clients sont susceptibles de prévaloir sur ledit intérêt légitime, notamment en raison d'un risque de discrimination fondée sur l'identité de genre.

2) L'article 6, paragraphe 1, premier alinéa, sous f), du règlement général sur la protection des données doit être interprété en ce sens que, afin d'apprécier la nécessité d'un traitement de données à caractère personnel au titre de cette disposition, il n'y a pas lieu de prendre en considération l'existence éventuelle d'un droit d'opposition de la personne concernée, au titre de l'article 21 de ce règlement.

CJUE, 9 janvier 2025, Mousse, C-394/23

Collecte de données des utilisateurs d'un réseau social issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers – Mise en relation de ces données avec le compte du réseau social des utilisateurs – Utilisation des données – Nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement – Condition

L'article 6, paragraphe 1, premier alinéa, sous f), du règlement 2016/679 doit être interprété en ce sens que le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, ne peut être considéré comme étant nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, au sens de cette disposition, qu'à la condition que ledit opérateur ait indiqué aux utilisateurs auprès desquels les données ont été collectées un intérêt légitime poursuivi par leur traitement, que ce traitement est opéré dans les limites du strict nécessaire pour la réalisation de cet intérêt légitime et qu'il ressort d'une pondération des intérêts opposés, au regard de l'ensemble des circonstances pertinentes, que les intérêts ou les libertés et les droits fondamentaux de ces utilisateurs ne prévalent pas sur ledit intérêt légitime du responsable du traitement ou d'un tiers.

CJUE, grande chambre, 4 juillet 2023, Meta Platforms e.a., C-252/21

Mise en place d'un système de vidéosurveillance dans les parties communes d'un immeuble à usage d'habitation – Existence – Conditions de licéité

L'article 6, paragraphe 1, sous c) et l'article 7, sous f) de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, lus à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, doivent être interprétés en ce sens qu'ils ne s'opposent pas à des dispositions nationales qui autorisent la mise en place d'un système de vidéosurveillance, tel que le système en cause au principal installé dans les parties communes d'un immeuble à usage d'habitation, aux fins de poursuivre des intérêts légitimes consistant à assurer la garde et la protection des personnes et des biens, sans le consentement des personnes concernées, si le traitement de données à caractère personnel opéré au moyen du système de vidéosurveillance en cause répond aux conditions posées audit article 7, sous f), ce qu'il incombe à la juridiction de renvoi de vérifier.

CJUE, 11 décembre 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18

Responsabilité conjointe du gestionnaire d'un site internet équipé du bouton « j'aime » de Facebook – Condition de licéité au titre de l'intérêt légitime

Lorsque le gestionnaire d'un site internet insère sur ledit site un module social permettant au navigateur du visiteur de ce site de solliciter des contenus du fournisseur dudit module et de transmettre à cet effet audit fournisseur des données à caractère personnel du visiteur (bouton « j'aime » de Facebook), ce site, comme le réseau social, doivent être regardés comme co-responsables du traitement consistant dans le recueil et la transmission à Facebook de données à caractère personnel des visiteurs du site.

Pour que ce traitement soit licite au titre de l'intérêt légitime, il est nécessaire que ce gestionnaire et ce fournisseur poursuivent chacun, avec ces opérations de traitement (communication et transmission des données), un intérêt légitime, au sens de l'article 7, sous f), de la directive 95/46, afin que celles-ci soient justifiées dans son chef.

CJUE, 29 juillet 2019, Fashion ID, C-40/17, points 93-97

Directive 95/46/CE – Demande par un particulier de communication des données personnelles d'une personne responsable d'un accident de la circulation afin d'exercer un droit en justice – Possibilité pour le responsable du traitement de faire droit à une telle demande

L'article 7, sous f), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, doit être interprété en ce sens qu'il n'impose pas l'obligation de communiquer des données à caractère personnel à un tiers afin de lui permettre d'introduire un recours en indemnisation devant une juridiction civile pour un dommage causé par la personne concernée par la protection de ces données. Toutefois, l'article 7, sous f), de cette directive ne s'oppose pas à une telle communication sur la base du droit national.

CJUE, 4 mai 2017, Rïgas satiksme, C-13/16

Restriction de l'intérêt légitime – Illicéité d'une règlementation nationale empêchant la collecte et l'utilisation des données à caractère personnel par un fournisseur de service de médias en ligne – Traitement visant à garantir le fonctionnement d'un service et sa facturation

L'article 7, sous f), de la directive 95/46 doit être interprété en ce sens qu'il s'oppose à une réglementation d'un État membre en vertu de laquelle un fournisseur de services de médias en ligne ne peut collecter et utiliser des données à caractère personnel afférentes à un utilisateur de ces services, en l'absence du consentement de celui-ci, que dans la mesure où cette collecte et cette utilisation sont nécessaires pour permettre et facturer l'utilisation concrète desdits services par cet utilisateur, sans que l'objectif visant à garantir la capacité générale de fonctionnement des mêmes services puisse justifier l'utilisation desdites données après une session de consultation de ceux-ci.

CJUE, 19 octobre 2016, Breyer, C-582/14

Réglementation nationale conditionnant la légitimité de l'intérêt conditionnée à un consentement ou au caractère public de la donnée – Inconventionnalité

L'article 7, sous f) de la directive 95/46/CE du 24 octobre 1995 s'oppose à une réglementation nationale qui, en l'absence du consentement de la personne concernée et pour autoriser le traitement de ses données à caractère personnel nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable de ce traitement ou par le ou les tiers auxquels ces données sont communiquées, exige, outre le respect des droits et libertés fondamentaux de cette dernière, que lesdites données figurent dans des sources accessibles au public, excluant ainsi de façon catégorique et généralisée tout traitement de données ne figurant pas dans de telles sources.

CJUE, 24 novembre 2011, ASNEF, C-468/10 et C-469/10

Conservation des informations bancaires d'un client – Prévalence des intérêts des personnes concernées sur l'intérêt légitime d'une société

L'intérêt légitime que peut avoir une société à conserver les informations bancaires d'un client qui a procédé à un achat en ligne, notamment son numéro de carte bancaire, afin de faciliter des paiements ultérieurs en le dispensant de saisir à nouveau cette information, ne saurait prévaloir sur l'intérêt des clients de protéger ces données, compte tenu de la sensibilité de ces informations bancaires et des préjudices susceptibles de résulter pour eux de leur captation et d'une utilisation détournée, et alors que de nombreux clients qui utilisent des sites de commerce en ligne en vue de réaliser des achats ponctuels ne peuvent raisonnablement s'attendre à ce que les entreprises concernées conservent de telles données sans leur consentement.

CE, 10ème-9ème chambres réunies, 10 décembre 2020, Cdiscount, n° 429571, T., point 9

Attentes raisonnables de la personne concernée – Utilisation de données publiquement accessibles pour alimenter un logiciel de reconnaissance faciale – Illicéité

Si elles peuvent raisonnablement s'attendre à ce que des tiers accèdent ponctuellement aux photographies mises en lignes par la personne concernée, le caractère publiquement accessible de celles-ci ne suffit pas pour considérer que les personnes concernées puissent raisonnablement s'attendre à ce que leurs images alimentent un logiciel de reconnaissance faciale, d'autant plus lorsque ce logiciel n'est pas public et la grande majorité des personnes concernées ignorent son existence.

Les personnes qui ont publié des photographies les représentant sur des sites web, ou consenti à cette publication auprès d'un autre responsable de traitement, ne s'attendent pas à ce que celles-ci soient réutilisées pour la création d'un logiciel de reconnaissance faciale (qui associe l'image d'une personne à un profil contenant l'ensemble des photographies sur lesquelles elle figure, les informations que ces photographies contiennent ainsi que les sites web sur lesquels elles se trouvent) et la commercialisation de ce logiciel à des forces de l'ordre.

CNIL, P, 26 novembre 2021, Mise en demeure, Société X, n° MED 2021-134, publié, points 64-65

Voir aussi : CNIL, FR, 17 octobre 2022, Sanction, Société X, n°SAN-2022-019, publié

Lobbying – Traitement consistant en la collecte d'informations visant à recenser les personnes influentes – Condition de justification par la poursuite de l'intérêt légitime – Obligation d'information des personnes

Un traitement de données à caractère personnel, consistant en la collecte d'informations visant à recenser les personnes influentes auprès desquelles une entreprise souhaite représenter ses intérêts peut, sous réserve de certaines conditions, être réalisé sur le fondement de l'intérêt légitime poursuivi par le responsable de traitement. En effet, un tel traitement peut être justifié par la poursuite de

l'intérêt légitime du responsable de traitement sous réserve que les intérêts et droits fondamentaux des personnes concernées ne prévalent pas sur les intérêts du responsable de traitement. Cette mise en balance entre les différents intérêts en présence impose notamment de prendre en compte les attentes raisonnables des personnes concernées quant à la nature des données collectées et la façon dont elles sont traitées pour la constitution du traitement litigieux, comme le prévoit le considérant 47 du RGPD.

Dans tous les cas, le responsable de traitement qui met en œuvre un tel traitement doit s'assurer du respect des obligations prévues par le RGPD et notamment de l'obligation d'information des personnes afin notamment que celles-ci puissent exercer leurs droits.

CNIL, FR, 26 juillet 2021, Sanction, Société X, n° SAN-2021-012, publié, points 74, 77

2.5 Pertinence et minimisation des données

Collecte, par une entreprise de transport, des données relatives à la civilité et à l'identité de genre de ses clients - 1) Traitement nécessaire à l'exécution d'un contrat liant la personne concernée – Exclusion – Traitement nécessaire aux fins des intérêts légitimes– Conditions – 2) Appréciation de l'intérêt légitime – Prise en compte du droit d'opposition – Exclusion

1) L'article 6, paragraphe 1, premier alinéa, sous b) et f), du règlement général sur la protection des données, lu en combinaison avec l'article 5, paragraphe 1, sous c), de ce règlement doit être interprété en ce sens que :

- le traitement de données à caractère personnel relatives à la civilité des clients d'une entreprise de transport, ayant pour finalité une personnalisation de la communication commerciale fondée sur leur identité de genre, ne paraît ni objectivement indispensable ni essentiel afin de permettre l'exécution correcte d'un contrat et, partant, ne peut pas être considéré comme étant nécessaire à l'exécution de ce contrat ;
- le traitement de données à caractère personnel relatives à la civilité des clients d'une entreprise de transport, ayant pour finalité une personnalisation de la communication commerciale fondée sur leur identité de genre, ne peut pas être considéré comme étant nécessaire aux fins des intérêts légitimes poursuivis par le responsable de ce traitement ou par un tiers, lorsque :
    - l'intérêt légitime poursuivi n'a pas été indiqué à ces clients lors de la collecte de ces données ; ou
    - ledit traitement n'est pas opéré dans les limites du strict nécessaire pour la réalisation de cet intérêt légitime ; ou
    - au regard de l'ensemble des circonstances pertinentes, les libertés et droits fondamentaux desdits clients sont susceptibles de prévaloir sur ledit intérêt légitime, notamment en raison d'un risque de discrimination fondée sur l'identité de genre.

2) L'article 6, paragraphe 1, premier alinéa, sous f), du règlement général sur la protection des données doit être interprété en ce sens que, afin d'apprécier la nécessité d'un traitement de données à caractère personnel au titre de cette disposition, il n'y a pas lieu de prendre en considération l'existence éventuelle d'un droit d'opposition de la personne concernée, au titre de l'article 21 de ce règlement.

CJUE, 9 janvier 2025, Mousse, C-394/23

---

1) Appréciation conjointe avec la condition de nécessité du traitement, en fonction de la base légale – 2) Publication de déclaration d'intérêts privés d'un directeur d'établissement recevant des fonds publics – Données nominatives relatives au conjoint, concubin ou partenaire – Absence de stricte nécessité

1) Pour l'examen de l'existence de la base légale de l'obligation légale, la condition tenant à la nécessité du traitement portant publication en ligne sur le site internet d'une autorité publique de données à caractère personnel contenues dans une déclaration d'intérêts privés que tout directeur d'établissement percevant des fonds publics est tenu de déposer auprès de cette autorité en vue d'assurer la prévalence de l'intérêt public, l'impartialité des décisions, la prévention des situations de conflits d'intérêts et la lutte contre la corruption doit être examinée conjointement avec le principe dit de la « minimisation des données » consacré à l'article 5, paragraphe 1, sous c), du RGPD.

2) Seules les données dont la publication est effectivement de nature à renforcer les garanties de probité et d'impartialité des responsables publics, à prévenir les conflits d'intérêts et à lutter contre la corruption dans le secteur public peuvent faire l'objet d'un tel traitement. La divulgation publique, en ligne, de données nominatives relatives au conjoint, concubin ou partenaire ainsi qu'aux personnes proches ou connues du déclarant susceptibles de donner lieu à un conflit d'intérêts, ou encore sur toute transaction conclue au cours des douze derniers mois dont la valeur excède 3000 euros paraît aller au-delà de ce qui est strictement nécessaire.

CJUE, grande chambre, 1er août 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, points 93-94

Communication par un opérateur économique d'informations à l'administration fiscale relatives aux contribuables ayant publié des annonces dans l'une des rubriques de son portail Internet – Conditions de licéité

La réglementation nationale régissant une demande de communication de données à caractère personnel adressée par l'administration d'un État membre à un opérateur économique doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles un prestataire de services en ligne est tenu de transmettre des données à caractère personnel relatives à ses utilisateurs (voir, en ce sens, arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 78 et jurisprudence citée).

Les dispositions du RGPD doivent être interprétées en ce sens qu'elles ne s'opposent pas à ce que l'administration fiscale d'un État membre impose à un prestataire de services d'annonces publiées sur internet de lui communiquer des informations relatives aux contribuables ayant publié des annonces dans l'une des rubriques de son portail internet pour autant, notamment, que ces données soient nécessaires au regard des finalités spécifiques pour lesquelles elles sont collectées et que la période sur laquelle porte la collecte desdites données n'excède pas la durée strictement nécessaire pour atteindre l'objectif d'intérêt général visé.

CJUE, 24 février 2022, Valsts ieņēmumu dienests , C-175/20, point 84

Traitement de données à caractère personnel relatives aux citoyens de l'Union non-ressortissants de l'État membre ayant pour objectif le soutien des autorités nationales en charge de l'application de la réglementation sur le droit de séjour – Conditions de licéité

Un traitement de données à caractère personnel relatives aux citoyens de l'Union non-ressortissants de l'État membre visé ayant pour objectif le soutien des autorités nationales en charge de l'application de la réglementation sur le droit de séjour ne répond à l'exigence de nécessité prévue à l'article 7, sous e), de la directive 95/46/CE du 24 octobre 1995 interprété à la lumière de l'interdiction de toute discrimination exercée en raison de la nationalité, que :

- s'il contient uniquement les données nécessaires à l'application par lesdites autorités de cette réglementation, et
- si son caractère centralisé permet une application plus efficace de cette réglementation en ce qui concerne le droit de séjour des citoyens de l'Union non-ressortissants de cet État membre.

Il appartient à la juridiction de renvoi de vérifier ces éléments en l'espèce au principal.

CJUE, grande chambre, 16 décembre 2008, Huber, C-524/06

Utilisation par un employeur d'un dispositif de vidéosurveillance pour le contrôle des règles d'hygiène et de sécurité – Disproportion – Inopposabilité au salarié des enregistrements issus de cette vidéosurveillance dans le cadre d'une procédure de licenciement

Aux termes de l'article L. 1121-1 du code du travail, nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

La cour d'appel a constaté que le salarié, qui exerçait seul son activité en cuisine, était soumis à la surveillance constante de la caméra qui y était installée. Elle en a déduit à bon droit que les enregistrements issus de ce dispositif de surveillance, attentatoire à la vie personnelle du salarié et disproportionné au but allégué par l'employeur de sécurité des personnes et des biens, n'étaient pas opposables au salarié et a, par ces seuls motifs, légalement justifié sa décision.

Cass, soc., 23 juin 2021, n°19-13.856, B., points 5-6

Utilisation par un employeur d'un système de géolocalisation pour le contrôle de la durée du travail de ses salariés – Caractère excessif – Existence, sauf lorsque ce contrôle ne peut pas être fait par un autre moyen, même moins efficace

Il résulte des articles 6 de la loi n° 78-17 du 6 janvier 1978 et L. 1121-1 du code du travail que l'utilisation par un employeur d'un système de géolocalisation pour assurer le contrôle de la durée du travail de ses salariés n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, fût-il moins efficace que la géolocalisation. En dehors de cette hypothèse, la collecte et le traitement de telles données à des fins de contrôle du temps de travail doivent être regardés comme excessifs au sens du 3° de l'article 6 de la loi du 6 janvier 1978.

CE, 10ème-9ème chambres réunies, 15 décembre 2017, Société Odeolis, n° 403776, Rec., point 7

Utilisation par un employeur d'un dispositif de vidéosurveillance continue pour lutter contre des vols susceptibles d'être perpétrés par ses propres salariés– Disproportion en l'espèce

Est disproportionné et peut légalement faire l'objet d'une sanction un dispositif de vidéosurveillance plaçant sous surveillance en permanence au moins un salarié. En l'espèce, la circonstance que la société ait voulu lutter contre des vols susceptibles d'être perpétrés par ses propres salariés ne permet pas de considérer que le dispositif était proportionné alors qu'en outre il était installé dans des locaux sécurisés, dont l'entrée ne peut s'effectuer qu'après autorisation et vérification d'identité.

CE, 10ème/9ème SSR, 18 novembre 2015, Société PS Consulting, n° 371196, Inédit., points 9-12

Transmission de données – Condition de limitation des données transmises à celles strictement nécessaires aux destinataires pour poursuivre les finalités du traitement

Il résulte des dispositions de l'article 6 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction applicable au litige que, pour être compatible avec les finalités d'un traitement, la transmission des données à caractère personnel doit être strictement limitée à celles qui permettent aux destinataires de poursuivre les finalités du traitement. Par suite, un traitement relatif à la prévention des atteintes à la sécurité publique en marge d'événements sportifs ne peut pas légalement prévoir que les associations et fédérations sportives, qui n'exercent aucune mission relative aux finalités poursuivies, puissent être destinataires des données collectées.

CE, 10ème/9ème SSR, 21 septembre 2015, Association de défense et d'assistance juridique des intérêts des supporters, n° 389815, Inédit., points 16-17

Données adéquates, pertinentes et non excessives – Condition non remplie – Conservation dans un traitement informatisé des données à caractère personnel recueillies lors de l'établissement ou du renouvellement des passeports de huit empreintes digitales alors que le passeport n'en contient que deux

Constitution d'un traitement automatisé centralisé des données à caractère personnel (état civil, image numérisée du visage et empreintes de huit doigts) recueillies auprès des personnes âgées d'au moins six ans lors de l'établissement ou du renouvellement des passeports.

La finalité de la consultation des empreintes digitales contenues dans le traitement automatisé (confirmer que la personne présentant une demande de renouvellement d'un passeport est bien celle à laquelle le passeport a été initialement délivré ou à s'assurer de l'absence de falsification des données contenues dans le composant électronique du passeport) peut être atteinte de manière suffisamment efficace en comparant les empreintes figurant dans le composant électronique du passeport avec celles conservées dans le traitement, sans qu'il soit nécessaire que ce dernier en contienne davantage.

Dès lors, le Conseil d'État annule l'article litigieux du fait de l'inconventionnalité de la collecte et de la conservation d'un plus grand nombre d'empreintes digitales que celles figurant dans le composant électronique, ces données n'étant ni adéquates, ni pertinentes et apparaissant excessives au regard des finalités du traitement informatisé.

CE, Assemblée, 26 octobre 2011, Association pour la promotion de l'image et autres, n° 317827, Rec., points 11-12

Données pertinentes – 1) Notion – 2) Application en l'espèce

1) Pour l'application de l'article 6 de la loi n°78-17 du 6 janvier 1978, les données pertinentes au regard de la finalité d'un traitement automatisé de données à caractère personnel sont celles qui sont en adéquation avec la finalité du traitement et qui sont proportionnées à cette finalité.

2) En l'espèce, les données enregistrées dans la « Base élèves 1er degré », relatives à l'identification de l'élève, de ses responsables légaux et des autres personnes à contacter en cas d'urgence ou autorisées à le prendre en charge à la sortie de l'école, ainsi qu'à la gestion des établissements, de la scolarité des élèves et de leurs activités parascolaires et périscolaires, sont en adéquation avec la finalité du traitement, qui est la gestion de l'enseignement scolaire de premier cycle, et sont proportionnées à cette finalité.

CE, 10ème/9ème SSR, 19 juillet 2010, M. X et Mme Y, n°317182, Rec., point 27

Opposition à la prospection – 1) Liste repoussoir – Données nécessaires pour la prise en compte de l'opposition – 2) Conservation de la civilité, du nom/prénom, date de naissance, numéro de téléphone, adresse électronique, ville ou code postal, niveau d'imposition et situation familiale des prospects ayant exercé leur droit d'opposition – Illicéité

Conservation des données d'opposition d'une personne à recevoir de la prospection commerciale.

1) Afin d'assurer l'effectivité du droit d'opposition, le responsable de traitement peut créer une « liste repoussoir » lui permettant de ne pas utiliser à nouveau les données de contact si elles venaient à lui être transmises à nouveau par une autre personne que la personne concernée. La CNIL recommande de conserver l'inscription à la « liste repoussoir » de la personne ayant fait opposition pendant une durée minimale de trois ans et de ne conserver que les empreintes de l'adresse ou du numéro utilisé pour la prospection. Cela permet de prendre en compte l'opposition dans le temps sans conserver de données directement identifiantes.

2) En l'espèce, la liste repoussoir comprenait la civilité, le nom, le prénom, la date de naissance, le numéro de téléphone, l'adresse électronique, la ville ou le code postal, le niveau d'imposition et la situation familiale alors que l'ensemble de ces données n'apparaissaient pas nécessaires au regard de la finalité liée à la prise en compte de l'opposition des prospects à recevoir de la prospection. Seules les données nécessaires à la prise en compte de l'opposition dans le temps et qui correspondent en l'espèce au numéro de téléphone et à l'adresse électronique de la personne concernée auraient dû être conservées sous une forme hachée. Il en résulte une méconnaissance de l'article 5-1-c) du RGPD.

CNIL, P, 26 juin 2023, Mise en demeure, Société X, n° MED-2023-040, non publié

Enregistrement systématique des appels téléphoniques entre téléopérateurs et prospects – Finalité d'établissement d'une preuve du contrat éventuellement conclu – Caractère non nécessaire si obligation d'une confirmation écrite de l'offre

Un responsable du traitement, qui souhaite enregistrer des conversations téléphoniques à des fins probatoires, doit démontrer qu'il ne dispose pas d'autres moyens moins intrusifs pour prouver que le contrat conclu à distance a bien a été conclu avec la personne concernée.

En application de l'article L.221-16 du code de la consommation, dès lors que la preuve de la souscription d'un contrat conclut à distance, à la suite d'un démarchage téléphonique, peut être apportée par la confirmation écrite de l'offre, l'enregistrement des conversations téléphoniques, passées entre les téléopérateurs et les prospects, à des fins de preuve de la formation du contrat, n'apparait pas nécessaire.

CNIL, FR, 8 juin 2023, Sanction, Société X, n° SAN-2023-008, publié, points 31, 34

Enregistrement systématique des appels téléphoniques entre téléopérateurs et prospects – 1) Finalité probatoire – Caractère excessif – 2) Finalité de formation – Caractère excessif

L'enregistrement intégral et systématique par une société de l'ensemble des appels téléphoniques sortants passés entre ses téléopérateurs et ses prospects commerciaux à des fins probatoires et de formation constitue un manquement à l'article 5-1-c) du RGPD, qui dispose que les données à caractère personnel doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ».

1) Concernant la finalité probatoire, l'article L.221-16 du code de la consommation dispose qu'« à la suite d'un démarchage par téléphone, le professionnel adresse au consommateur, sur papier ou sur

support durable, une confirmation de l'offre qu'il a faite et reprenant toutes les informations prévues à l'article L. 221-5. Le consommateur n'est engagé par cette offre qu'après l'avoir signée et acceptée par écrit ou avoir donné son consentement par voie électronique ». Il en résulte que la souscription d'un contrat conclu à distance est prouvée par un autre moyen que l'enregistrement des appels téléphoniques passés avec les prospects.

2) Concernant la finalité relative à la formation, un enregistrement aléatoire de seulement quelques conversations téléphoniques permettrait à la personne chargée de la formation de disposer des éléments nécessaires à la réalisation de sa mission.

CNIL, P, 29 mars 2022, Mise en demeure, Société X, n° MED-2022-021, non publié

Identifiant spécifique et distinct de l'identifiant national pour la mise en œuvre d'un traitement spécifique

Dans le cadre d'un projet de décret autorisant la mise en œuvre par le ministère de l'éducation nationale d'un traitement ayant pour finalité d'améliorer la prise en charge et le parcours scolaire des élèves à besoins éducatifs particuliers, de mieux individualiser les réponses pédagogiques et de garantir aux familles la mise en place d'adaptations pédagogiques dès le repérage de difficultés d'apprentissage, la CNIL considère que la création et l'utilisation d'un identifiant spécifique et distinct de l'identifiant national élève (INE) permettra, conformément à sa doctrine, de segmenter les traitements afin d'éviter des interconnexions ou rapprochements de données qui ne sont pas nécessaires, et de limiter les risques de réidentification des personnes en cas de fuite de données.

CNIL, P, 15 juillet 2021, Avis sur projet de décret, Livret de parcours inclusif (LPI), n° 2021-082, publié, point 16

Systèmes d'identification par reconnaissance faciale de mineurs – Objectifs pouvant être atteints par des moyens aussi efficaces et moins intrusifs

Les principes de nécessité d'un traitement fondé sur l'intérêt public et de minimisation des données s'opposent à la mise en œuvre de systèmes d'identification par reconnaissance faciale d'enfants à des fins de contrôle d'accès à des établissements scolaires, dès lors que les objectifs de sécurisation et la fluidification des entrées dans de tels établissements peuvent être atteints par des moyens aussi efficaces et moins intrusifs et compte tenu de la protection particulière dont doivent bénéficier les enfants, quand bien même ces systèmes seraient mis en œuvre à titre expérimental et reposeraient sur le consentement des élèves concernés.

CNIL, P, 25 octobre 2019, Demande de conseil, Lycées de la région X, DI 191260, non publié

2.6 Exactitude des données

1) Effets de l'amnistie et de la réhabilitation – Interdiction de rappeler l'existence de condamnations, de sanctions, d'interdictions, de déchéances ou d'incapacités – Conséquence – Obligation de prévoir l'effacement des données correspondantes sur les fichiers permettant dans les tribunaux la gestion automatisée des procédures – 2) Conséquence de l'annulation d'un arrêté méconnaissant ces règles

1) Si le ministre de la justice, a prévu, au troisième alinéa de l'article 6 de l'arrêté du 18 juin 1986 et de l'arrêté du 13 avril 1993, tel que modifié par les arrêtés du 22 octobre 2001, que les fichiers

informatiques institués par ces textes, dans le but d'automatiser la gestion des procédures, seraient mis à jour en cas d'amnistie et de réhabilitation « par mention et en conformité avec les dispositions [...] des articles 133-9 à 11 pour l'amnistie et 133-16 pour la réhabilitation », ce dispositif, qui ne prévoit aucun effacement des données, ne suffit pas à garantir que les principes posés par le code pénal qui interdisent de « rappeler l'existence » de condamnations, de sanctions, d'interdictions, de déchéances ou d'incapacités, seront respectés. Illégalité des arrêtés en tant qu'ils concernent l'amnistie et la réhabilitation.

2) L'annulation contentieuse d'arrêtés fixant le régime de fichiers informatiques illégaux au motif qu'ils ne prévoyaient pas l'effacement des condamnations ayant fait l'objet d'une amnistie ou d'une réhabilitation a nécessairement pour conséquence l'obligation pour le ministre de la justice de prendre, dans un délai raisonnable, un arrêté modifiant les arrêtés du 18 juin 1986 et du 13 avril 1993 afin de prévoir les conditions et les limites dans lesquelles ces fichiers devront être mis à jour pour tenir compte des amnisties et réhabilitations. Il lui incombe de prévoir explicitement que cette modification devra consister en l'effacement de toutes les mentions de nature à rappeler l'existence des condamnations, sanctions, interdictions, déchéances ou incapacités et que ne pourra subsister dans le fichier que la référence à la loi d'amnistie ou à la décision portant réhabilitation.

CE, 6ème/4ème SSR, 5 mars 2003, M. X, n° 241325, Rec, points 4-5

2.7 Conservation

Législation nationale prévoyant une obligation extrêmement large de conservation de toutes les communications Internet de tous les utilisateurs – Violation de l'article 8 CESDH

La législation contestée exige la conservation et le stockage automatiques et continus du contenu de toutes les communications Internet (communications vocales, textuelles, visuelles, sonores, vidéo ou d'autres communications électroniques) pendant une durée de six mois et des données de connexion correspondantes pendant une durée d'un an. Elle concerne tous les utilisateurs, même en l'absence de soupçon raisonnable de participation à des activités criminelles ou à des activités mettant en danger la sécurité nationale, ou de toute autre raison de penser que la conservation des données peut contribuer à la lutte contre les formes graves de criminalité ou à la protection de la sécurité nationale. Il n'y a aucune limitation du champ d'application de la mesure en termes d'application territoriale ou temporelle ou de catégories de personnes susceptibles de voir leurs données à caractère personnel conservées. La Cour conclut que l'ingérence est exceptionnellement étendue et grave. La législation ne peut être considérée comme nécessaire dans une société démocratique et porte atteinte à l'essence même du droit au respect de la vie privée garanti par l'article 8 de la Convention. L'État défendeur a donc outrepassé toute marge d'appréciation acceptable à cet égard.

CEDH, 13 février 2024, Podchasov c. Russie, n°33696/19, point 70

Collecte et conservation de données dans une base de données de la police relative à l'« extrémisme national » – Données révélant les convictions politiques – Faible probabilité d'infraction du fait de l'âge du requérant – Conservation des données injustifiée du fait de l'absence de garanties et de délais – Violation de l'article 8 CEDH

Le requérant, un militant de longue date, protestait contre la collecte et la conservation, dans une base de données de la police relative à l'« extrémisme national », de données personnelles le concernant.

La Cour a conclu à la violation de l'article 8 de la Convention.

Si la Cour EDH reconnaît un besoin impérieux de recueillir des données à caractère personnel concernant le requérant, elle considère en revanche que la *conservation* des données relatives au requérant ne répondait pas à un besoin impérieux. En l'absence de toute règle fixant la durée maximale de conservation de pareilles données, le requérant dépendait entièrement de la diligence avec laquelle les autorités appliqueraient les garanties du code de pratique applicable, très souples par nature, pour veiller au caractère proportionné de la durée de conservation des données le concernant. Lorsqu'un État décide de mettre en place un dispositif de ce type, la nécessité de garanties procédurales effectives devient déterminante. Ces garanties doivent permettre la suppression des données à caractère personnel dès que la poursuite de leur conservation devient disproportionnée.

Les données à caractère personnel concernant le requérant auraient pu être conservées indéfiniment. Certes, le requérant pouvait demander que ces données lui soient communiquées et soient supprimées, ce qu'il a fait. Néanmoins, il apparaît que cette garantie a eu un effet limité, les autorités ayant refusé de supprimer les données concernées ou de motiver la décision de les conserver. L'absence de garanties effectives est particulièrement préoccupante dans le cas du requérant, en ce que les données personnelles conservées révèlent des opinions politiques et méritent donc une protection accrue. L'article 11 offre une protection spécifique aux personnes qui participent à des protestations pacifiques, mais aussi une protection spéciale aux syndicats, dont le requérant a participé à certains rassemblements.

Dans la définition de la notion d'extrémisme national donnée en lien avec la « base de données relative à l'extrémisme » dans le cadre de la procédure interne, il est fait référence à la collecte de données sur des groupes et individus ayant agi « hors du processus démocratique ». Il apparaît donc que la police n'a pas respecté la définition qu'elle avait elle-même établie, en ce qu'elle a conservé des données relatives à la participation du requérant à des manifestations politiques pacifiques.

Il n'a pas été démontré que la conservation des données concernant le requérant, et plus particulièrement de celles relatives à sa participation à des manifestations pacifiques, revêtait un caractère absolument nécessaire, ni qu'elle répondait aux besoins d'une enquête donnée.

La Cour n'est pas convaincue que la suppression des données soit une tâche d'une complexité excessive. Il serait totalement contraire à la nécessité de protéger le droit à la vie privée consacré par l'article 8 qu'un État puisse créer une base de données dans laquelle il serait difficile d'examiner ou de modifier les données, puis qu'il puisse invoquer la manière dont cette base de données a été conçue pour justifier son refus de supprimer des informations y figurant.

CEDH, 24 janvier 2019, Affaire Catt c. Royaume-Uni, n° 43514/15

Expiration de la durée de conservation initiale des données – Tri des données pertinentes à archiver – Archivage intermédiaire – Base de données d'archives dédiée ou séparation logique

La durée de conservation des données à caractère personnel doit être déterminée en fonction de la finalité poursuivie par le traitement. Lorsqu'elles ne sont plus nécessaires au besoin de la finalité pour laquelle elles ont été collectées, les données doivent soit être supprimées, soit faire l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses. Les données ainsi placées en archivage intermédiaire, le sont pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont conservées, conformément aux dispositions en vigueur. Ainsi, après avoir opéré un tri des données pertinentes à archiver, le responsable de traitement doit prévoir, à cet effet, une base de données d'archives dédiée ou une séparation logique dans la base de données active. Cette séparation logique est assurée par la mise en place de mesures techniques et organisationnelles garantissant que seules

les personnes ayant un intérêt à traiter les données en raison de leurs fonctions puissent y accéder. Au-delà de ces durées de conservation en archive intermédiaire, les données à caractère personnel doivent, sauf exception, être supprimées ou anonymisées.

CNIL, FR, 8 septembre 2022, Sanction, Groupement X, n° SAN-2022-018, publié, point 24

2.7.1 Durée de conservation

Législation nationale prévoyant la conservation par les autorités de police, à des fins de prévention et de détection des infractions pénales de données à caractère personnel, y compris biométriques et génétiques, concernant des personnes ayant fait l'objet d'une condamnation pénale définitive jusqu'au décès de ces personnes - Inconventionnalité

L'article 4, paragraphe 1, sous c) et e), de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, lu en combinaison avec les articles 5 et 10, l'article 13, paragraphe 2, sous b), ainsi que l'article 16, paragraphes 2 et 3, de celle-ci, et à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'il s'oppose à une législation nationale qui prévoit la conservation, par les autorités de police, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, de données à caractère personnel, notamment de données biométriques et génétiques, concernant des personnes ayant fait l'objet d'une condamnation pénale définitive pour une infraction pénale intentionnelle relevant de l'action publique, et ce jusqu'au décès de la personne concernée, y compris en cas de réhabilitation de celle-ci, sans mettre à la charge du responsable du traitement l'obligation de vérifier régulièrement si cette conservation est toujours nécessaire, ni reconnaître à ladite personne le droit à l'effacement de ces données, dès lors que leur conservation n'est plus nécessaire au regard des finalités pour lesquelles elles ont été traitées, ou, le cas échéant, à la limitation du traitement de celles-ci.

CJUE, 30 janvier 2024, NG c./ Direktor na Glavna direktsia « Natsionalna politsia » pri Ministerstvo na vatreshnite raboti – Sofia, C-118/22

Collecte et conservation de données reflétant l'orientation sexuelle supposée – Données ne reposant sur aucune base factuelle avérée – Absence de démonstration de l'encadrement de la durée de conservation – Durée de conservation excessive – Violation de l'article 8 CEDH

Ont été collectées et conservées, dans une base de données initialement exploitée par l'un des établissements de l'Établissement Français du Sang, des données personnelles indiquant que le requérant était concerné par la contre-indication au don de sang, alors prévue pour les hommes ayant eu un rapport sexuel avec un homme en droit interne. De telles données comportent des indications explicites sur la vie sexuelle et sur l'orientation sexuelle supposée du requérant. Le fait que cette contre-indication était conservée avec la simple référence à un code et non la description explicite d'un comportement sexuel n'est pas déterminant. Il était en outre prévu que les données saisies en 2004 soient conservées jusqu'en 2278.

La Cour EDH conclut que cette collecte et conservation de données personnelles sensibles constitue une ingérence dans le droit au respect de la vie privée du requérant. Néanmoins, cette ingérence était « prévue par la loi » et poursuivait le but légitime de la protection de la santé.

La collecte et la conservation de données personnelles relatives aux résultats des procédures de sélection des candidats au don du sang, et en particulier aux motifs d'exclusion du don éventuellement retenus, contribuent à garantir la sécurité transfusionnelle. Sans qu'il soit besoin de rechercher si d'autres critères de sélection des donneurs étaient envisageables, la collecte et la conservation des données litigieuses reposaient sur des motifs pertinents et suffisants.

Eu égard à la sensibilité des données personnelles litigieuses, qui comportent des indications sur les pratiques et l'orientation sexuelles du requérant, il est particulièrement important qu'elles répondent aux exigences de qualité prévues à l'article 5 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe. Il importe en particulier qu'elles soient exactes et, le cas échéant, mises à jour, qu'elles soient adéquates, pertinentes et non excessives par rapport aux finalités du traitement, et que leur durée de conservation n'excède pas celle qui est nécessaire. Par ailleurs, les données litigieuses, qui touchaient à l'intimité du requérant, ont été collectées et conservées sans le consentement explicite du requérant. En conséquence, la Cour se doit de procéder à cet examen de façon rigoureuse.

En premier lieu, s'agissant de l'exactitude des données personnelles, celle-ci doit être appréciée au regard de la finalité pour laquelle ces données ont été collectées. Dans le traitement litigieux, cette catégorie de données avait pour finalité d'assurer le respect d'une contre-indication au don spécifique, que le droit interne prévoyait alors de façon permanente. À cette fin, elle devait reposer sur une base factuelle précise et exacte. Or, le requérant s'est vu appliquer une contre-indication propre aux hommes ayant eu un rapport sexuel avec un homme au seul motif qu'il avait refusé de répondre à des questions relatives à sa sexualité lors de l'entretien médical préalable au don. Aucun des éléments soumis à l'appréciation du médecin ne lui permettait de tirer une telle conclusion sur ses pratiques sexuelles. C'est pourtant ce motif d'exclusion du don qui fut renseigné et conservé. Les données collectées se fondaient sur de simples spéculations et ne reposaient sur aucune base factuelle avérée. Or, c'est aux autorités qu'il incombe de démontrer l'exactitude des données collectées. De surcroît, elles n'ont pas avoir été mises à jour à la suite des protestations et de la plainte du requérant.

Par ailleurs, il est inadéquat de collecter une donnée personnelle relative aux pratiques et à l'orientation sexuelles sur le seul fondement de spéculations ou de présomptions. Au surplus, il aurait suffi, pour atteindre l'objectif de sécurité transfusionnelle recherché, de garder trace du refus du requérant de répondre aux questions relatives à sa sexualité, cet élément étant de nature à justifier, à lui seul, un refus de la candidature au don de sang.

En second lieu, le Gouvernement ne démontre pas qu'à l'époque des faits, la durée de conservation des données litigieuses était encadrée de telle sorte qu'elle ne puisse pas excéder celle nécessaire aux finalités pour lesquelles elles ont été collectées. Au moment de la collecte de ces données en 2004, l'outil informatique employé par l'ÉFS prévoyait leur conservation jusqu'en 2278, rendant ainsi possible leur utilisation de manière répétée. À la date du 26 mai 2016, soit près de douze ans après leur collecte, les données relatives au motif d'exclusion étaient encore conservées. À cet égard, la durée de conservation des données doit être encadrée pour chacune des catégories de données concernées et elle doit être révisée si les finalités pour lesquelles elles ont été collectées ont évolué. Au vu de la pratique constante de l'ÉFS, la durée excessive de conservation des données litigieuses a rendu possible leur utilisation répétée à l'encontre du requérant, entraînant son exclusion automatique du don de sang.

Au vu de l'ensemble des éléments qui précèdent, l'État défendeur a outrepassé sa marge d'appréciation en la matière.

CEDH, 8 septembre 2022, Affaire Drelon c. France, n°3153/16, 27758/18, points 86-100

Durée de conservation supérieure au délai de prescription pour une infraction – Admissibilité en l'espèce

Dans le cadre d'un traitement de données ayant notamment pour finalités de constater l'ensemble des infractions non routières faisant l'objet d'une amende forfaitaire relevées au moyen d'appareils électroniques permettant l'établissement d'un procès-verbal électronique, la durée de conservation de cinq ans des données relatives aux contraventions non routières et la durée de conservation de dix ans des données relatives aux délits non routiers n'est pas disproportionnée, eu égard en particulier aux délais de prescription de six ans des peines délictuelles et de trois ans des peines contraventionnelles, respectivement prévus par les articles 133-3 et 133-4 du code pénal, ainsi qu'aux règles de procédure qui régissent le recouvrement des amendes forfaitaires, en particulier les délais de recours et de mise en paiement.

Dans le cas d'espèce, les délais de prescription ne s'imposent pas à la conservation des données. En effet, la prescription de l'action publique et la prescription de la peine peuvent faire l'objet, l'une et l'autre, d'interruptions. Dans la mesure où les délais de conservation ont été fixés non pas pour la prévention de la récidive, mais pour couvrir la procédure dans son ensemble, incluant l'encaissement effectif de l'amende et le cas échéant les procédures juridictionnelles, les durées de dix ans pour les délits et de cinq ans pour les contraventions ne sont pas disproportionnées.

CE, 10ème–9ème chambres réunies, 24 septembre 2021, Médecins du Monde et autres, n°441317, Inédit., point 5

Traitements automatisés de données à caractère personnel intéressant la sûreté de l'État ou la sécurité publique – Obligation de fixer une durée maximale de conservation et de la respecter – Obligation de préciser cette durée dans l'acte autorisant le traitement – Absence – Cas particuliers des personnes âgées de moins de 13 ans

Le Conseil d'État (section de l'intérieur) a donné un avis favorable à un projet de décret portant création d'un traitement automatisé de données à caractère personnel, dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD).

Le projet crée un traitement automatisé de données à caractère personnel permettant, à l'occasion de la réalisation d'enquêtes administratives sur le fondement des articles L. 114-1, L. 114-2 et L. 211-11-1 du code de la sécurité intérieure, de consulter automatiquement d'autres traitements automatisés de données à caractère personnel ou d'entrer en relation avec eux. Cette consultation peut prendre la forme d'une consultation automatique ou d'une mise en relation.

En application des dispositions du 5° de l'article 6 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les responsables de tout traitement doivent veiller à ne conserver les données du traitement que pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. La fixation, par ces responsables, d'une durée de conservation des données est donc obligatoire, même si, comme c'est possible pour ceux des traitements intéressant la sûreté de l'État ou la sécurité publique mentionnés à l'article 1er du décret du 15 mai 2007, cette durée peut ne pas être mentionnée dans l'acte réglementaire autorisant le traitement.

Mais le Conseil d'État considère que la collecte, dans le cadre de ces mêmes traitements, de données relatives à des personnes âgées de moins de 13 ans, doit s'accompagner de la fixation, par l'acte réglementaire autorisant ce traitement, d'une durée de conservation de ces données.

CE, Section de l'intérieur, 4 juillet 2017, Avis n° 393336, Projet de décret portant création d'un traitement automatisé dénommé « Automatisation de la consultation centralisée de renseignements et de données »

Données relatives aux impayés – Conservation au-delà du règlement de la somme due

Les conséquences ou les risques résultant de la commission d'un impayé ne peuvent être réputés avoir disparu dès le règlement de la dette. Il n'est dès lors pas disproportionné de prévoir une conservation des données relatives aux incidents de cette nature pendant une durée suffisante, au-delà du règlement de la somme due, pour prévenir le renouvellement de tels incidents.

CE, 10ème-9ème chambres réunies, 13 juin 2016, SASP Paris-Saint-Germain Football, n° 377194, Inédit., point 8

Carte nationale d'identité – Collecte, conservation et consultation des empreintes digitales – Durée de conservation illimitée faute de dispositions expresses la régissant – Illégalité

Faute de dispositions expresses la régissant, la durée de conservation des empreintes digitales relevées sur le fondement de l'article 5 du décret du 22 octobre 1955 est illimitée. Une telle durée de conservation ne peut être regardée comme nécessaire aux finalités du fichier, eu égard à la durée de validité de la carte nationale d'identité et au délai dans lequel tout détenteur d'une carte nationale d'identité périmée peut en solliciter le renouvellement. Elle est donc illégale.

CE, 10ème/9ème SSR, 18 novembre 2015, Mme B...D... et Mme A...C..., n° 372111, T., point 6

Traitement public encadré par décret – Conservation des données pour une finalité non prévue par l'acte réglementaire – Illicéité

Eu égard à la finalité du fichier ayant notamment trait à la gestion des contentieux entre l'administration pénitentiaire et les personnes placées sous main de justice, la durée de conservation de deux ans prévue à l'article R. 57-9-21 à compter de la date de levée d'écrou n'est pas excessive. En revanche, la conservation ultérieure de ces données pour un délai de huit ans, qui poursuit, selon la garde des sceaux, la conduite éventuelle de contentieux, est dépourvue de fondement légal dès lors que cette finalité n'est pas explicitée par le décret attaqué et que la durée de conservation ainsi définie ne s'y rattache pas spécifiquement.

CE, 10ème/9ème SSR, 9 novembre 2015, Conseil national de l'ordre des médecins, n° 383313, Inédit., point 8

Durée totale de conservation des données relatives à l'identification des élèves scolarisés équivalent à 35 ans – Durée excessive – Conséquence – Illégalité totale de la décision mettant en œuvre le traitement

Si les données relatives à l'identification des élèves scolarisés peuvent être conservées au sein de la « Base nationale des identifiants des élèves » pendant la durée du cycle d'étude - premier cycle en l'état actuel du fichier, cycle complet d'étude en cas de généralisation de l'utilisation de l'identifiant à l'enseignement secondaire et à l'enseignement supérieur -, une durée totale de conservation de 35 ans n'apparaît pas nécessaire aux finalités du traitement et est donc excessive au regard des dispositions du 5° de l'article 6 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Ce vice entache d'illégalité l'ensemble de la décision mettant en œuvre le traitement.

CE, 10ème/9ème SSR, 19 juillet 2010, M. X et Mme Y, n° 334014, T., point 13

Création d'un traitement automatisé destiné à faciliter la mise en œuvre des mesures d'éloignement des étrangers (décret du 26 décembre 2007) – Durée de conservation des données étendue à 3 ans pour certaines d'entre elles – Stricte nécessité – Absence – Conséquence – Illégalité

En l'absence de justification de l'extension à 3 ans, à compter de l'éloignement effectif, de la durée de conservation des données relatives à l'identification de l'étranger et de ses enfants, aux caractéristiques de la mesure d'éloignement, à la soustraction éventuelle de l'étranger à l'exécution de cette mesure, à l'exercice de recours contentieux et à la demande de laissez-passer auprès des autorités consulaires du pays vers lequel l'éloignement est ordonné, celle-ci ne répond pas à l'exigence de stricte nécessité découlant de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Illégalité du décret dans cette mesure.

CE, Section, 30 décembre 2009, Association SOS Racisme et GISTI, n° 312051, Rec., points 19-21

Opposition à la prospection – Liste repoussoir –Conservation des données nécessaires à la prise en compte de l'opposition – Durée minimale recommandée de trois ans

Afin d'assurer l'effectivité du droit d'opposition, le responsable de traitement peut créer une « liste repoussoir » lui permettant de ne pas utiliser à nouveau les données de contact si elles venaient à lui être transmises à nouveau par une autre personne que la personne concernée. La CNIL recommande de conserver l'inscription à la « liste repoussoir » de la personne ayant fait opposition pendant une durée minimale de trois ans et de ne conserver que les empreintes de l'adresse ou du numéro utilisé pour la prospection. Cela permet de prendre en compte l'opposition dans le temps sans conserver de données directement identifiantes.

CNIL, P, 26 juin 2023, Mise en demeure, Société X, n°MED-2023-040, non publié

Véhicules connectés – Géolocalisation – Durée de conversation des données à caractère personnel excessive au regard de la finalité du traitement

Le fait que le point de départ de la durée de conservation des données de géolocalisation soit lié non pas au contrat de location mais à la fin de la relation commerciale avec l'utilisateur ne permet pas de respecter le principe selon lequel les données à caractère personnel ne doivent pas être conservées pour une durée qui excède celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

En l'espèce, la société a conservé les données de géolocalisation en cause pour une durée qui excédait celle nécessaire au regard des finalités pour lesquelles elles étaient traitées et a ainsi méconnu ses obligations au regard de l'article 5.1.e du RGPD.

CNIL, FR, 7 juillet 2022, Sanction, Société X, n°SAN-2022-015, publié, points 74-75

Respect de la durée de conservation par anonymisation des données – Licéité

L'anonymisation peut être considérée comme un moyen permettant de se conformer aux obligations en matière de limitation de la conservation lorsqu'à l'issue d'une période de conservation en base active pendant la durée d'une relation contractuelle, une société procède à un premier tri des données en anonymisant les données non pertinentes et en conservant, en base d'archivage intermédiaire, les données permettant de répondre aux obligations légales ou lorsqu'elles présentent un intérêt

administratif pour la société, et lorsqu'à l'issue de cette période d'archivage intermédiaire les données sont automatiquement anonymisées.

CNIL, FR, 23 juin 2022, Clôture d'injonction, Société X, n° SAN-2022-012, non publié

Traitements publics encadrés par un acte réglementaire – 1) Obligation d'inscrire l'archivage intermédiaire dans l'acte réglementaire – Appréciation d'espèce – 2) Obligation d'inscrire l'archivage définitif dans l'acte réglementaire – Absence

Cas d'un traitement de l'État permettant d'enregistrer des informations sur les ressortissants français et leurs ayants droit ainsi que documents relatifs à une situation de crise à l'étranger en vue d'en faciliter la gestion et d'informer et associer les personnes concernées.

1) Une fois que les données ne sont plus utilisées dans le cadre de la gestion opérationnelle liée à l'évènement survenu à l'étranger ou pour réaliser les statistiques prévues, il est recommandé de mettre en place un archivage intermédiaire afin de limiter la consultation de ces données à des personnes spécifiquement habilitées. Eu égard à l'écart entre la durée d'utilisation opérationnelle des données et leur durée de conservation en base intermédiaire (10 ans), le principe d'un tel archivage intermédiaire devrait en l'espèce être inscrit dans le décret portant création du traitement, à titre de garantie apportée aux personnes concernées.

2) S'agissant de l'archivage définitif au titre de l'application des règles régissant les archives publiques issues du code du patrimoine, un acte réglementaire régissant un traitement public réserve toujours implicitement l'application des obligations du code du patrimoine et l'archivage définitif n'a pas besoin d'être expressément prévu par l'acte réglementaire.

CNIL, P, 21 avril 2022, Avis sur projet de décret, n° 2022-051, non publié

Obligations à l'issue de la durée de conservation des données lorsque la finalité poursuivie par le traitement est atteinte

La durée de conservation des données à caractère personnel doit être déterminée en fonction de la finalité poursuivie par le traitement. Lorsque cette finalité est atteinte, les données doivent en principe être supprimées, anonymisées ou faire l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses.

L'effectivité de la mise en œuvre d'une politique de durée de conservation des données est le pendant nécessaire de sa définition et permet d'assurer que les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Cela permet notamment, de réduire les risques d'usage non autorisé des données en cause, par un salarié ou par un tiers.

CNIL, FR, 29 octobre 2021, Sanction, X, n°SAN-2021-019, publié, points 56-57

2.7.2 Modalités de conservation

2.8 Sécurité

Exception à l'obligation d'information - Procédure de réclamation – Périmètre des vérifications - Obligations de sécurité consacrées à l'article 32 du RGPD – Exclusion

Les obligations consacrées à l'article 32 du RGPD, qui doivent être respectées en toute hypothèse et indépendamment de l'existence ou non d'une obligation d'information en vertu de l'article 14 de ce règlement, sont de nature et de portée différentes par rapport à l'obligation d'information prévue à cet article 14. Ainsi, en cas de réclamation au titre de l'article 77, paragraphe 1, du RGPD, au motif que le responsable du traitement a invoqué, à tort, l'exception prévue à l'article 14, paragraphe 5, sous c), de ce règlement, l'objet des vérifications à effectuer par l'autorité de contrôle est circonscrit par le champ d'application du seul article 14 dudit règlement, le respect de l'article 32 de celui-ci ne faisant pas partie de ces vérifications.

CJUE, 28 novembre 2024, Másdi, C-169/23, points 72, 73

Mesure consistant à réserver l'accès à un fichier à des personnes spécialement habilitées – Incidence d'une irrégularité sur la décision prise après la consultation du fichier – Cas d'un agrément refusé après consultation du TAJ

Il résulte du 1° du I de l'article R. 40-29 du code de procédure pénale (CPP) que les agents habilités selon les modalités prévues au 1° du I de l'article R. 40-28 peuvent consulter les données à caractère personnel figurant dans le traitement des antécédents judiciaires (TAJ), qui se rapportent à des procédures judiciaires closes ou en cours, sans autorisation du ministère public, dans le cadre des enquêtes prévues à l'article L. 114-1 du code de la sécurité intérieure (CSI), applicable en particulier à l'instruction des demandes d'agrément des personnes chargées des visites de sûreté portuaire. Dès lors que l'article L. 5332-8 du code des transports prévoit la possibilité que certains traitements automatisés de données à caractère personnel soient consultés au cours de l'enquête conduite par l'administration dans le cadre de ses pouvoirs de police, préalablement à la délivrance d'un agrément individuel, la circonstance que l'agent ayant procédé à cette consultation n'aurait pas été, en application des articles R. 40-23, R. 40-28 et du 1° du I de l'article R. 40-29 du CPP, individuellement désigné et régulièrement habilité à cette fin, si elle est susceptible de donner lieu aux procédures de contrôle de l'accès à ces traitements, n'est pas, par elle-même, de nature à entacher d'irrégularité la décision prise sur la demande d'agrément.

CE, 5ème–6ème chambres réunies, 22 juin 2022, M. B... A..., n° 452969, T., points 3, 5

Absence de contrôle régulier des mesures techniques et organisationnelles prises par le sous-traitant – Insuffisante robustesse de la politique de mots de passe – Manquements à l'article 32 RGPD

L'absence de mise en œuvre par un responsable du traitement d'un contrôle régulier sur les mesures techniques et organisationnelles prises par son sous-traitant chargé d'assurer la sécurité de son site web ayant pour conséquence directe la vulnérabilité du système informatique à l'origine de la violation des données de près de 200 000 clients européens, ainsi que le manque de robustesse de la politique de mots de passe de la société eu égard aux catégories de données traitées qui incluent notamment le numéro de sécurité sociale de ses clients, accroissant l'exposition de son système à un risque d'attaque informatique, sont de nature à caractériser un manquement aux dispositions de l'article 32 du RGPD.

CE, 10ème chambre, 26 avril 2022, Optical Center, n° 449284, Inédit., point 5

Élections des représentants du personnel – Vote électronique par internet – Protection du caractère personnel du vote – Modalités retenues n'offrant pas une protection du caractère personnel du vote d'un niveau équivalent à celui des autres modalités de vote

Dans le cadre d'élections des représentants du personnel au sein des instances de représentation du personnel de la fonction publique hospitalière, si le vote électronique par internet est susceptible de constituer une modalité de vote au même titre que le vote à l'urne et le vote par correspondance, il implique, en raison de ses spécificités et des conditions de son utilisation, que des garanties adaptées soient prévues pour que le respect des principes généraux du droit électoral de complète information de l'électeur, de libre choix de celui-ci, d'égalité entre les candidats, de secret du vote, de sincérité du scrutin et de contrôle du juge soit assuré à un niveau équivalent à celui des autres modalités de vote.

Dès lors, d'une part, que l'identification du demandeur qui sollicite la mise en œuvre d'une procédure de « réassort » (nouvelles communication des éléments d'authentification nécessaires pour participer au scrutin) s'effectue par la seule vérification de ses nom, prénom, date et lieu de naissance, informations qui peuvent aisément être connues de tiers, et, d'autre part, que le moyen de communication par lequel sont envoyés l'identifiant et le nouveau mot de passe est celui qu'indique le demandeur qui sollicite ce « réassort », sans qu'il soit garanti qu'il ne serait accessible qu'à l'électeur, et alors même qu'un même numéro de téléphone ou une même adresse électronique ne peut être utilisé que pour une seule demande de « réassort », les requérants sont fondés à soutenir que les modalités retenues pour le vote électronique par internet n'offraient pas une protection du caractère personnel du vote d'un niveau équivalent à celui des autres modalités de vote.

Compte tenu de l'importance du recours au vote électronique dans les scrutins en cause et de l'impossibilité de déterminer le nombre de cas dans lesquels a été mise en œuvre, pour chacune des instances concernées, la procédure dite de « réassort », les syndicats requérants sont fondés à demander l'annulation de l'ensemble des opérations électorales en vue de la désignation des représentants du personnel.

CE, 8ème–3ème chambres réunies, 26 janvier 2021, Union des syndicats CGT des agents de l'AP-HM, n° 437993, Inédit., points 16, 19-21

Données biométriques – Collecte par des personnels spécifiquement désignés par les compagnies aériennes – Exigence d'une connexion internet sécurisée répondant aux normes du référentiel général de sécurité (RGS) et de certificats d'authentification

Saisi d'un projet de décret relatif à la création d'un traitement automatisé de données à caractère personnel pour la production des certificats de membre d'équipage sécurisés biométriques, le Conseil d'État (section de l'intérieur) estime nécessaire que le décret précise que la transmission des données personnelles collectées dans des stations d'enrôlement installées dans les locaux des compagnies aériennes par connexion internet sécurisée à l'Imprimerie nationale obéisse aux règles du référentiel général de sécurité (RGS) mentionné au décret n° 2010-112 du 2 février 2010 et que les personnels des compagnies aériennes spécifiquement désignés pour la collecte soient titulaires d'un certificat d'authentification répondant aux normes du RGS. Le projet de décret est modifié en ce sens.

CE, Section de l'intérieur, 5 février 2019, Avis n° 396472, Projet de décret relatif à la création d'un traitement automatisé de données à caractère personnel pour la production des certificats de membre d'équipage sécurisés biométriques

---

Dossiers Patients Informatisés - 1) Politique d'habilitation – Droits de consultation des médecins – a) Accès à tout le dossier de leurs patients sauf certains éléments paramétrés comme sensibles - Admissibilité – b) Accès aux dossiers de tous les patients de l'établissement hospitalier – Inadmissibilité - 2) Journaux d'accès – a) Obligation d'effectuer des contrôles réguliers – b) Absence d'analyse régulière des journaux d'accès au DPI – Manquement à l'article 32 RGPD

1) a) Politique d'habilitation pour les dossiers des patients informatisés (DPI) dans un hôpital. Est admissible un paramétrage du DPI prévoyant qu'un médecin peut consulter tout le dossier de ses patients, sans limite d'antériorité, à l'exception de séjours qui peuvent être paramétrés au sein du DPI en accès restreints, car présentant une sensibilité particulière pour la vie privée, ainsi qu'à certains évènements futurs programmés à accès restreints. Un tel paramétrage répond à l'exigence de définir des droits en fonction du métier exercé au sein de la structure hospitalière en application de l'article L.1110-12 du Code de la santé publique et satisfait à l'exigence de protection de la confidentialité des données par une politique d'habilitation appropriée résultant de l'article 32 du RGPD.

b) N'est pas admissible en revanche le paramétrage qui prévoit que les médecins peuvent consulter les dossiers de tous les patients présents dans le DPI alors même qu'ils ne feraient pas partie de leur équipe de soins. Un tel paramétrage est contraire aux articles L.1110-4 et L.1110-12 du code de la santé publique, qui exigent que les habilitations tiennent compte de la notion d'équipe de soins.

2) a) Eu égard au volume et à la sensibilité des données traitées au sein du DPI, des contrôles réguliers de ces accès doivent être opérés, afin d'identifier ceux susceptibles d'être frauduleux ou illégitimes (par exemple un nombre trop élevé de dossiers consultés, ou un usage fréquent du mode « bris de glace » lorsqu'il est mis en place). Il est fortement recommandé d'exercer ces contrôles par le biais d'une analyse automatisée ou semi-automatisée, permettant de garantir la sécurité et la confidentialité des données à caractère personnel traitées.

b) L'absence de contrôle régulier des journaux d'accès au DPI, alors qu'il contient des données sensibles, qui concernent un nombre important de personnes constitue un manquement à l'article 32 du RGPD.

CNIL, P, 19 décembre 2024, Mise en demeure, Centre hospitalier universitaire X, n° MED 2024-176, non publié

Voir aussi : CNIL, P, 26 avril 2024, Mise en demeure, Centre hospitalier régional X, n° MED 2024-056, non publié

Accès à des données personnelles non publiques - Utilisation de compte partagés – 1) Cas général – Manquement en principe – 2) Cas des administrateurs – Manquement grave en principe

1) Au titre des mesures élémentaires de sécurité, il est en principe nécessaire que l'accès à un système d'information contenant des données à caractère personnel qui n'ont pas vocation à être publiées se fasse à travers un compte individuel, auquel l'utilisateur se connecte par un identifiant et un facteur d'authentification propres. En effet, seuls les comptes individuels permettent une bonne traçabilité des accès et des actions effectués sur le système. Les comptes partagés rendent beaucoup plus difficile l'imputabilité d'une action et compliquent le travail d'investigation en cas d'incident de sécurité ou de violation de données.

Par ailleurs, s'agissant des mots de passe, conformément aux règles élémentaires relatives à la sécurité des systèmes d'information, un mot de passe doit, pour être efficace, demeurer secret et individuel. Or, lorsqu'un compte est partagé entre plusieurs personnes, cette règle n'est plus respectée.

2) Cette exigence d'individualisation des comptes présente une acuité particulière s'agissant des administrateurs, qui disposent de droits plus étendus sur les données à caractère personnel traitées par le système, ce qui en fait des cibles d'attaque informatique et rend nécessaire de pouvoir détecter rapidement et efficacement une violation de données réalisées par l'un d'entre eux. À défaut, et en particulier lorsque des systèmes ou des équipements ne permettent pas de disposer de plusieurs comptes d'administration, des mesures complémentaires doivent être mises en œuvre pour assurer l'imputabilité des actions (ex. : bastion, main courante…) et assurer la protection du secret.

L'absence de telles mesures et/ou d'individualisation des comptes est susceptible de constituer un manquement à l'article 32 du RGPD.

CNIL, P., 24 juillet 2024, Mise en demeure, Société X, n°MED-2024-107, non publié

Dossiers Patients Informatisés - Equipe médicale – Notion - Accès – Politique d'habilitation – Critères

En application des articles L.1110-4 et L.1110-12 du code de la santé publique et de la Politique générale de sécurité des systèmes d'information de santé élaborée par l'Agence du Numérique en Santé (PGSSI-S), le responsable de traitement d'un dispositif de dossiers patients informatisés (DPI) doit mettre en place une politique d'habilitation rigoureuse et adaptée aux besoins de l'établissement, de sorte que chaque professionnel de santé et agent de l'établissement n'accède qu'aux dossiers dont il a à connaître. Cette politique d'habilitation doit combiner deux critères :

- d'une part, le métier exercé : ainsi, un agent responsable de l'accueil des patients dans la structure ne doit accéder qu'au dossier administratif du patient et non aux données médicales, alors qu'un médecin accèdera également aux données médicales ;
- d'autre part, la prise en compte de la notion d'équipe de soins, telle que définie par l'article L. 1110-12 du code de la santé publique précité, afin que seuls les professionnels effectivement impliqués dans la prise en charge d'un patient ou dans les soins qui lui sont prodigués puissent avoir accès aux informations couvertes par le secret médical.

En outre, il est recommandé de prévoir des mesures de confidentialité renforcées pour certains dossiers particuliers (par exemple, les dossiers de patients provenant d'un établissement pénitentiaire).

Les habilitations accordées peuvent être complétées d'un mode « bris de glace », défini par le référentiel d'authentification des acteurs de santé de la PGSSI-S comme *« l'attribution temporaire et exceptionnelle de droits étendus en situation de crise »*, permettant aux agents administratifs et professionnels de santé, en cas d'urgence, d'avoir accès à d'autres données pour tout patient. L'utilisation de ce mode « bris de glace » doit être particulièrement bien tracé et surveillé afin que toute personne y ayant recours puisse être identifiée et justifier des conditions de son utilisation.

Le paramétrage d'un DPI ne permettant pas de limiter le recours en mode « bris de glace » aux situations exceptionnelles est susceptible de constituer un manquement à l'article 32 du RGPD.

CNIL, P, 26 avril 2024, Mise en demeure, Centre hospitalier régional X, n° MED 2024-056, non publié

Envoi de courriels à un ensemble de destinataires – Utilisation de la fonction « copie carbone invisible » (Cci) – Obligation - Appréciation en fonction des circonstances de l'envoi

En application de l'article 32 du RGPD, il appartient au responsable de traitement d'assurer la sécurité des traitements de données à caractère personnel qu'il effectue. A ce titre, le responsable de traitement doit veiller à la confidentialité des données qu'il traite en prenant des mesures raisonnables pour éviter leur divulgation ou communication à des tiers qui n'ont pas à en connaître. En particulier, s'agissant de l'envoi d'un courriel à un ensemble de destinataires, le responsable de traitement doit s'interroger sur le point de savoir si chaque personne à qui le courriel est adressé peut ou non avoir connaissance de l'ensemble des destinataires. Pour porter cette appréciation, qui doit être faite en fonction des circonstances de l'envoi, notamment l'objet du courriel ainsi que le nombre et la qualité des destinataires, il y a lieu de tenir compte du fait que la communication en « copie carbone» (Cc) entraînera aussi la divulgation à des tiers de l'adresse électronique de chacun des destinataires. Lorsqu'il apparaît que le nom ou l'adresse électronique des destinataires ne doivent pas être visibles par tous, l'expéditeur du message est tenu d'utiliser la fonction « copie carbone invisible» (Cci). Dans certains cas, il peut être approprié de mettre un destinataire en Cci tout en indiquant dans le corps du courriel à quelles personnes il a été envoyé, s'il est pertinent que les destinataires aient cette information.

CNIL, P, 23 avril 2024, Rappel aux obligations légales, société X, n° ROL 2024-049, non publié

---

1) Mot de passe –Utilisation du NIR – Comme moyen d'identification des personnes – Licéité – En tant que mot de passe sécurisé – Illicéité en principe - 2) Risque de divulgation des adresses postales à partir du NIR

1) La CNIL considère que le numéro d'identification des personnes au répertoire national d'identification des personnes physiques (NIR, ou « numéro de sécurité sociale ») peut constituer un moyen d'identification des personnes sur des systèmes informatiques mais ne devrait pas être utilisé comme un secret pour l'authentification. Le NIR était déjà considéré comme un secret faiblement robuste, du fait de son caractère en partie dicté par certaines caractéristiques de la personne (sexe, date de naissance etc.) ; le contexte de violations massives de données comprenant ce numéro en 2024, associé au nom et au prénom des personnes concernées, ne fait que renforcer cette position.

2) En l'espèce, projet d'utilisation du NIR pour vérifier l'adresse postale dont dispose l'administration. Bien que le ministère ait précisé que l'usager devra également valider un test captcha afin de limiter l'accès à la plateforme par des systèmes automatisés d'aspiration de données en ligne, ce qui limite le risque d'atteinte massive aux données des électeurs, le système initialement étudié laisse courir un risque de divulgation des adresses postales à un tiers qui disposerait du NIR d'une personne. Or la CNIL rappelle que l'adresse postale est un élément qui doit pouvoir rester confidentiel et protégé si la personne le souhaite (notamment si elle a fait opposition aux annuaires). Dans certains contextes (violences familiales en particulier), il est indispensable que cette confidentialité soit fortement assurée. La CNIL a donc recommandé la modification du projet.

CNIL, SP, 11 avril 2024, Demande d'avis relative à un projet de décret modifiant les conditions d'organisation du scrutin destiné à mesurer l'audience des organisations syndicales auprès des salariés des entreprises de moins de onze salariés

---

Caractère suffisant des mesures de sécurité – Fonction de hachage SHA-1 – Possible manquement aux obligations de l'article 32 du RGPD

Le recours à la fonction SHA-1 pour le hachage des mots de passe n'est plus considéré comme conforme à l'état de l'art, ainsi qu'il ressort en particulier du guide de sélection d'algorithmes cryptographiques édité par l'ANSSI, en date du 8 mars 2021, qui indique que celle-ci est " proscrite pour une utilisation générale ". En l'état actuel de la technique, la CNIL a établi des recommandations spécifiques dans son guide au profit des développeurs, en recommandant de stocker les mots de passe "sous forme de hachage (hash) au moyen d'une librairie éprouvée, comme Argon2, yescrypt, scrypt, balloon, bcrypt et, dans une moindre mesure, PBKDF2". En conséquence, l'utilisation en l'espèce d'une fonction obsolète pour procéder au hachage des mots de passe est en principe constitutive d'un manquement aux obligations de l'article 32 du RGPD.

CNIL, FR, 29 décembre 2023, Sanction, Société X, n° SAN-2023-023, publié

Sécurité des logiciels – Obligation d'utiliser une version suivie intégrant les correctifs de sécurité – Version d'un logiciel n'étant plus suivie – Utilisation temporaire – Admissibilité selon la sensibilité des données traitées et les risques encourus par les personnes

Tout logiciel doit en principe être utilisé dans une version permettant encore de recevoir et d'intégrer les correctifs de sécurité, fournis par un éditeur compétent. L'utilisation d'une version d'un logiciel qui n'est plus suivie par le ou les éditeurs compétents ne peut constituer qu'une situation temporaire, en attendant une adaptation des systèmes internes du responsable de traitement à une montée de

version du logiciel ou un transfert vers un autre logiciel. L'admissibilité de l'utilisation temporaire d'une version non suivie d'un logiciel dépend de la sensibilité des données traitées et des risques encourus par les personnes.

CNIL, P, 6 avril 2023, Mise en demeure, Société X, n°MED-2023-019, non publié

Caractère suffisant des mesures de sécurité – 1) Critères d'appréciation – 2) Exigences de robustesse des mots de passe – Mesure de sécurité complémentaire

1) Il résulte des dispositions de l'article 32 du RGPD que le responsable de traitement est tenu de s'assurer que le traitement automatisé de données qu'il met en œuvre est suffisamment sécurisé. Le caractère suffisant des mesures de sécurité s'apprécie, d'une part, au regard des caractéristiques du traitement et des risques qu'il induit, d'autre part, en tenant compte de l'état de connaissances et du coût des mesures. La mise en place d'une politique d'authentification robuste constitue une mesure élémentaire de sécurité qui participe généralement au respect des obligations de l'article 32 du RGPD.

2) La Commission recommande que, pour satisfaire aux exigences de robustesse des mots de passe et assurer un niveau de sécurité suffisant, lorsque l'authentification repose, comme en l'espèce, sur un identifiant et un mot de passe, sans mise en place d'une mesure de sécurité complémentaire, le mot de passe comporte au minimum douze caractères et contienne au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial. À défaut, la Commission recommande qu'un mot de passe comporte au moins huit caractères, contenant trois des quatre catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux), à condition qu'il s'accompagne d'une mesure de sécurité complémentaire afin d'assurer un niveau de sécurité et de confidentialité suffisant.

CNIL, FR, 30 novembre 2022, Sanction, Société X, n° SAN-2022-022, publié, points 55, 57

Caractère suffisant des mesures de sécurité – Critères d'appréciation – Politique d'authentification robuste – Stockage – Fonction de hachage MD5 – Possible manquement aux obligations de l'article 32 du RGPD

Le responsable de traitement est tenu de s'assurer que le traitement automatisé de données qu'il met en œuvre est suffisamment sécurisé. Le caractère suffisant des mesures de sécurité s'apprécie d'une part, au regard des caractéristiques du traitement et des risques qu'il induit, d'autre part, en tenant compte de l'état de connaissances et du coût des mesures. La mise en place d'une politique d'authentification robuste constitue une mesure élémentaire de sécurité qui participe généralement au respect des obligations de l'article 32 du RGPD. Ainsi, il est nécessaire de veiller à ce qu'un mot de passe permettant de s'authentifier sur un système ne puisse pas être divulgué. Le recours à la fonction de hachage MD5 pour stocker des mots de passe n'est plus considéré comme à l'état de l'art depuis 2004. Son utilisation en cryptographie ou en sécurité est susceptible de constituer un manquement aux obligations de l'article 32 du RGPD.

CNIL, FR, 24 novembre 2022, Sanction, Société X, n° SAN-2022-021, publié, point 62

Système de journalisation

Dans le cadre d'un décret précisant les modalités et les conditions de recevabilité de la saisine d'une institution par voie de pétition et définissant les règles relatives à l'accès aux informations collectées, la mise en place d'un système de journalisation, permettant de conserver une trace des opérations de consultation, création et modification des données est indispensable, conformément à la délibération de la CNIL n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation.

En particulier, une durée de conservation des journaux de six à douze mois est préconisée, et ces journaux doivent faire l'objet d'un contrôle automatique régulier, afin de détecter les comportements anormaux et de générer des alertes le cas échéant. Le traitement proactif de ces journaux est d'autant plus pertinent que les données relatives à une pétition ont vocation à être traitées rapidement et peuvent conduire à des prises de décisions significatives pour l'institution et la société.

Si aucune disposition du RGPD n'impose effectivement de prévoir un système de journalisation dans l'acte réglementaire créant le traitement, le fait de le prévoir dans le décret oblige l'administration à le mettre en place et constitue une garantie importante. Il est d'ailleurs à noter que de nombreux décrets et arrêtés réglementant des traitements de données à caractère personnel le prévoient.

CNIL, P, 17 février 2022, Avis sur projet de décret, CESE, n° 2022-023, publié, point 15

Signalements dans un fichier par des zones de texte libre – Garantie possible pour compenser les risques induits par ces zones – Impossibilité de rechercher dans le fichier à partir des mots dans les signalements

Lors que l'enregistrement de signalements dans un fichier est possible par le biais de zones de texte libre pouvant conduire à enregistrer des données variées et parfois sensibles, il est recommandé d'assurer qu'il ne soit pas possible d'effectuer des recherches dans le fichier à partir des mots rédigés dans ces signalements, afin de limiter les mésusages possibles de ces données.

CNIL, P, 17 février 2022, Avis sur projet de décret, n° 2022-021, non publié

Transmission en clair d'un mot de passe permanent – Manquement à l'article 32 RGPD

La transmission, en clair, d'un mot de passe qui n'est ni temporaire, ni à usage unique et dont le renouvellement n'est pas imposé, le rend aisément et immédiatement utilisable par un tiers qui aurait un accès indu au message qui le contient. Ce tiers pourrait ainsi accéder à toutes les données à caractère personnel présentes dans le compte utilisateur de la personne concernée. Le fait que le mot de passe soit en lui-même robuste et que les personnes soient incitées à modifier leur mot de passe ne suffit pas à compenser ces risques, qui peuvent notamment entraîner des usurpations d'identité et des tentatives d'hameçonnage. Ces faits sont susceptibles de caractériser un manquement aux obligations de sécurité résultant de l'article 32 du RGPD.

CNIL, FR, Sanction, 28 décembre 2021, Société X, n°SAN-2021-021, publié, point 104

Mesures appropriées pour assurer la confidentialité des données – 1) Information des utilisateurs du système et contrôle de l'usage aux moyens de journaux de connexion – 2) Gestion des habilitations

En application de l'article 32 du RGPD, le responsable de traitement doit mettre en place des mesures appropriées pour assurer la confidentialité des données et éviter que les données soient traitées de façon illicite par le fait de personnes qui n'ont pas besoin d'en connaître.

1) La prévention des mésusages et des violations de données peut être en partie assurée par des mesures organisationnelles, notamment en informant les utilisateurs du système d'information sur les données qu'ils sont autorisés à traiter pour leurs missions, et en contrôlant l'usage qui en est fait, par exemple aux moyens de journaux de connexion.

2) En complément de ces mesures, la gestion des habilitations à consulter ou à utiliser un système d'information doit tendre à limiter les accès aux seules données à caractère personnel dont un utilisateur a besoin pour l'accomplissement de ses missions.

CNIL, FR, 29 octobre 2021, Sanction, X, n° SAN-2021-019, publié, point 62

Identifiant spécifique et distinct de l'identifiant national pour la mise en œuvre d'un traitement spécifique – Limitation des risques de réidentification des personnes en cas de fuite de données

Dans le cadre d'un projet de décret autorisant la mise en œuvre par le ministère de l'éducation nationale d'un traitement ayant pour finalité d'améliorer la prise en charge et le parcours scolaire des élèves à besoins éducatifs particuliers, de mieux individualiser les réponses pédagogiques et de garantir aux familles la mise en place d'adaptations pédagogiques dès le repérage de difficultés d'apprentissage, la CNIL considère que la création et l'utilisation d'un identifiant spécifique et distinct de l'identifiant national élève (INE) permettra, conformément à sa doctrine, de segmenter les traitements afin d'éviter des interconnexions ou rapprochements de données qui ne sont pas nécessaires, et de limiter les risques de réidentification des personnes en cas de fuite de données.

CNIL, P, 15 juillet 2021, Avis sur projet de décret, Livret de parcours inclusif (LPI), n° 2021-082, publié, point 16

Caractérisation du manquement à l'obligation de sécurité du traitement – 1) L'absence de violation de données ne suffit pas à démontrer l'absence de manquement à l'article 32 du RGPD. – 2) Appréciation des mesures techniques et organisationnelles mises en œuvre par le responsable de traitement ou le sous-traitant

L'absence de violation de données à caractère personnel ne suffit pas à démontrer l'absence de manquement aux obligations de sécurité résultant de l'article 32 du RGPD, pas plus qu'une violation de données ne suffit à caractériser en soi un manquement. Il appartient à la formation restreinte de vérifier que le responsable de traitement ou, le cas échéant, le sous-traitant, a mis en œuvre, en application de cet article, des mesures techniques et organisationnelles appropriées pour prévenir les risques de violations et de mésusage de ces données.

Le caractère approprié des mesures s'apprécie en vérifiant que le mis en cause a proportionné ces mesures, en l'état des informations dont il pouvait disposer par des diligences raisonnables, à la gravité et à la probabilité des risques prévisibles, en fonction de la nature et du contexte du traitement de données, ainsi que du coût et de la complexité des mesures possibles.

CNIL, FR, 14 juin 2021, Sanction, Société X, n° SAN-2021-008, publié, point 15

2.9 Violations de données

2.9.1 Notification à l'autorité de contrôle

Obligation du responsable du traitement de notifier à la CNIL une violation de données à caractère personnel (art. 33) – Portée

Il résulte du paragraphe 1 de l'article 33 du règlement (UE) 2016/679 du 27 avril 2016 (RGPD) que l'obligation de notifier à la Commission nationale de l'informatique et des libertés (CNIL) une violation de données à caractère personnel susceptible de faire naître un risque pour les droits et libertés des personnes physiques ne s'impose pas au responsable du traitement dans le cas où la CNIL l'a elle-même informé de cette violation et a engagé son contrôle sur la base des informations portées à sa connaissance par ailleurs.

CE, 10ème-9ème chambres réunies, 22 juillet 2022, M. D... C..., n°449694, T., point 4

2.9.2 Notification à la personne concernée

2.10 Protection des données dès la conception et par défaut

2.10.1 Dès la conception

Enregistrement de signalements dans un fichier – Zones de texte libre – Limitation des mésusages

Lorsque l'enregistrement de signalements dans un fichier est possible par le biais de zones de texte libre pouvant conduire à enregistrer des données variées et parfois sensibles, il est recommandé d'assurer qu'il ne soit pas possible d'effectuer des recherches dans le fichier à partir des mots rédigés dans ces signalements, afin de limiter les mésusages possibles de ces données.

CNIL, P, 17 février 2022, Avis sur projet de décret, n° 2022-021, non publié

Mesures techniques et organisationnelles pour ne plus traiter les données suite à une demande de résiliation d'une ligne téléphonique

Cas d'une personne ayant souscrit une ligne téléphonique principale et une ligne téléphonique secondaire dans le cadre d'un abonnement téléphonique et qui résilie seulement la ligne principale/secondaire.

Si l'information qu'une personne a été titulaire d'une ligne mobile résiliée peut effectivement être conservée à des fins d'exécution du contrat et à des fins comptables, ou encore pour la gestion du contentieux, il n'est en revanche pas nécessaire de continuer à traiter cette information, et notamment le numéro de la ligne résiliée, dans le cadre de l'émission des facturations en cours, et de la faire apparaître sur ces dernières, alors que l'utilisation d'un identifiant permettant d'identifier le débiteur des différentes lignes mobiles (principales et secondaires) peut être mobilisée à la place. Il appartient au responsable du traitement de prévoir, dès la conception, des mesures organisationnelles et techniques pour ne plus traiter ces données dans ce cadre à la suite d'une demande de résiliation d'une ligne principale par la personne concernée.

CNIL, FR, Sanction, 28 décembre 2021, Société X, n°SAN-2021-021, publié, point 94

2.10.2 Par défaut

Recours à un symbole couramment utilisé en informatique pour un usage inhabituel – Méconnaissance du principe de protection des données par défaut

Le paramétrage par défaut d'une application prévoyant qu'elle n'est pas quittée lorsque la fenêtre principale est fermée en cliquant sur un « X » en haut à droite, mécanisme qui permet généralement de quitter un logiciel, et conduisant à ce que des données à caractère personnel de l'utilisateur puissent être communiquées à des tiers sans qu'il en ait nécessairement conscience, méconnaît les exigences de l'article 25, paragraphe 2, du RGPD qui impose la protection des données par défaut.

CNIL, FR, 10 novembre 2022, Sanction, Société X, n° SAN-2022-020, publié, points 62-63

2.11 Conditions de licéité du traitement de catégories particulières de données

2.11.1 Données manifestement rendues publiques

1) Consultation par un utilisateur d'un réseau social d'un site internet ou d'une application en rapport avec des données sensibles – Collecte de données insérées par les utilisateurs et par des interfaces intégrées, des cookies ou autres – Mise en relation desdites données avec le compte du réseau social de l'utilisateur – Traitement portant sur des catégories particulières de données – 2) Consultation de sites internet ou d'applications en lien avec une ou des catégories particulières de données – Données collectées par des cookies ou des technologies d'enregistrement – Données manifestement rendues publiques – Exclusion – 3) Données insérées sur des sites internet, des applications ou lors de l'activation de boutons – Données manifestement rendues publiques – Inclusion uniquement dans les cas où l'utilisateur a explicitement exprimé son choix au préalable

1) L'article 9, paragraphe 1, du règlement 2016/679 doit être interprété en ce sens que dans le cas où un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs des catégories visées à cette disposition et, le cas échéant, y insère des données en s'inscrivant ou en effectuant des commandes en ligne, le traitement de données à caractère personnel par l'opérateur de ce réseau social en ligne, consistant en la collecte, au moyen d'interfaces intégrées, de cookies ou de technologies d'enregistrement similaires, des données issues de la consultation de ces sites et de ces applications ainsi que des données insérées par l'utilisateur, en la mise en relation de l'ensemble de ces données avec le compte du réseau social de celui-ci et en l'utilisation desdites données par cet opérateur, doit être considéré comme un « traitement portant sur des catégories particulières de données à caractère personnel », au sens de ladite disposition, qui est en principe interdit, sous réserve des dérogations prévues à cet article 9, paragraphe 2, lorsque ce traitement de données permet de révéler des informations relevant d'une de ces catégories, que ces informations concernent un utilisateur de ce réseau ou toute autre personne physique.

2) L'article 9, paragraphe 2, sous e), du règlement 2016/679 doit être interprété en ce sens que lorsqu'un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs des catégories visées à l'article 9, paragraphe 1, de ce règlement, il ne rend pas manifestement publiques, au sens de la première de ces dispositions, les données relatives à cette consultation, collectées par l'opérateur de ce réseau social en ligne à travers des cookies ou des technologies d'enregistrement similaires.

3) Lorsqu'il insère des données dans de tels sites Internet ou dans de telles applications ou lorsqu'il active des boutons de sélection intégrés à ces sites et à ces applications, tels que les boutons « j'aime » ou « partager » ou les boutons permettant à l'utilisateur de s'identifier sur ces sites ou ces applications en utilisant les identifiants de connexion liés à son compte d'utilisateur du réseau social, son numéro de téléphone ou son adresse électronique, un tel utilisateur ne rend manifestement publiques, au sens de cet article 9, paragraphe 2, sous e), les données ainsi insérées ou résultant de l'activation de ces boutons que dans le cas où il a explicitement exprimé son choix au préalable, le cas échéant sur la base d'un paramétrage individuel effectué en toute connaissance de cause, de rendre les données le concernant publiquement accessibles à un nombre illimité de personnes.

CJUE, grande chambre, 4 juillet 2023, Meta Platforms e.a., C-252/21, point 85

Conditions de licéité de l'exploitation par l'administration fiscale de données librement accessibles sur les plateformes en ligne – Réserve du Conseil constitutionnel en l'espèce sur la notion de données librement accessibles

Expérimentation autorisant les administrations fiscales et douanières à collecter et exploiter les contenus librement accessibles sur les sites internet des opérateurs de plateformes en ligne et manifestement rendus publics par leurs utilisateurs.

Le Conseil d'État rappelle qu'en vertu de la décision du Conseil constitutionnel n°2019-796 DC du 17 décembre 2019 les sites ou les plateformes dont les données ne sont accessibles qu'après inscription ou saisie d'un mot de passe ne peuvent donner lieu à collecte et exploitation. Il précise en outre que les commentaires rédigés par des tiers et relatifs au titulaire du compte ne peuvent faire l'objet d'aucune exploitation.

Le Conseil d'État écarte des dispositions permettant :

- de collecter des contenus qui ne seraient accessibles qu'après inscription tout en précisant que la création de comptes est possible aux seules fins de pouvoir collecter de façon automatique des contenus autrement accessibles sans inscription préalable,
- la collecte et l'exploitation des commentaires figurant sur les pages des utilisateurs de plateformes.

CE, Assemblée générale (section des finances), 24 septembre 2020, Avis n°400911, Projet de loi de finances pour 2021

Les exceptions prévues à l'article 9 du RGPD ont vocation à s'appliquer non seulement aux traitements relevant du RGPD mais aussi aux traitements relevant du seul titre Ier de la loi Informatique et Libertés

En vertu de l'article 6 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés, le traitement des données sensibles n'est possible, sauf disposition législative spéciale l'autorisant, que s'il s'inscrit dans le cadre de l'une des exceptions prévues à l'article 9 du RGPD ou, s'agissant de traitements relevant du champ d'application des articles 31 et 32 de la loi Informatique et Libertés (en particulier le champ d'application de la directive « Police-Justice » et les traitements intéressant la sûreté et la défense nationale), s'il est autorisé selon les modalités prévues à ces articles, à savoir un décret en Conseil d'État après avis de la CNIL.

Il y a lieu d'interpréter le titre Ier de la loi Informatique et Libertés de façon à ce que ses dispositions ne portent pas une atteinte disproportionnée à des droits ou objectifs de valeur constitutionnelle. Dès lors, il est nécessaire de lire la loi de sorte que les traitements ne relevant que du titre Ier puissent bénéficier de certaines exceptions à l'interdiction de traiter des données sensibles, notamment pour les données manifestement rendues publiques, pour les traitements d'intérêt public, ou en cas de consentement de la personne. Le renvoi aux exceptions de l'article 9 du RGPD opéré par l'article 6 de la loi Informatique et Libertés doit être entendu comme ayant vocation à s'appliquer non seulement aux traitements relevant du RGPD mais aussi aux traitements relevant des autres titres, et notamment ceux relevant du seul titre Ier.

Cette question ne se pose que pour le titre Ier dès lors que, pour les traitements du titre III (directive « Police-Justice »), la loi a prévu des dispositions spéciales, transposant la directive sur ce point et que, pour ceux du titre IV, tous les traitements relèveront du champ des articles 31 et 32 et seront autorisés par décret en Conseil d'État.

CNIL, P, 17 février 2022, Avis sur projet de décret, n° 2022-021, non publié

Réseaux sociaux – Paramétrage de confidentialité des comptes – Caractère public des données traitées dans le cadre d'une communauté d'intérêts fermées – Absence

La possibilité offerte aux utilisateurs d'un réseau social de paramétrer la confidentialité de leurs comptes ne confère pas un caractère public à leurs données dès lors que celles-ci sont traitées dans le cadre d'une communauté d'intérêts fermée et accessible à ses seuls membres.

CNIL, FR, 27 avril 2017, Sanction, Sociétés X et Y, n° SAN-2017-006, publié, point 128

2.11.2 Données révélant les convictions religieuses

Candidature d'adhésion à un organisme ayant une finalité religieuse – Contacts réguliers – Licéité du traitement

Les personnes envoyant une candidature, avec les pièces requises, pour adhérer à un organisme ayant une finalité politique, philosophique ou religieuse doivent être assimilées à des personnes entretenant des contacts réguliers avec cet organisme au sens de l'article 9.2.d) du RGPD. L'organisme peut dès lors traiter licitement les données sensibles contenues dans la candidature, sur ce fondement ou celui du consentement, pour examiner et statuer sur la candidature. En cas de rejet de la candidature, il doit supprimer les données sensibles.

CNIL, P, 6 juillet 2021, Courrier présidente, SA 211064, non publié

2.11.3 Données de santé

Traitement de données concernant la santé fondé sur l'article 9, paragraphe 2, sous h) du RGPD – Double condition de licéité – Respect des exigences de l'article 9, paragraphe 2, sous h) et de l'article 6, paragraphe 1 du RGPD

L'article 9, paragraphe 2, sous h), et l'article 6, paragraphe 1, du règlement 2016/679 doivent être interprétés en ce sens qu'un traitement de données concernant la santé fondé sur cette première disposition doit, afin d'être licite, non seulement respecter les exigences découlant de celle-ci, mais aussi remplir au moins l'une des conditions de licéité énoncées à cet article 6, paragraphe 1.

CJUE, 21 décembre 2023, Krankenversicherung Nordrhein, C-667/21

Vigilance dans la communication des données de nature médicale

Le droit au respect de la vie privée requiert que soit observée une particulière vigilance dans la communication des données à caractère personnel de nature médicale.

CC, 2021-917 QPC,11 juin 2021, Union nationale des syndicats autonomes de la fonction publique, point 3

Droit d'accès aux documents administratifs - Communication à un tiers d'un registre de contention et d'isolement avec occultation des éléments permettant d'identifier les patients et les soignants, mais sans occultation des identifiants " anonymisés " des patients – Atteinte à la protection de la vie privée et du secret médical – Illicéité

Demande de communication d'un registre de contentieux et d'isolement au titre du droit d'accès aux documents administratifs. Dans le cas où l'identité des patients a fait l'objet d'une pseudonymisation, laquelle ne permet l'identification des personnes en cause qu'après recoupement d'informations, il appartient au juge administratif d'apprécier si, eu égard à la sensibilité des informations en cause et aux efforts nécessaires pour identifier les personnes concernées, leur communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. En l'espèce, compte tenu de la nature des informations en cause, qui touchent à la santé mentale des patients, et du nombre restreint de personnes pouvant faire l'objet d'une mesure de contention et d'isolement, facilitant ainsi leur identification, alors au demeurant que les autorités énumérées à la dernière phrase du deuxième alinéa de l'article L. 3222-5-1 du code de la santé publique peuvent accéder à l'ensemble des informations figurant sur les registres et contrôler l'activité des établissements concernés, l'identifiant dit " anonymisé " figurant dans ces registres, qu'il s'agisse, selon la pratique du centre hospitalier, de " l'identifiant permanent du patient " (IPP) ou d'un identifiant spécialement défini, doit être regardé comme une information dont la communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. Cet identifiant n'est donc communicable qu'au seul intéressé en vertu des dispositions de l'article L. 311-6 du code des relations entre le public et l'administration.

CE, 10ème chambre, 22 mars 2024, Centre hospitalier Le Vinatier, n°471369, Inédit, point 6

Dossiers Patients Informatisés - Equipe médicale – Notion - Accès – Politique d'habilitation – Critères

En application des articles L.1110-4 et L.1110-12 du code de la santé publique et de la Politique générale de sécurité des systèmes d'information de santé élaborée par l'Agence du Numérique en Santé (PGSSI-S), le responsable de traitement d'un dispositif de dossiers patients informatisés (DPI) doit mettre en place une politique d'habilitation rigoureuse et adaptée aux besoins de l'établissement, de sorte que chaque professionnel de santé et agent de l'établissement n'accède qu'aux dossiers dont il a à connaître. Cette politique d'habilitation doit combiner deux critères :

- d'une part, le métier exercé : ainsi, un agent responsable de l'accueil des patients dans la structure ne doit accéder qu'au dossier administratif du patient et non aux données médicales, alors qu'un médecin accèdera également aux données médicales ;
- d'autre part, la prise en compte de la notion d'équipe de soins, telle que définie par l'article L. 1110-12 du code de la santé publique précité, afin que seuls les professionnels effectivement impliqués dans la prise en charge d'un patient ou dans les soins qui lui sont prodigués puissent avoir accès aux informations couvertes par le secret médical.

En outre, il est recommandé de prévoir des mesures de confidentialité renforcées pour certains dossiers particuliers (par exemple, les dossiers de patients provenant d'un établissement pénitentiaire).

Les habilitations accordées peuvent être complétées d'un mode « bris de glace », défini par le référentiel d'authentification des acteurs de santé de la PGSSI-S comme *« l'attribution temporaire et exceptionnelle de droits étendus en situation de crise »*, permettant aux agents administratifs et professionnels de santé, en cas d'urgence, d'avoir accès à d'autres données pour tout patient. L'utilisation de ce mode « bris de glace » doit être particulièrement bien tracé et surveillé afin que toute personne y ayant recours puisse être identifiée et justifier des conditions de son utilisation.

Le paramétrage d'un DPI ne permettant pas de limiter le recours en mode « bris de glace » aux situations exceptionnelles est susceptible de constituer un manquement à l'article 32 du RGPD.

CNIL, P, 26 avril 2024, Mise en demeure, Centre hospitalier régional X, n° MED 2024-056, non publié

Motifs d'intérêt public dans le domaine de la santé publique

Application StopCovid – Absence de méconnaissance du droit au respect de la vie privée et du RGPD –Absence d'atteinte au secret médical – Poursuite de l'objectif de protection de la santé publique

Le projet de décret vise à permettre la mise en œuvre d'une application informatique, dénommée « StopCovid », qui pourra être téléchargée sur les téléphones mobiles et qui permettra d'informer les utilisateurs de ces téléphones du fait qu'ils ont été à proximité de personnes diagnostiquées positives au virus du covid-19 via la technologie « Bluetooth ». Ni les personnes dépistées, ni les cas contacts ne sont identifiés, les utilisateurs de l'application ne disposent que de très peu d'informations les concernant et le projet de décret consacre le caractère libre et volontaire du téléchargement et de l'utilisation de l'application.

Eu égard à l'objectif de protection de la santé publique poursuivi, le décret ne méconnait pas ni le droit au respect de la vie privée ni le RGPD. En particulier, la durée du traitement, fixée à six mois après la fin de l'état d'urgence sanitaire, de même que la durée de conservation de l'historique de proximité des utilisateurs, fixée à quinze jours à compter de l'émission des données, paraissent adaptées.

Le Conseil d'État estime en outre que ce projet ne porte pas atteinte au secret médical garanti par l'article L. 1110-4 du code de la santé publique, lequel ne s'impose qu'aux professionnels.

En revanche, le Conseil d'État émet un avis défavorable à une disposition prévoyant que le téléchargement et l'utilisation de l'application ne peuvent donner lieu à des avantages ou droits spécifiques qui seraient refusés aux personnes n'ayant pas téléchargé ou n'utilisant pas l'application et qu'aucun tiers ne peut obliger une personne à utiliser l'application, ni exercer un droit de regard sur l'existence de l'application ou son contenu, dès lors que ces dispositions édictent des interdictions, notamment applicables aux relations entre personnes privées, qui relèvent des principes fondamentaux des obligations civiles et commerciales dont la détermination est réservée au législateur par l'article 34 de la Constitution.

Toutefois, des limites sont posées par la législation en vigueur à des pratiques consistant pour des personnes privées à subordonner des droits ou avantages à l'utilisation de cette application.

CE, Section sociale, 26 mai 2020, Avis n° 400231, Projet de décret autorisant la mise en œuvre d'un traitement de données dénommé « StopCovid »

Données sensibles – Traitement automatisé de données à caractère personnel relatif aux pensions d'invalidité – Intérêt public autorisant le traitement des données relatives à la santé – Existence – Respect du secret médical – Existence

Un décret autorise la mise en œuvre, par le ministère de la défense d'un traitement automatisé de données à caractère personnel ayant pour finalités, d'une part, la gestion administrative des demandes de pensions d'invalidité présentées en application du code des pensions militaires d'invalidité et des victimes de la guerre et, d'autre part, la préparation et le suivi de la liquidation des dossiers des pensions attribuées au titre du même code. Ce décret, eu égard à son objet et à ses finalités, est justifié par un intérêt public et échappe ainsi, en application du IV de l'article 8 de la loi n°78-17 du 6 janvier 1978, à l'interdiction de collecte et de traitement des données à caractère personnel relatives à la santé prévue par le I du même article. Compte tenu des dispositions de l'article 5 de la loi n°55-356 du 3 avril 1955, qui autorisent la communication de renseignements médicaux ou de pièces médicales susceptibles de faciliter l'instruction d'une demande de pension aux services

administratifs chargés de l'instruction des demandes, dont les agents sont eux-mêmes tenus au secret professionnel, le décret n'a par lui-même et ne pourrait d'ailleurs avoir légalement ni pour objet ni pour effet d'autoriser les services du ministère de la défense à accéder à des données personnelles relatives à la santé dans des conditions dérogeant aux exigences de protection du secret médical garanti par les dispositions de l'article L. 1110-4 du code de la santé publique.

CE, 10ème/9ème SSR, 15 octobre 2014, Union nationale du personnel en retraite de la gendarmerie et autres, n°358876, T., point 11

Conditions de mise en œuvre

Contrôle administratif des congés d'invalidité – Transmission d'informations médicales – Atteinte disproportionnée au droit au respect de la vie privée en l'espèce

Des dispositions légales encadrant la transmission, aux services administratifs compétents et aux fins de vérification des conditions encadrant le congé pour invalidité temporaire imputable au service, de données de nature médicale relatives à des agents publics, portent une atteinte disproportionnée au droit au respect de la vie privée dès lors qu'elles répondent aux conditions suivantes : la transmission de ces données intervient sans recueillir préalablement le consentement des agents intéressés et sans que le secret médical puisse être opposé aux services administratifs qui en font la demande ; cette communication peut concerner un très grand nombre d'agents au sein des services administratifs concernés, dont la désignation n'est subordonnée à aucune habilitation spécifique et dont les demandes de communication ne sont soumises à aucun contrôle particulier ; les renseignements en cause peuvent être obtenus auprès de toute personne ou organisme.

CC, 2021-917 QPC,11 juin 2021, Union nationale des syndicats autonomes de la fonction publique, points 5-10

Médecins et secrétaires médicaux, tenus au secret professionnel, ayant accès aux données médicales de patients enregistrées par d'autres médecins dans le cadre d'un système d'information commun – Absence de qualification de tiers non autorisés

Attendu qu'il est notamment reproché aux prévenus, du chef du délit prévu par les articles 42 ancien de la loi n°78-17 du 6 janvier 1978, et 226-17 du code pénal, d'avoir, jusqu'en 1994, mis en place un système permettant à chacun des médecins utilisateurs et à leurs secrétaires d'accéder aux informations d'ordre médical figurant dans les fichiers créés par les autres médecins ;

Attendu que, pour relaxer les prévenus à raison de ces faits, la cour d'appel retient à raison que les médecins appartenant au syndicat interprofessionnel des médecins du travail du pays d'Aix (SIMTPA) et leurs secrétaires médicales, tenus au secret professionnel, ne peuvent être considérés comme des tiers non autorisés au sens des articles 29 de la loi Informatique et Libertés et 226-17 du code pénal.

Cass, crim., 30 octobre 2001, n° 99-82.136, Inédit., points 3-4

Secret médical (art. L. 1110-4 du CSP) – Accès aux données du dossier médical des patients – 1) Accès des commissaires aux comptes – Méconnaissance, en tant que ne sont pas prévues des mesures techniques et organisationnelles propres à garantir le respect du secret médical – 2) Accès des prestataires extérieurs – Illégalité, en tant qu'il

n'est pas assorti de garanties suffisantes pour assurer que l'accès n'excède pas celui strictement nécessaire à l'exercice de leur mission

Décret n° 2018-1254 du 26 décembre 2018 prévoyant l'accès des commissaires aux comptes, dans le cadre de leur mission légale de certification des comptes des établissements publics de santé, et de prestataires extérieurs, aux fins de traitement des données, aux données du dossier médical des patients, lesquelles portent sur l'identité du patient, son lieu de résidence, ses pathologies et les actes de diagnostic et de soins réalisés au cours de son séjour dans l'établissement.

1) Il résulte de l'article L. 823-9 du code de commerce que les commissaires aux comptes doivent seulement, pour l'accomplissement de leur mission légale de certification des comptes des établissements publics de santé, être en mesure de justifier que les comptes annuels de ces établissements sont réguliers et sincères et donnent une image fidèle du résultat des opérations de l'exercice écoulé ainsi que de leur situation financière et de leur patrimoine.

Il ressort des pièces du dossier, notamment des observations de caractère général présentées par le Haut Conseil du commissariat aux comptes (H3C) en application de l'article R. 625-3 du code de justice administrative, que l'accès à l'ensemble des données de santé, issues du dossier médical des patients, mentionnées à l'article R. 6113-1 du code de la santé publique (CSP), est nécessaire à l'accomplissement de cette mission, pour un échantillon de dossiers permettant de vérifier par sondage la fiabilité et la traçabilité des données utilisées pour le calcul des recettes de l'établissement, depuis l'admission du patient jusqu'à la facturation.

En revanche, il n'en ressort pas que cette mission ne puisse être accomplie à partir de données faisant l'objet de mesures de protection techniques et organisationnelles adéquates, telles que - à défaut du recours, à titre d'expert, à un médecin responsable de l'information médicale dans un autre établissement - la pseudonymisation des données, dont l'article 25 du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD) prévoit la mise en œuvre pour protéger les droits de la personne concernée et garantir, à cette fin, que les personnes dont les données sont traitées ne puissent être identifiées.

Par suite, si le décret attaqué a pu, sans méconnaître la portée de l'article L. 6113-7 du CSP, pour encadrer les conditions dans lesquelles les commissaires aux comptes ont accès à ces données, se borner, d'une part, à prévoir qu'ils peuvent seulement les consulter, dans le cadre de leur mission légale, sans création ni modification de données, avec une information adaptée des patients, en en limitant la conservation à la durée strictement nécessaire à cette mission et en rappelant l'obligation de secret à laquelle ils sont soumis et, d'autre part, à limiter leur accès aux seules données « nécessaires (...) dans la stricte limite de ce qui est nécessaire à leurs missions », sans exclure par principe leur accès à aucune de ces données, il est en revanche entaché d'illégalité en tant qu'il ne prévoit pas de mesures techniques et organisationnelles propres à garantir la protection du droit de la personne concernée au respect du secret médical rappelé par l'article L. 1110-4 du CSP.

2) En se bornant à prévoir que les prestataires extérieurs qui contribuent au traitement des données à caractère personnel mentionnées à l'article R. 6113-1 du CSP sont placés sous la responsabilité du médecin responsable de l'information médicale, qu'ils interviennent dans le cadre de leur contrat de sous-traitance, qu'ils sont soumis à l'obligation de secret, dont la méconnaissance est punie conformément aux articles 226-13 et 226-14 du code pénal, qu'ils peuvent accéder « aux seules données à caractère personnel nécessaires (...) dans la stricte limite de ce qui est nécessaire à leurs missions » et qu'ils ne peuvent conserver les données mises à disposition par l'établissement au-delà de la durée strictement nécessaire aux activités qui leur ont été confiées par contrat, sans prévoir de mesures techniques et organisationnelles propres à assurer que seules sont traitées, avec des garanties suffisantes, les données identifiantes qui sont nécessaires au regard des finalités du traitement ni de dispositions destinées à garantir qu'ils accomplissent effectivement ces activités sous l'autorité du praticien responsable de l'information médicale, quel qu'en soit le lieu, le décret attaqué n'a pas prévu de garanties suffisantes pour assurer que l'accès aux données n'excède pas celui qui est strictement nécessaire à l'exercice de la mission qui leur est reconnue par la loi.

CE, 1ère-4ème chambres réunies, 25 novembre 2020, Conseil national de l'ordre des médecins, n° 428451, T., points 10, 13

2.11.4 Données biométriques

Législation nationale prévoyant la conservation par les autorités de police, à des fins de prévention et de détection des infractions pénales de données à caractère personnel, y compris biométriques et génétiques, concernant des personnes ayant fait l'objet d'une condamnation pénale définitive jusqu'au décès de ces personnes - Inconventionnalité

L'article 4, paragraphe 1, sous c) et e), de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, lu en combinaison avec les articles 5 et 10, l'article 13, paragraphe 2, sous b), ainsi que l'article 16, paragraphes 2 et 3, de celle-ci, et à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'il s'oppose à une législation nationale qui prévoit la conservation, par les autorités de police, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, de données à caractère personnel, notamment de données biométriques et génétiques, concernant des personnes ayant fait l'objet d'une condamnation pénale définitive pour une infraction pénale intentionnelle relevant de l'action publique, et ce jusqu'au décès de la personne concernée, y compris en cas de réhabilitation de celle-ci, sans mettre à la charge du responsable du traitement l'obligation de vérifier régulièrement si cette conservation est toujours nécessaire, ni reconnaître à ladite personne le droit à l'effacement de ces données, dès lors que leur conservation n'est plus nécessaire au regard des finalités pour lesquelles elles ont été traitées, ou, le cas échéant, à la limitation du traitement de celles-ci.

CJUE, 30 janvier 2024, NG c./ Direktor na Glavna direktsia « Natsionalna politsia » pri Ministerstvo na vatreshnite raboti – Sofia, C-118/22

Directive (UE) 2016/680 Police-justice – 1) Article 6, sous a) (Distinction claire entre les données à caractère personnel de différentes catégories de personnes) Procédure d'exécution forcée de la collecte de données biométriques – Admissibilité - Conditions – 2) Article 4, paragraphe 1, sous a) à c) (Traitement de données biométriques et de données génétiques) - Notion de « nécessité absolue » - Caractère systématique de la collecte – Illicéité

1) L'article 6, sous a) (distinction entre les différentes catégories de personnes concernées), de la directive 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données ainsi que les articles 47 et 48 de la charte des droits fondamentaux de l'Union européenne doivent être interprétés en ce sens qu'ils ne s'opposent pas à une législation nationale qui prévoit que, en cas de refus de la personne mise en examen pour une infraction intentionnelle poursuivie d'office, de coopérer spontanément à la collecte des données biométriques et génétiques la concernant aux fins de leur enregistrement, la juridiction pénale compétente est tenue d'autoriser une mesure d'exécution forcée de cette collecte, sans disposer du pouvoir d'apprécier s'il existe des motifs sérieux de considérer que la personne concernée a commis l'infraction pour laquelle elle est mise en examen, pour autant que le droit national garantisse ultérieurement le contrôle juridictionnel effectif des conditions de cette mise en examen, dont découle l'autorisation de procéder à ladite collecte.

2) L'article 10 de la directive 2016/680 (traitement de catégories particulières de données), lu en combinaison avec l'article 4, paragraphe 1, sous a) à c), ainsi qu'avec l'article 8, paragraphes 1 et 2, de

cette directive, doit être interprété en ce sens qu'il s'oppose à une législation nationale qui prévoit la collecte systématique des données biométriques et génétiques de toute personne mise en examen pour une infraction intentionnelle poursuivie d'office aux fins de leur enregistrement, sans prévoir l'obligation, pour l'autorité compétente, de vérifier et de démontrer, d'une part, si cette collecte est absolument nécessaire à la réalisation des objectifs concrets poursuivis et, d'autre part, si ces objectifs ne peuvent pas être atteints par des mesures constituant une ingérence de moindre gravité pour les droits et les libertés de la personne concernée.

CJUE, 26 janvier 2023, Ministerstvo na vatreshnite raboti, C-205/21

Garantir dans la législation que les données biométriques ne seront pas utilisées ou conservées à des fins autres que la délivrance du passeport ou du document de voyage – Absence d'obligation pesant sur les États membres

L'article 4, paragraphe 3, du règlement n° 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres n'oblige pas les États membres à garantir, dans leur législation, que les données biométriques rassemblées et conservées conformément audit règlement ne seront pas rassemblées, traitées et utilisées à des fins autres que la délivrance du passeport ou du document de voyage, un tel aspect ne relevant pas du champ d'application dudit règlement.

CJUE, 16 avril 2015, Willems e.a, C-446/12 à C-449/12, point 53

Prélèvement d'empreintes digitales – Protection des passeports contre une utilisation frauduleuse – Proportionnalité

Il n'a pas été porté à la connaissance de la Cour l'existence de mesures susceptibles de contribuer, de manière suffisamment efficace, au but tenant à la protection des passeports contre leur utilisation frauduleuse, tout en portant des atteintes moins importantes aux droits reconnus par les articles 7 et 8 de la Charte que celles entraînées par la méthode fondée sur les empreintes digitales. Ce recueil est donc proportionné.

CJUE, 17 octobre 2013, Schwarz, C-291/12, point 53

Recours à la reconnaissance faciale en temps réel à des fins de prévention des infractions pénales – Mesures particulièrement intrusives en l'espèce et traitement de données sensibles – Manifestation d'opinions politiques – Inconventionnalité

Dans une jurisprudence constante, la Cour EDH juge que la conservation de photographies par la police, combinée à la possibilité de leur appliquer des techniques de reconnaissance faciale, constitue une ingérence dans l'exercice du droit à la vie privée. La Cour rappelle également qu'il est essentiel, dans le cadre de la mise en œuvre de la technologie de reconnaissance faciale, de disposer de règles détaillées régissant la portée et l'application des mesures ainsi que de garanties solides contre le risque d'abus et d'arbitraire. La nécessité de disposer de garanties est d'autant plus grande lorsque la technologie de reconnaissance faciale est utilisée en temps réel.

En l'espèce, le requérant russe qui a manifesté pacifiquement dans le métro moscovite, et dont des photographies et une vidéo ont été publiées sur un canal public de Telegram, a été identifié à partir de ces éléments, localisé puis interpellé, au moyen d'une technologie de reconnaissance faciale en temps réel.

Partant du principe selon lequel les mesures litigieuses poursuivaient le but légitime de la prévention des infractions pénales, la Cour estime que les mesures prises contre le requérant ont été particulièrement intrusives, surtout le recours à la technologie de reconnaissance faciale en temps réel. Un niveau élevé de justification est donc nécessaire pour qu'elles puissent être considérées comme « nécessaires dans une société démocratique », le niveau de justification le plus élevé étant

requis pour l'utilisation de cette technologie. De plus, les données à caractère personnel qui ont été traitées renfermant des informations sur la participation du requérant à une manifestation pacifique, elles ont par conséquent révélé les opinions politiques de l'intéressé. Elles appartenaient donc aux catégories particulières de données sensibles qui appellent un niveau de protection accru.

Le droit interne russe autorisait le traitement des données biométriques à caractère personnel dans le cadre de l'enquête et des poursuites engagées pour toute infraction, quelles qu'en fussent la nature et la gravité.

Le requérant a été poursuivi pour une infraction administrative mineure qui n'a représenté aucun risque pour l'ordre public ou la sécurité des transports. Il n'a pas été accusé d'avoir commis un acte répréhensible au cours de sa manifestation. L'utilisation d'une technologie de reconnaissance faciale très intrusive pour identifier et arrêter les participants à des actions de protestation pacifiques pourrait produire un effet dissuasif dans le domaine des droits à la liberté d'expression et de réunion.

Dans ces conditions, le traitement des données à caractère personnel du requérant au moyen de la technologie de reconnaissance faciale dans le cadre de la procédure administrative, ne répondait pas à un « besoin social impérieux » et ne pouvait être considéré comme « nécessaire dans une société démocratique ». La Cour EDH conclut donc à une violation de l'article 8.

CEDH, 4 octobre 2023, Glukhin c. Russie, n°11519/20

Conservation pendant cinq ans des photographies, du signalement et des empreintes digitales et palmaires d'un récidiviste subordonnée à des garanties et à un contrôle individualisé – Absence de violation de l'article 8 CEDH

Le recueil et la conservation de divers types de données personnelles s'analysent en une ingérence dans le droit du requérant au respect de sa vie privée. La prise d'empreintes palmaires, en particulier, constitue une mesure qui, sur le plan de son intensité et de l'utilisation future éventuelle des données recueillies, est très similaire à celle de la prise d'empreintes digitales. Par conséquent, les mêmes considérations doivent s'appliquer. Il y a lieu de considérer que le signalement du requérant et son enregistrement dans les fichiers de la police aux fins d'une identification future sont comparables à la prise d'une photographie, quoique moins intrusifs. L'article 8 est donc de même applicable à cette mesure. L'ingérence litigieuse était conforme à la loi et avait pour objectif la prévention du crime ainsi que la protection des droits d'autrui en facilitant les enquêtes relatives à de futures infractions.

La mesure litigieuse ménageait un juste équilibre entre des intérêts publics et privés concurrents et relève donc de la marge d'appréciation de l'État défendeur.

Pour apprécier la proportionnalité de l'ingérence, il est important que le recueil et la conservation des données d'identification dont il est question en l'espèce – photographies, empreintes digitales et palmaires et signalement – aient constitué une ingérence moins intrusive que le recueil d'échantillons cellulaires et la conservation de profils ADN, qui contiennent des informations beaucoup plus sensibles.

En ce qui concerne la durée de la conservation des données d'identification en question, le droit interne pertinent prévoit des délais précis au terme desquels la nécessité de conserver les données doit être réexaminée. L'objet de la conservation ainsi que le type et l'importance du motif de la conservation doivent être pris en compte dans cette appréciation. Dans une affaire comme celle du requérant – un délinquant adulte dont les infractions ne sont ni mineures ni particulièrement graves selon la définition de la directive applicable – la règle veut que les données personnelles soient supprimées au bout de cinq ans en l'absence d'ouverture d'une nouvelle enquête pénale visant le requérant dans ce délai. Le requérant peut donc obtenir la suppression de ses données dans les fichiers de police si son comportement démontre que les données ne sont plus nécessaires au travail de la police. La présente affaire se distingue par conséquent d'affaires telles que *S. et Marper et Gaughran c. Royaume-Uni*, qui concernaient la conservation de données pour une durée

indéterminée, ou *M.K. c. France*, dans laquelle il avait été constaté qu'en pratique, les données étaient conservées pendant vingt-cinq ans.

En outre, en l'espèce, la nécessité de conserver les données en question peut faire l'objet d'un réexamen – par la police, susceptible de contrôle juridictionnel. Rien n'indique que les données d'identification sont insuffisamment protégées contre des abus tels qu'un accès ou une diffusion non autorisés.

Au vu du degré relativement limité de l'intrusion et de la durée du recueil des données d'identification en question, de l'effet limité sur la vie quotidienne du requérant de la conservation des données dans une base de données interne de la police et de la présence de garanties, la mesure litigieuse constituait une ingérence proportionnée dans le droit du requérant au respect de sa vie privée.

CEDH, 11 juin 2020, Affaire P.N c Allemagne, n°74440/17

Conservation, sans limitation de durée et sans possibilité de réexamen de la situation, du profil ADN, des empreintes digitales et de la photographie d'une personne reconnue coupable d'une infraction mineure – Caractère disproportionné – Violation de l'article 8 CEDH

Etaient conservés, sans limitation de durée et sans possibilité de réexamen, le profil ADN, les empreintes digitales et la photographie du requérant qui avait été reconnu coupable de conduite en état d'ivresse en Irlande du Nord et dont la condamnation avait été rayée de son casier judiciaire à l'expiration du délai prévu par la loi.

La Cour EDH a conclu à la violation de l'article 8 de la Convention.

La conservation du profil ADN et des empreintes digitales du requérant s'analyse en une atteinte à son droit au respect de sa vie privée. La conservation des données biométriques et des photographies poursuivait un but légitime, à savoir la prévention des infractions pénales.

Les États jouissent d'une marge d'appréciation réduite lorsqu'ils sont appelés à fixer des limites concernant la conservation des données biométriques de personnes ayant été condamnées. Néanmoins, la durée de conservation de ces données ne constitue pas nécessairement un critère déterminant lorsqu'il s'agit de rechercher si un État a outrepassé sa marge d'appréciation en la matière. La question de savoir si les règles mises en place tiennent compte de la gravité de l'infraction commise et de la nécessité de conserver les données en question et si des garanties effectives ont été mises en place revêt également de l'importance. Lorsqu'un État se place aux confins de sa marge d'appréciation en s'attribuant le pouvoir le plus étendu en matière de conservation des données, c'est-à-dire le pouvoir de conserver des données sans limitation de durée, l'existence de certaines garanties effectives devient déterminante.

Les autorités ont conservé les données biométriques et la photographie du requérant sans prendre en considération ni la gravité de l'infraction commise ni la nécessité de conserver ces données sans limitation de durée. En outre, la police n'avait le pouvoir d'effacer les données biométriques et les photographies de personnes reconnues coupables que dans des cas exceptionnels. Par ailleurs, aucune disposition ne permettait au requérant de présenter une demande d'effacement si la conservation des données le concernant n'apparaissait plus pertinente compte tenu de la finalité du fichier, au regard de la nature de l'infraction qu'il avait commise, de son âge lors de sa commission, du temps écoulé depuis lors et de sa personnalité actuelle. En conséquence, il apparaît que les possibilités de réexamen étaient tellement restreintes qu'elles en devenaient presque hypothétiques.

Le caractère indifférencié des pouvoirs de conservation du profil ADN, des empreintes digitales et de la photographie du requérant au motif qu'il avait été reconnu coupable d'une infraction, entre-temps radiée de son casier judiciaire, sans examen de la gravité de l'infraction commise ni de la nécessité de conserver indéfiniment les données en question, et sans possibilité réelle de réexamen de la mesure litigieuse, n'a pas ménagé un juste équilibre entre les intérêts publics et privés concurrents en jeu. L'État jouissait d'une marge d'appréciation légèrement plus ample en ce qui concerne la conservation des empreintes digitales et des photographies. Néanmoins, cette marge d'appréciation n'était pas suffisamment ample pour que la conservation des données concernées puisse être considérée comme proportionnée compte tenu des circonstances de la cause, et notamment de l'absence de garanties suffisantes, et plus particulièrement de l'absence de possibilité réelle de réexamen de la mesure litigieuse.

L'État défendeur a donc outrepassé la marge d'appréciation acceptable à cet égard. Partant, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique.

CEDH, 13 février 2020, Affaire Gaughran c. Royaume-Uni, n°45245/15

Drones – Interdiction législative de procéder à de la reconnaissance faciale sur les images – Portée

En application du deuxième alinéa de l'article L. 242-4 du code de la sécurité intérieure, les dispositifs aéroportés ne peuvent procéder à la captation du son, ni comporter de traitements automatisés de reconnaissance faciale. Ces dispositifs aéroportés ne peuvent procéder à aucun rapprochement, interconnexion ou mise en relation automatisée avec d'autres traitements de données à caractère personnel. Toutefois, ces dispositions ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient pas placés sur ces dispositifs aéroportés.

CC, 2021-834 DC, 20 janvier 2022, Loi relative à la responsabilité pénale et à la sécurité intérieure, point 30

Traitement destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage – Disproportionnalité au regard de l'objet, de la sensibilité des données, de sa possible interrogation à d'autres fins – Inconstitutionnalité

La création d'un traitement de données à caractère personnel destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage permet de sécuriser la délivrance de ces titres et d'améliorer l'efficacité de la lutte contre la fraude. Elle est ainsi justifiée par un motif d'intérêt général.

Toutefois, compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française. Les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles. Les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne. Les dispositions de la loi relative à la protection de l'identité autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de

renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire.

Il résulte de ce qui précède qu'eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi. Par suite, les articles 5 et 10 de la loi relative à la protection de l'identité doivent être déclarés contraires à la Constitution.

CC, 2012-652 DC,22 mars 2012, Loi relative à la protection de l'identité, points 8-11

Nécessité absolue d'un dispositif de reconnaissance faciale déployé à des fins policières – Conditions

L'enregistrement dans un traitement automatisé de données à caractère personnel d'une photographie de personnes mises en cause comportant les données biométriques nécessaires à la mise en œuvre d'un dispositif de reconnaissance faciale et permettant aux agents habilités d'identifier une personne à partir de l'image de son visage via une recherche automatisée pour les finalités mentionnées à l'article 230-6 du code de procédure pénale tel que le prévoit l'article R. 40-26 alinéa 16 de ce code répond à la condition de nécessité absolue posée par l'article 88 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés une telle identification et le rapprochement avec les données enregistrées dans le traitement pouvant s'avérer absolument nécessaires à la recherche des auteurs d'infractions et à la prévention des atteintes à l'ordre public.

CE, 10ème chambre, 26 avril 2022, La Quadrature du Net, n°442364, Inédit., point 5

2.11.5 Données relatives aux mineurs

Protection des mineurs sur internet – 1) Objectif d'intérêt général pouvant justifier des dispositifs de contrôle automatisé – Exigence de proportionnalité – 2) Cas des dispositifs de contrôle parental – a) Proportionnalité en principe – Protection des données dès la conception et par défaut – b) Recommandation de fonctionnement uniquement en local sur les terminaux du ménage

1) La protection des mineurs sur internet, eu égard aux risques spécifiques auxquels ils sont exposés (pédophilie, harcèlement, arnaques…) et à la facilité d'accès à des contenus inadaptés constitue un objectif d'intérêt général. Cette protection passe par de nombreux canaux, au premier rang desquels figure l'éducation au numérique, à laquelle diverses autorités publiques, dont la CNIL, contribuent.

La mise en place de dispositifs de contrôle automatisé constitue un moyen pertinent pour assurer cette protection. Cependant, la CNIL souligne, d'une part, qu'ils doivent s'inscrire dans le cadre d'une action plus globale de sensibilisation, d'éducation et de protection de la jeunesse dans ses usages numériques ; d'autre part, que ces dispositifs peuvent impliquer la collecte de données personnelles et une forme de surveillance des mineurs, et qu'un équilibre doit donc être trouvé entre ce contrôle et le respect de leur vie privée et de leur autonomie. Parmi les dispositifs de contrôle automatisé, la CNIL a recommandé, à de nombreuses reprises, de favoriser l'usage de dispositifs à la main des utilisateurs plutôt que de solutions centralisées ou qui leur soient imposées.

2) a) Le développement de dispositifs de contrôle parental, qui conduit à une responsabilisation du ménage pour limiter l'accès à des contenus sensibles par les mineurs, semble particulièrement respectueuse des droits des individus. Ces outils doivent être développés dans le respect d'une approche de protection des données dès la conception et par défaut, consacrée par le RGPD.

b) La CNIL recommande de configurer les dispositifs de contrôle parental de sorte que, par défaut, pour les fonctionnalités de base, ils fonctionnent sans entraîner de remontée de données à caractère personnel vers des serveurs ou sans qu'il soit nécessaire de créer un compte sur un serveur. Une telle configuration est distincte des opérations d'authentification ou de création de comptes utilisateurs pouvant être requises afin d'utiliser le terminal et qui peuvent nécessiter une liaison avec un serveur distant.

CNIL, SP, 9 mars 2023, Avis sur deux projets de décret, Loi n°2022-030 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet, n°2023-023, publié, points 4, 5, 24

Traitement visant à améliorer la prise en charge et le parcours scolaire des élèves à besoins éducatifs particuliers – Contrat de sous-traitance – Interdiction de transférer les données en dehors de l'Union européenne

Dans le cadre d'un projet de décret autorisant la mise en œuvre par le ministère de l'éducation nationale d'un traitement ayant pour finalité d'améliorer la prise en charge et le parcours scolaire des élèves à besoins éducatifs particuliers, dont des élèves handicapés, compte tenu des données traitées, de la minorité d'un grand nombre de personnes concernées par le traitement, du cadre dans lequel elles sont recueillies et du considérant 38 du RGPD qui indique que « les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel », la CNIL considère que le contrat de sous-traitance devrait prévoir l'interdiction de transférer les données en dehors de l'Union européenne.

CNIL, P, 15 juillet 2021, Avis sur projet de décret, Livret de parcours inclusif (LPI), n° 2021-082, publié, point 29

2.11.6 Données d'infraction

Traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes – Loi adaptant la législation nationale au RGPD – 1) Poursuite d'objectifs d'intérêt général – 2) Champ des personnes autorisées suffisamment restreint – Mise en œuvre encadrée – Conformité

Les dispositions contestées modifient l'article 9 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin de fixer le régime des traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes, lorsque ces traitements ne sont pas mis en œuvre par les autorités compétentes à des fins pénales au sens de la directive européenne du 27 avril 2016.

1) En premier lieu, d'une part, en adoptant ces dispositions, le législateur a entendu permettre la mise en œuvre de traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes par des personnes collaborant au service public de la justice, telles que des associations d'aide aux victimes ou d'accompagnement de personnes placées sous main de justice. Il a également entendu ouvrir cette faculté aux personnes victimes ou mises en cause dans une procédure pénale, afin de leur permettre de préparer ou de mettre en œuvre un recours en justice. Ce faisant, le législateur a poursuivi des objectifs d'intérêt général.

2) En second lieu, d'une part, en prévoyant qu'elles s'appliquent aux personnes morales de droit privé collaborant au service public de la justice appartenant à des catégories dont la liste est fixée par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, ainsi qu'aux personnes agissant soit en tant que victimes ou mises en cause soit pour le

compte de ces dernières, les dispositions contestées circonscrivent suffisamment le champ des personnes ainsi autorisées à mettre en œuvre un traitement de données à caractère personnel en matière pénale. D'autre part, la mise en œuvre de ces traitements ne peut être effectuée, dans le premier cas, que dans la mesure strictement nécessaire à la mission exercée par la personne collaborant au service public de la justice et, dans le second, que pour une durée strictement proportionnée aux finalités poursuivies par les personnes victimes ou mises en cause. Dans ce dernier cas, la communication à un tiers n'est possible que sous les mêmes conditions et dans la mesure strictement nécessaire à la poursuite des mêmes finalités. Enfin, la mise en œuvre de ces traitements de données est subordonnée au respect des garanties prévues par le règlement européen du 27 avril 2016, en particulier les conditions posées à ses articles 5 et 6, et à celles prévues par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le législateur, qui n'était pas tenu de prévoir un dispositif d'autorisation préalable des traitements de données en cause, n'a donc pas méconnu le droit au respect de la vie privée.

CC, 2018-765 DC,12 juin 2018, Loi relative à la protection des données personnelles, points 41-42, 47-53

Autorisation donnée à des personnes privées de traiter de données à caractère personnel relatives à des infractions pour repérer des contrefaçons en ligne – Licéité – Condition – Limitation à la protection des droits des victimes

Les dispositions combinées de l'article L. 34-1 du code des postes et des communications électroniques, tel qu'il est modifié par l'article 14 de la loi favorisant la diffusion et la protection de la création sur internet et des troisième et cinquième alinéas de l'article L. 331-21 du code de la propriété intellectuelle et de son article L. 331-24, tels qu'ils résultent de l'article 5 de cette loi, ont pour effet de modifier les finalités en vue desquelles des personnes privées peuvent mettre en œuvre des traitements portant sur des données relatives à des infractions. Elles permettent en effet que, désormais, les données recueillies relatives aux infractions de contrefaçon commises sur internet acquièrent un caractère nominatif non seulement dans le cadre d'une procédure judiciaire, mais également dans le cadre de la procédure conduite devant la commission de protection des droits de la haute autorité pour la diffusion des œuvres et la protection des droits sur internet.

À la suite de la censure résultant des considérants 19 et 20 de sa décision, le Conseil constate que la commission de protection des droits ne peut prononcer les sanctions prévues par la loi déférée : seul un rôle préalable à une procédure judiciaire lui est confié. Une telle intervention est justifiée par l'ampleur des contrefaçons commises au moyen d'internet et l'utilité, dans l'intérêt d'une bonne administration de la justice, de limiter le nombre d'infractions dont l'autorité judiciaire sera saisie. Il en résulte que les traitements de données à caractère personnel mis en œuvre par les sociétés et organismes précités ainsi que la transmission de ces données à la commission de protection des droits pour l'exercice de ses missions s'inscrivent dans un processus de saisine des juridictions compétentes.

En outre, ces traitements seront soumis aux exigences prévues par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Les données ne pourront être transmises qu'à cette autorité administrative ou aux autorités judiciaires. Il appartiendra à la Commission nationale de l'informatique et des libertés, saisie pour autoriser de tels traitements, de s'assurer que les modalités de leur mise en œuvre, notamment les conditions de conservation des données, seront strictement proportionnées à cette finalité.

CC, 2009-580 DC,10 juin 2009, Loi favorisant la diffusion et la protection de la création sur internet, points 24-29

Mesure d'identification d'une adresse IP par le juge sur le fondement de l'article 145 du code de procédure civile – Communication nécessaire à l'exercice ou à la défense d'un droit en justice – Licéité – Conditions

Hors des conditions prévues par le code des postes et des communications électroniques (saisie d'adresse IP pour la recherche, la constatation et la poursuite d'infractions pénales) et la loi pour la confiance dans l'économie numérique (qui ne s'applique pas aux correspondances privées que sont des courriels anonymes adressés à des personnes identifiées), une mesure à fin d'identification d'une adresse IP peut être ordonnée par un juge, sur le fondement de l'article 145 du code de procédure civile, selon lequel s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé.

Une telle mesure peut être regardée comme légalement admissible lorsque la communication à un tiers d'une adresse IP est nécessaire à l'exercice ou à la défense d'un droit en justice, qu'elle ne porte pas une atteinte disproportionnée au droit à la vie privée de la personne dont les données sont ainsi communiquées à un tiers et qu'enfin, ce tiers fasse de ces données un usage licite.

Cass, 2e civ., 23 juin 2021, n°18-18.824, Inédit., points 8-9

Constatations visuelles effectuées sur internet et renseignements – Propriété intellectuelle – Contrefaçons – Exclusion

Ne constituent pas un traitement de données à caractère personnel relatives à des infractions, au sens des articles 2, 9 et 25de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les constatations visuelles effectuées sur internet et les renseignements recueillis en exécution de l'article L. 331-2 du code de la propriété intellectuelle par un agent assermenté qui, sans recourir à un traitement préalable de surveillance automatisé, utilise un appareillage informatique et un logiciel de pair à pair, pour accéder manuellement, aux fins de téléchargement, à la liste des œuvres protégées irrégulièrement proposées sur la toile par un internaute, dont il se contente de relever l'adresse IP pour pouvoir localiser son fournisseur d'accès en vue de la découverte ultérieure de l'auteur des contrefaçons.

Cass, crim., 13 janvier 2009, n°08-84.088, B., point 6

2.11.7 Traitement du NIR

Transmission du NIR pour un répertoire des logements locatifs sociaux et de leurs habitants – Mise en œuvre de la politique d'attribution des logements – Objectif d'intérêt général – Modalités de collecte, d'enregistrement, de conservation, et de communication adéquates et proportionnées – Conformité

L'article L. 411-10 du code de la construction et de l'habitation prévoit que le ministère chargé du logement tient un répertoire des logements locatifs sociaux et de leurs habitants, pour permettre l'élaboration et la mise en œuvre des politiques publiques de l'habitat.

Le c du 1° du paragraphe I de l'article 78 de la loi relative à l'égalité et à la citoyenneté complète cet article L. 411-10. Il prévoit que, pour alimenter ce répertoire, les bailleurs sociaux transmettent au ministère chargé du logement le numéro d'immatriculation au répertoire national d'identification des personnes physiques de chaque occupant majeur d'un logement locatif social.

En adoptant les dispositions contestées, le législateur a entendu que le ministère chargé du logement soit en mesure d'établir une cartographie de l'occupation socio-économique du parc de logements

sociaux, afin d'améliorer la mise en œuvre de la politique en matière d'attribution de ces logements. Il a ainsi poursuivi un objectif d'intérêt général.

Si les collectivités territoriales et certains de leurs établissements publics peuvent obtenir du représentant de l'État dans la région les informations relatives aux logements situés sur leur territoire contenues dans le répertoire, c'est, en vertu du huitième alinéa de l'article L. 411-10, à la condition que ces informations aient été préalablement rendues anonymes.

Par ailleurs, le législateur a prévu au 4° du paragraphe I de l'article 78 que l'exploitation des données du répertoire par le groupement d'intérêt public mentionné à l'article L. 441-2-1 du code de la construction et de l'habitation est réalisée de manière à rendre impossible l'identification des intéressés.

Il en résulte que le législateur a retenu des modalités de collecte, d'enregistrement, de conservation, et de communication du numéro d'immatriculation au répertoire national d'identification des personnes physiques adéquates et proportionnées à l'objectif poursuivi. Par conséquent, le grief tiré de la méconnaissance du droit au respect de la vie privée doit être écarté.

CC, 2016-745 DC, 26 janvier 2017, Loi relative à l'égalité et à la citoyenneté, points 22-23, 26-29

« Base nationale des identifiants élèves » – Identifiant de portée générale – Exclusion

En raison de son champ sectoriel, la « base nationale des identifiants élèves » ne peut être regardée comme un identifiant de portée générale au sens de l'article 8 de la directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

CE, 10ème/9ème SSR, 18 novembre 2015, M. A...C... et Mme B...D..., n° 384869, Rec., point 5

2.11.8 Données de connexion

1) Législation nationale prévoyant une obligation extrêmement large de conservation de toutes les communications Internet de tous les utilisateurs – Violation de l'article 8 CEDH – 2) Accès direct aux communications sans présentation d'une autorisation d'interception aux fournisseurs de services – Absence de garanties adéquates et suffisantes contre les abus liés à l'accès des autorités répressives aux communications Internet et aux données de communication connexes stockées – 3) Obligation légale de déchiffrer les communications cryptées de bout en bout – Disproportion

1) La législation contestée exige la conservation et le stockage automatiques et continus du contenu de toutes les communications Internet (communications vocales, textuelles, visuelles, sonores, vidéo ou d'autres communications électroniques) pendant une durée de six mois et des données de connexion correspondantes pendant une durée d'un an. Elle concerne tous les utilisateurs, même en l'absence de soupçon raisonnable de participation à des activités criminelles ou à des activités mettant en danger la sécurité nationale, ou de toute autre raison de penser que la conservation des données peut contribuer à la lutte contre les formes graves de criminalité ou à la protection de la sécurité nationale. Il n'y a aucune limitation du champ d'application de la mesure en termes d'application territoriale ou temporelle ou de catégories de personnes susceptibles de voir leurs données à caractère personnel conservées. La Cour conclut que l'ingérence est exceptionnellement étendue et grave. La législation ne peut être considérée comme nécessaire dans une société démocratique et porte atteinte à l'essence même du droit au respect de la vie privée garanti par l'article 8 de la Convention. L'État défendeur a donc outrepassé toute marge d'appréciation acceptable à cet égard.

2) Contrairement à la législation en cause qui prévoit un accès direct aux communications Internet par les services de sécurité sans autorisation judiciaire préalable, la Cour recommande une obligation de présenter une autorisation au fournisseur de services de communication avant d'obtenir l'accès aux communications d'une personne en ce qu'elle constitue une garantie importante contre les abus des autorités répressives, en veillant à ce qu'une autorisation en bonne et due forme soit obtenue dans tous les cas de surveillance secrète.

3) L'obligation légale de déchiffrer les communications chiffrées de bout en bout risque d'équivaloir à une obligation pour les fournisseurs de tels services d'affaiblir le mécanisme de chiffrement pour tous les utilisateurs et n'est donc pas proportionnée aux buts légitimes poursuivis.

CEDH, 13 février 2024, Podchasov c. Russie, n°33696/19, points 70, 73 et 79

Article 15, paragraphe 1, directive 2002/58/CE – 1) Législation permettant l'accès d'autorités publiques aux données de trafic et de localisation – Prévention, recherche, détection, poursuite d'infractions pénales – Illicéité en l'absence de limitation à certaines procédures – 2) Réglementation donnant compétence au ministère public pour autoriser l'accès d'une autorité publique aux données de trafic et de localisation – Illicéité

L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, (directive vie privée et communications électroniques), lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens :

> 1) qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période ;
> 2) qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale.

CJUE, grande chambre, 2 mars 2021, Prokuratuur, C-746/18

Directive 2002/58 – 1) Champ d'application – Réglementation nationale imposant aux fournisseurs de services de communications électroniques de transmettre des données relatives au trafic et à la localisation aux services de sécurité et de renseignement – Objectif de protection de la sécurité nationale – Inclusion – 2) Faculté pour les États membres de limiter la portée de certains droits et obligations – Réglementation nationale imposant aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et à la localisation aux services de sécurité et de renseignement – Objectif de protection de la sécurité nationale – Inadmissibilité

1) L'article 1er, paragraphe 3, l'article 3 et l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lus à la lumière de l'article 4, paragraphe 2, TUE, doivent être interprétés en ce sens que relève du champ d'application de cette directive une réglementation nationale permettant à une autorité étatique d'imposer aux fournisseurs de services de communications électroniques de transmettre aux services de sécurité et de renseignement des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale.

2) L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement.

CJUE, grande chambre, 6 octobre 2020, Privacy International, C-623/17

Accès aux données visant à l'identification des titulaires des cartes SIM – Finalité de lutte contre tout type d'infraction – Atteinte proportionnée à la vie privée

L'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

CJUE, grande chambre, 2 octobre 2018, Ministerio Fiscal, C-207/16

Réglementation nationale prévoyant l'accès des autorités nationales aux données relatives au trafic et des données de localisation – Accès aux données non limités à des fins précises – Absence de contrôle préalable par une juridiction ou une autorité administrative indépendante – Absence d'exigence de conservation des données sur le territoire de l'Union – Incompatibilité avec le droit de l'Union

L'article 15, paragraphe 1, de la directive 2002/58/CE du 12 juillet 2002 s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.

CJUE, grande chambre, 21 décembre 2016, Tele2 Sverige, C-203/15 et C-698/15

Accès aux données de connexion dans le cadre de la procédure pénale – Réquisition de données de connexion à l'initiative du juge d'instruction ou d'un officier de police judiciaire autorisé par une commission rogatoire délivrée par ce magistrat –

Information judiciaire – Conciliation équilibrée entre l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et le droit au respect de la vie privée

Dans le cadre d'une instruction, les dispositions contestées autorisent le juge d'instruction ainsi que l'officier de police judiciaire à se faire communiquer des données de connexion ou à y avoir accès.

Les données de connexion comportent notamment les données relatives à l'identification des personnes, à leur localisation et à leurs contacts téléphoniques et numériques ainsi qu'aux services de communication au public en ligne qu'elles consultent. Compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée.

Toutefois, en premier lieu, en adoptant les dispositions contestées, le législateur a poursuivi l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions. En second lieu, la réquisition de données de connexion intervient à l'initiative du juge d'instruction, magistrat du siège dont l'indépendance est garantie par la Constitution, ou d'un officier de police judiciaire qui y a été autorisé par une commission rogatoire délivrée par ce magistrat. D'une part, ces dispositions ne permettent la réquisition de données de connexion que dans le cadre d'une information judiciaire, dont l'ouverture n'est obligatoire qu'en matière criminelle et pour certains délits. Si une information peut également être ouverte pour les autres infractions, le juge d'instruction ne peut informer, en tout état de cause, qu'en vertu d'un réquisitoire du procureur de la République ou, en matière délictuelle et dans les conditions prévues aux articles 85 et suivants du code de procédure pénale, à la suite d'une plainte avec constitution de partie civile. D'autre part, dans le cas où la réquisition de données de connexion est mise en œuvre par un officier de police judiciaire en exécution d'une commission rogatoire, cette commission rogatoire, datée et signée par le magistrat, précise la nature de l'infraction, objet des poursuites, et fixe le délai dans lequel elle doit être retournée avec les procès-verbaux dressés pour son exécution par l'officier de police judiciaire. Ces réquisitions doivent se rattacher directement à la répression de cette infraction et sont, conformément à l'article 152 du code de procédure pénale, mises en œuvre sous la direction et le contrôle du juge d'instruction. En outre, conformément aux articles 175–2 et 221-1 du code de procédure pénale, la durée de l'information ne doit pas, sous le contrôle de la chambre de l'instruction, excéder un délai raisonnable au regard de la gravité des faits reprochés à la personne mise en examen, de la complexité des investigations nécessaires à la manifestation de la vérité et de l'exercice des droits de la défense.

Dès lors, les dispositions contestées opèrent une conciliation équilibrée entre l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et le droit au respect de la vie privée.

CC, 2022-1000 QPC, 17 juin 2022, M. Ibrahim K., points 10-17

Accès aux données de connexion dans le cadre de la procédure pénale – Cas des enquêtes de flagrance, limitées dans le temps – Encadrement des réquisitions – Conformité au droit au respect de la vie privée

Sont déclarées conformes à la Constitution et ne méconnaissent pas le droit au respect de la vie privée des dispositions permettant au procureur de la République ou à l'officier de police judiciaire ou, sous le contrôle de ce dernier, à l'agent de police judiciaire, par tout moyen, de requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel, lorsqu'elles poursuivent l'objectif de valeur constitutionnelle de recherche des auteurs d'infraction et dès lors que d'une part, ces dispositions ne permettent les réquisitions de données que dans le cadre d'une enquête de police portant sur un crime flagrant ou un délit flagrant puni d'une peine d'emprisonnement et,

d'autre part, la durée de cette enquête est limitée à huit jours. Celle-ci ne peut être prolongée, pour une nouvelle durée maximale de huit jours, sur décision du procureur de la République, que si l'enquête porte sur un crime ou un délit puni d'une peine d'emprisonnement égale ou supérieure à cinq ans et si les investigations ne peuvent être différées.

Ces réquisitions ne peuvent intervenir qu'à l'initiative du procureur de la République, d'un officier de police judiciaire ou, sous le contrôle de ce dernier, d'un agent de police judiciaire. Ces officiers et agents étant placés sous la direction du procureur de la République, les réquisitions sont mises en œuvre sous le contrôle d'un magistrat de l'ordre judiciaire auquel il revient, en application de l'article 39-3 du code de procédure pénale, de contrôler la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits.

CC, 2022-993 QPC, 20 mai 2022, M. Lofti H, points 10-14

Droit d'obtenir communication des données de connexion conféré aux agents de la Hadopi – Objectif de sauvegarde de la propriété intellectuelle – Informations particulièrement attentatoires à la vie privée – Absence de lien direct avec le manquement – Absence de garanties propres à assurer une conciliation entre le droit au respect de la vie privée et l'objectif de sauvegarde de la propriété intellectuelle – Non-conformité

Dispositions conférant aux agents de la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi) le droit d'obtenir communication et copie des données de connexion détenues par les opérateurs de communication électronique.

En adoptant ces dispositions, le législateur a entendu renforcer la lutte contre les pratiques de contrefaçon sur internet, qui répond à l'objectif de sauvegarde de la propriété intellectuelle. En outre, ce droit de communication, qui n'est pas assorti d'un pouvoir d'exécution forcée, n'est ouvert qu'aux agents publics de la Haute autorité, dûment habilités et assermentés, qui sont soumis, dans l'utilisation de ces données, au secret professionnel. Enfin, le troisième alinéa de l'article L. 331-21 du code de la propriété intellectuelle subordonne son exercice aux nécessités de la procédure mise en œuvre par la commission de protection des droits.

Toutefois, ce droit de communication peut s'exercer sur toutes les données de connexion détenues par les opérateurs de communication électronique. Or, compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, de telles données fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée. Elles ne présentent pas non plus nécessairement de lien direct avec le manquement à l'obligation de respect du droit d'auteur et des droits voisins énoncée à l'article L. 336-3.

Il résulte de ce qui précède que, dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation qui ne soit pas manifestement déséquilibrée entre le droit au respect de la vie privée et l'objectif de sauvegarde de la propriété intellectuelle.

CC, 2020-841 QPC, 20 mai 2020, La Quadrature du Net et autres, points 9-10, 14-18

Voir aussi : CC, 2018-764 QPC, 15 février 2019, M. Paulo M., point 8 ; CC, 2017-753 DC, 8 septembre 2017, Loi organique pour la confiance dans la vie politique, points 57-59 ; CC, 2017-646/647 QPC, 21 juillet 2017, M. Alexis K. et autre, points 8-9 ; CC, 2015-715 DC, 5 août 2015, Loi pour la croissance, l'activité et l'égalité des chances économiques, points 135, 137

Sécurité sociale – Droit de communication des données de connexion des assurés sociaux reconnu aux agents des organismes de la sécurité sociale – Absence de

garanties propres à assurer une conciliation entre droit au respect de la vie privée et la lutte contre la fraude en matière de protection sociale – Non-conformité

Compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée. Par ailleurs, elles ne présentent pas de lien direct avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation. Dans ces conditions, en instaurant un tel droit de communication de données de connexion, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre le droit au respect de la vie privée et la lutte contre la fraude en matière de protection sociale.

CC, 2019-789 QPC, 14 juin 2019, Mme Hanen S., point 15

Accès en temps réel aux données de trafic et de localisation – Prévention du terrorisme – Conformité partielle

Les dispositions contestées permettent à l'autorité administrative, pour la prévention du terrorisme, d'obtenir le recueil en temps réel des données de connexion relatives, d'une part, à une personne préalablement identifiée susceptible d'être en lien avec une menace et, d'autre part, aux personnes appartenant à l'entourage de la personne concernée par l'autorisation lorsqu'il y a des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation. Cette technique de recueil de renseignement est autorisée pour une durée de quatre mois renouvelable, conformément à l'article L. 821-4 du code de la sécurité intérieure.

D'une part, le recueil des données de connexion en temps réel ne peut être mis en œuvre que pour les besoins de la prévention du terrorisme. Ne peuvent, par ailleurs, être recueillis que les informations ou documents traités ou conservés par les opérateurs de télécommunication, les fournisseurs d'accès à un service de communication au public en ligne ou les hébergeurs de contenu sur un tel service.

D'autre part, cette technique de recueil de renseignement s'exerce dans les conditions prévues au chapitre Ier du titre II du livre VIII du code de la sécurité intérieure. En vertu de l'article L. 821-4 de ce code, elle est autorisée par le Premier ministre ou les collaborateurs directs auxquels il a délégué cette compétence, sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, après avis préalable de la Commission nationale de contrôle des techniques de renseignement. Elle est autorisée pour une durée de quatre mois renouvelable. En vertu du paragraphe II de l'article L. 851-2, la procédure d'urgence absolue prévue à l'article L. 821-5 de ce code n'est pas applicable. En application de l'article L. 871-6 du même code, les opérations matérielles nécessaires à la mise en place de la technique mentionnée à l'article L. 851-2 ne peuvent être exécutées, dans leurs réseaux respectifs, que par des agents qualifiés des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications.

Enfin, cette technique de renseignement est réalisée sous le contrôle de la Commission nationale de contrôle des techniques de renseignement. La composition et l'organisation de cette autorité administrative indépendante sont définies aux articles L. 831-1 à L. 832-5 du code de la sécurité intérieure dans des conditions qui assurent son indépendance. Ses missions sont définies aux articles L. 833-1 à L. 833-11 du même code dans des conditions qui assurent l'effectivité de son contrôle. Conformément aux dispositions de l'article L. 841-1 du même code, le Conseil d'État peut être saisi par toute personne souhaitant vérifier qu'aucune technique de recueil de renseignement n'est irrégulièrement mise en œuvre à son égard ou par la Commission nationale de contrôle des techniques de renseignement.

Il résulte de ce qui précède que le législateur a assorti la procédure de réquisition des données de connexion, lorsqu'elle s'applique à une personne préalablement identifiée susceptible d'être en lien avec une menace, de garanties propres à assurer une conciliation qui n'est pas manifestement

déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public et celle des infractions et, d'autre part, le droit au respect de la vie privée.

En revanche, en application des dispositions contestées, cette procédure de réquisition s'applique également aux personnes appartenant à l'entourage de la personne concernée par l'autorisation, dont il existe des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation. Ce faisant, le législateur a permis que fasse l'objet de cette technique de renseignement un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit. Ainsi, faute d'avoir prévu que le nombre d'autorisations simultanément en vigueur doive être limité, le législateur n'a pas opéré une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le droit au respect de la vie privée.

CC, 2017-648 QPC, 4 août 2017, La Quadrature du Net et autres, points 5, 7-11

Salariés protégés – Exclusion de l'interception des communications téléphoniques et l'identification des correspondants – Examen par l'employeur des relevés de communications – Illégalité

Pour l'accomplissement de leur mission légale et la préservation de la confidentialité qui s'y attache, les salariés protégés, au nombre desquels se trouvent les membres du conseil et les administrateurs des caisses de sécurité sociale, doivent pouvoir disposer sur leur lieu de travail d'un matériel ou procédé excluant l'interception par l'employeur de leurs communications téléphoniques et l'identification de leurs correspondants.

Viole dès lors l'article L. 2411-1 13° du code du travail, ensemble les articles 6, 17 et 21 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et 7 de la délibération n° 2005-019 du 3 février 2005 de la Commission nationale de l'informatique et des libertés, la cour d'appel qui, pour débouter un salarié, administrateur de l'URSSAF, de sa demande de résiliation judiciaire de son contrat de travail, retient que l'employeur s'était contenté d'examiner les relevés des communications téléphoniques du téléphone mobile mis à disposition du salarié par l'entreprise, alors qu'il résultait de ses constatations que l'examen par l'employeur des relevés litigieux permettait l'identification des correspondants du salarié.

Cass, soc., 4 avril 2012, n°10-20.845, B., points 3-4

Annulation du refus d'abroger des dispositions réglementaires en tant qu'elles ne prévoient pas un réexamen périodique de l'existence d'une menace pour la sécurité nationale justifiant l'obligation pour les opérateurs de conserver de manière généralisée et indifférenciée les données de trafic et de localisation – 1) Injonction de compléter ces dispositions dans un délai de six mois – 2) Opérateurs pouvant se soustraire à cette obligation avant l'expiration de ce délai – Absence dans la mesure où une telle menace a été constatée par le juge

Par son arrêt du 6 octobre 2020 La Quadrature du Net et autres (C-511/18, C-512/18, C-520/18), la Cour de justice de l'Union européenne (CJUE) a dit pour droit que la directive 2002/58/CE du 12 juillet 2002 ne s'opposait pas à ce que des mesures législatives permettent, aux fins de sauvegarde de la sécurité nationale, d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de trafic et des données de localisation, sous réserve qu'une décision soumise à un contrôle effectif constate l'existence d'une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, pour une durée limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. Il ressort en outre du point 135 de cet arrêt que la responsabilité des Etats membres en matière de sécurité nationale, au sens du droit de l'Union, correspond à l'intérêt primordial de

protéger les fonctions essentielles de l'Etat et les intérêts fondamentaux de la société, et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'Etat en tant que tel, telles que notamment des activités de terrorisme.

1) Ni l'article L. 34-1 du code des postes et des communications électroniques (CPCE) ni l'article 6 de la loi n° 2004-575 du 21 juin 2004 ne prévoient un réexamen périodique, au regard des risques pour la sécurité nationale, de la nécessité de maintenir l'obligation faite aux personnes concernées de conserver les données de connexion. Ces articles, ainsi, par suite, que l'article R. 10-13 du CPCE et le décret n° 2011-219 du 25 février 2011, en tant qu'ils ne subordonnent pas le maintien en vigueur de cette obligation au constat, à échéance régulière, qui ne saurait raisonnablement excéder un an, de la persistance d'une menace grave, réelle et actuelle ou prévisible, pour la sécurité nationale sont, dans cette mesure, contraires au droit de l'Union européenne. Il résulte de ce qui précède que, s'agissant de l'objectif de sauvegarde de la sécurité nationale, le refus d'abroger l'article R. 10-13 du CPCE et l'article 1er du décret du 25 février 2011 doit être annulé en tant seulement que leurs dispositions ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, s'agissant des données qu'elles mentionnent autres que celles afférentes à l'identité civile, aux comptes et aux paiements des utilisateurs et aux adresses IP. Il y a lieu d'enjoindre au Gouvernement de compléter ces dispositions dans un délai de six mois à compter de la présente décision.

2) Il ressort des pièces du dossier que la France est, à la date de la présente décision, confrontée à une menace grave, réelle et non seulement prévisible mais actuelle pour sa sécurité nationale, appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure (CSI) qui, par son intensité, revêt un caractère grave et réel. Cette menace est, à la date de la présente décision, non seulement prévisible mais aussi actuelle. Cette menace procède d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés. Par ailleurs, la France est particulièrement exposée au risque d'espionnage et d'ingérence étrangère, en raison notamment de ses capacités et de ses engagements militaires et de son potentiel technologique et économique. La France est également confrontée à des menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes. Dans la mesure où il résulte de la présente décision que la réalité et la gravité de la menace pesant sur la sécurité nationale justifient l'obligation de conservation généralisée et indifférenciée de l'ensemble des données de connexion à cette fin, les opérateurs ne sauraient, avant l'expiration du délai de six mois laissé au Gouvernement pour compléter les dispositions litigieuses, se soustraire à cette obligation et aux sanctions dont sa méconnaissance est assortie au motif que la durée de l'injonction qui leur est faite n'a pas été limitée dans le temps par le pouvoir réglementaire.

CE, Assemblée, 21 avril 2021, French Data Network et autres, n° 393099, Rec., points 44-46

2.12 Conditions de licéité des traitements algorithmiques

Notion de décision informatisée – Calcul automatisé d'une valeur de probabilité de la solvabilité d'une personne – Inclusion – Conditions

L'article 22, paragraphe 1, du RGPD doit être interprété en ce sens que l'établissement automatisé, par une société fournissant des informations commerciales, d'une valeur de probabilité fondée sur des données à caractère personnel relatives à une personne et concernant la capacité de celle-ci à honorer des engagements de paiement à l'avenir constitue une « décision individuelle automatisée », au sens de cette disposition, lorsque dépend de manière déterminante de cette valeur de probabilité le fait qu'une tierce partie, à laquelle ladite valeur de probabilité est communiquée, établisse, exécute

ou mette fin à une relation contractuelle avec cette personne.

CJUE, 7 décembre 2023, SCHUFA Holding, C-634/21

Droit constitutionnel d'accès aux documents administratifs – Procédure de préinscription à l'entrée en premier cycle Parcoursup – Publication obligatoire à l'issue de la procédure des critères d'examen des candidatures indiquant dans quelle mesure des traitements algorithmiques ont été utilisés

Les dispositions du dernier alinéa du paragraphe I de l'article L. 612-3 du code de l'éducation ne sauraient, sans méconnaître le droit d'accès aux documents administratifs garanti par l'article 15 de la Déclaration de 1789, être interprétées comme dispensant chaque établissement d'enseignement supérieur de publier, à l'issue de la procédure nationale de préinscription à l'entrée en premier cycle et dans le respect de la vie privée des candidats, le cas échéant sous la forme d'un rapport, les critères en fonction desquels les candidatures ont été examinées et précisant, le cas échéant, dans quelle mesure des traitements algorithmiques ont été utilisés pour procéder à cet examen.

CC, 2020-834 QPC, 3 avril 2020, UNEF, point 17

Résultats d'un traitement algorithmique – Prise en compte par une juridiction parmi d'autres éléments d'appréciation – Admission

Si les dispositions de l'article 2 de la loi n°78-17 du 6 janvier 1978 font obstacle à ce qu'une juridiction saisie d'un litige dont la solution suppose l'appréciation d'un comportement humain fonde sa décision sur les seuls résultats d'un traitement automatisé d'informations, elles n'ont en revanche ni pour objet ni pour effet de lui interdire de prendre en compte, parmi d'autres éléments d'appréciation, les résultats d'un tel traitement.

CE, 4ème/5ème SSR, 4 février 2004, Caisse primaire d'assurance maladie de la Gironde, n° 240023, Rec., point 1

Déploiement de dispositifs de caméras augmentées dans l'espace public poursuivant une finalité dite « police -justice » - Interdiction en l'absence de cadre légal spécifique

L'article 4, paragraphe 1, de la loi no 78-17 du 6 janvier 1978 dispose que les données à caractère personnel doivent être « traitées de manière licite, loyale ».

Par leur fonctionnement même, reposant sur la détection et l'analyse en continu et en temps réel des attributs ou des comportements des individus, les dispositifs de « caméras augmentées » présentent, par nature, des risques pour les personnes concernées. En outre, les dispositifs de « caméras augmentées » mis en oeuvre dans l'espace public à des fins de police administrative générale ou de police judiciaire sont susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques, raison pour laquelle un encadrement législatif apparaît nécessaire, en application de l'article 34 de la Constitution du 4 octobre 1958.

Dès lors, les dispositifs de caméras augmentées qui poursuivent une finalité dite de « police-justice » dans l'espace public sont interdits en l'absence de cadre légal spécifique.

En l'espèce, la commune utilisait de tels dispositifs en l'absence de cadre légal, notamment afin d'alerter les forces de l'ordre suite à la détection de véhicules roulant à contre-sens sur la chaussée et de détecter des attroupements lorsque le nombre de personnes détectées dans une zone définie dépassait un seuil préfixé.

CNIL, P, 24 juillet 2024, mise en demeure, Commune de X, décision n° MED 2024-109, non publié

2.13 Conditions de licéité des traitements de publication de données personnelles

Possibilité de communication orale à toute personne de données relatives à des condamnations pénales d'une personne physique figurant dans un fichier– 1) Illicéité – 2) Nature du demandeur de société commerciale ou un particulier – Indifférence

1) Les dispositions du règlement 2016/679, notamment l'article 6, paragraphe 1, sous e), et l'article 10 de celui-ci, doivent être interprétées en ce sens qu'elles s'opposent à ce que des données relatives à des condamnations pénales d'une personne physique figurant dans un fichier tenu par une juridiction puissent être communiquées oralement à toute personne aux fins de garantir un accès du public à des documents officiels, sans que la personne demandant la communication ait à justifier d'un intérêt spécifique à obtenir lesdites données.

2) La circonstance que cette personne soit une société commerciale ou un particulier n'ayant pas d'incidence à cet égard.

CJUE, 7 mars 2024, Endemol Shine Finland, C-740/22, point 59

Directive 95/46/CE – Article 6, paragraphe 1, sous e) (durée de conservation) – Données soumises à la publicité au registre des sociétés – Première directive 68/151/CEE – Article 3 – Dissolution de la société concernée – Limitation de l'accès des tiers à ces données

L'ingérence dans le droit à la vie privée et à la protection des données personnel qu'emporte la publicité des données nominatives contenues dans le registre des sociétés n'est pas disproportionné eu égard :

- au nombre de données concernées ;
- au fait qu'elle vise à assurer la sécurité juridique dans les rapports entre les sociétés et les tiers ainsi qu'à protéger les intérêts des tiers par rapport aux sociétés par actions et aux sociétés à responsabilité limitée.

Il ne peut donc être garanti aux personnes physiques dont les données sont inscrites dans le registre des sociétés le droit d'obtenir, après un certain délai à compter de la dissolution de la société, l'effacement des données à caractère personnel les concernant.

En revanche, les États membres peuvent exceptionnellement déroger à cette exigence de publicité. Il leur appartient de déterminer si les personnes physiques, visées à l'article 2, paragraphe 1, sous d) et j) de la directive 68/151/CEE, à savoir, d'une part, les personnes qui ont le pouvoir d'engager une société à l'égard des tiers et de la représenter en justice et celles qui participent à l'administration, à la surveillance ou au contrôle de la société et, d'autre part, les liquidateurs d'une société, peuvent demander à l'autorité chargée de la tenue, respectivement, du registre central, du registre du commerce ou du registre des sociétés de vérifier, sur la base d'une appréciation au cas par cas, s'il est exceptionnellement justifié, pour des raisons prépondérantes et légitimes tenant à leur situation particulière, de limiter, à l'expiration d'un délai suffisamment long après la dissolution de la société concernée, l'accès aux données à caractère personnel les concernant, inscrites dans ce registre, aux tiers justifiant d'un intérêt spécifique à la consultation de ces données.

CJUE, 9 mars 2017, Manni, C-398/15

Publication du nom des bénéficiaires et du montant des bénéficiaires de la Politique Agricole Commune (PAC) – Ingérence excessive dans la vie privée

La publication du nom de l'ensemble des bénéficiaires des aides de la Politique Agricole Commune (PAC) et du montant perçu constitue une ingérence excessive dans la vie privée. Est possible, en revanche, une publication limitée en fonction de la durée, de la fréquence et de l'importance des aides perçues – par exemple, une publication de la liste des principaux bénéficiaires de la PAC.

CJUE, grande chambre, 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 , C-93/09, points 80-83

Divulgation des revenus de salariés d'entités publiques – Nécessaire et appropriée à l'objectif de bonne gestion des ressources publiques

La divulgation des revenus de salariés d'entités publiques à des fins de publication est compatible avec le droit de l'Union si elle est nécessaire et appropriée à l'objectif de bonne gestion des ressources publiques. Il incombe aux juridictions nationales de vérifier s'il est nécessaire d'anonymiser ou non ces données.

CJUE, 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01, C-139/01

Photographies d'une personnalité publique prises à son insu et montrant sa vie quotidienne – Activités relevant purement de la vie privée d'une personnalité non politique, sans fonction officielle – Absence de contribution à un débat d'intérêt général pour la société – « Espérance légitime » de protection et de respect de sa vie privée – Violation de l'article 8 CEDH

La requérante, fille aînée du prince Rainier III de Monaco, souhaite faire interdire toute nouvelle publication, dans des magazines allemands de la presse à sensation, de photographies prises à son insu et la montrant dans sa vie quotidienne et en dehors de son domicile, seule ou accompagnée.

La Cour EDH affirme que la publication de photographies montrant la requérante seule ou accompagnée d'un adulte dans des activités purement privées de sa vie quotidienne relevait de sa « vie privée ». Ces photos et les commentaires les accompagnant ont été publiés dans le cadre d'un reportage destiné à satisfaire la curiosité d'un certain public sur les détails de la vie privée de la princesse, qui n'est pas une personnalité politique et ne remplit aucune fonction officielle pour le compte de l'Etat monégasque. Les publications litigieuses ne contribuaient donc pas à un débat d'intérêt général pour la société, malgré la notoriété de la requérante.

Par ailleurs, la Cour souligne que toute personne, même connue du grand public, doit pouvoir bénéficier d'une « espérance légitime » de protection et de respect de sa vie privée, laquelle comporte une dimension sociale. Or les photos critiquées - qui se rapportent exclusivement aux détails de la vie privée de la requérante - ont été prises à son insu et sans son consentement, dans un contexte de harcèlement quotidien par les photographes. De plus, une protection accrue de la vie privée s'impose face aux progrès techniques qui permettent notamment la réalisation systématique de photos et leur diffusion auprès d'un large public.

Les juridictions allemandes, en qualifiant la requérante de personnalité « absolue » de l'histoire contemporaine, n'ont permis à celle-ci de se prévaloir d'une protection de sa vie privée que si elle se trouve en dehors de son domicile dans un endroit isolé, à l'abri du public, et de surcroît si elle parvient à le prouver, ce qui peut s'avérer difficile. Selon la Cour, ce critère de l'isolement spatial est en pratique trop vague et difficile à déterminer à l'avance pour la personne concernée. L'Etat, tenu de remplir son

obligation positive de protection de la vie privée et du droit à l'image à l'égard de la Convention, n'a pas assuré une protection effective de la vie privée de la requérante.

La Cour EDH conclut donc à une violation de l'article 8.

CEDH, grande chambre, 24 juin 2004, Affaire Von Hannover c/Allemagne, n°59320/00

Diffusion dans les médias d'images d'une personne tentant de mettre fins à ses jours – Ingérence grave dans le droit au respect de la vie privée – Base légale et poursuite de buts légitimes – Absence de raisons pertinentes et suffisantes propres à justifier l'ingérence – Violation de l'article 8 CEDH

Le requérant a tenté de mettre fin à ses jours en se tailladant les poignets, sans savoir qu'une caméra de surveillance avait filmé toute la scène. Après le sauvetage du requérant par la police, avertie par l'opérateur qui regardait les caméras de surveillance, la séquence a été diffusée dans les médias, sans masquer le visage du requérant.

La Cour EDH estime que la divulgation de la séquence litigieuse constitue une ingérence grave dans le droit du requérant au respect de sa vie privée. Sa diffusion dans plusieurs médias, à l'échelle à la fois locale et nationale, excède largement ce qu'un passant aurait pu voir ou ce qui aurait été observé à des fins de sécurité.

La Cour considère que la divulgation avait bien une base légale et poursuivait des buts légitimes que constituent la sûreté publique, la défense de l'ordre, la prévention des infractions pénales et la protection des droits d'autrui.

Cependant, eu égard aux circonstances de l'espèce, la Cour estime qu'il n'y avait pas de raisons pertinentes et suffisantes propres à justifier que la divulgation directement au public, d'une part, de photographies tirées de la séquence, sans avoir au préalable obtenu le consentement du requérant ou caché son identité, et d'autre part, d'images aux médias sans avoir pris des mesures pour s'assurer autant que possible qu'un tel masquage serait effectué par eux. L'objectif que constitue la prévention de la criminalité et le contexte de la divulgation exigeaient en l'espèce une vigilance et un contrôle particuliers sur ces points.

CEDH, 28 janvier 2003, Affaire Peck c/ Royaume Uni, n°44647/98

Mention des noms du constituant, des bénéficiaires et de l'administrateur d'un trust – Absence de mention précisant la qualité et les motifs justifiant la consultation du registre – Atteinte disproportionnée au droit au respect de la vie privée

La mention, dans un registre accessible au public, des noms du constituant, des bénéficiaires et de l'administrateur d'un trust fournit des informations sur la manière dont une personne entend disposer de son patrimoine. Il en résulte une atteinte au droit au respect de la vie privée. Or, le législateur, qui n'a pas précisé la qualité ni les motifs justifiant la consultation du registre, n'a pas limité le cercle des personnes ayant accès aux données de ce registre, placé sous la responsabilité de l'administration fiscale. Dès lors, les dispositions contestées portent au droit au respect de la vie privée une atteinte manifestement disproportionnée au regard de l'objectif poursuivi.

CC, 2016-591 QPC,21 octobre 2016, Mme Helen S, point 6

Dispositif imposant de rendre publics certaines données à caractère personnel aux fins de prévenir les conflits d'intérêts – Conformité à la Constitution

L'obligation de rendre publics, sur un site internet public unique, l'objet précis, la date, l'identité du bénéficiaire direct, l'identité du bénéficiaire final, le montant, y compris les rémunérations et les avantages en nature ou en espèces, des conventions conclues par les entreprises produisant ou commercialisant des produits à finalité sanitaire destinés à l'homme ou assurant des prestations associées à ces produits avec les autres acteurs du secteur de la santé porte atteinte au droit au respect de la vie privée. Cette publication est destinée à garantir l'exhaustivité des informations relatives à l'existence et à la nature des liens d'intérêt entre les professionnels de santé et ces entreprises. Cette atteinte est justifiée par l'exigence constitutionnelle de protection de la santé et par l'objectif d'intérêt général de prévention des conflits d'intérêt. Eu égard aux exigences particulières qui pèsent sur les acteurs du secteur de la santé et à la gravité des conséquences des conflits d'intérêt dans ce secteur, le législateur a opéré une conciliation qui n'est pas manifestement déséquilibrée entre les principes constitutionnels en cause. Par suite, le grief tiré de la méconnaissance du droit au respect de la vie privée doit être écarté.

CC, 2015-727 DC, 21 janvier 2016, Loi de modernisation de notre système de santé, point 92

2.14 Atteinte à un système de traitement automatisé de données (articles 323-1 et suivants du code pénal)

1) Modifications ou suppressions de données dans un système de traitement automatisé de données – Illégalité – Conditions – 2) Maintien ou accès en sachant ne pas y être autorisé dans un système de traitement automatisé de données– Infraction

1) Des modifications ou suppressions de données contenues dans un système de traitement automatisé, en violation de la réglementation en vigueur, sont frauduleuses, au sens de l'article 323-3 du code pénal, y compris si elles sont opérées par une personne ayant un droit d'accès au système, lorsqu'elles ont été sciemment dissimulées à au moins un autre utilisateur d'un tel système, même s'il n'est pas titulaire de droits de modification.

2) Se rend coupable de l'infraction prévue à l'article 323-1 du code pénal la personne qui, sachant qu'elle n'y est pas autorisée, pénètre, ou se maintient, dans un système de traitement automatisé de données.

Cass, crim., 8 juin 2021, n° 20-85.853, B., points 7-13

Suppression de données dans un système de traitement automatisé de donnée – Légalité – Conditions

Les atteintes aux systèmes de traitement automatisé de données prévues aux articles 323-1 à 323-3 du code pénal ne sauraient être reprochées à la personne qui, bénéficiant des droits d'accès et de modification des données, procède à des suppressions de données, sans les dissimuler à d'éventuels autres utilisateurs du système, lorsqu'en l'espèce la personne mise en cause, seule utilisatrice du système, avait procédé à des saisies de données, puis à leur effacement, afin qu'elles n'apparaissent pas dans un journal de comptabilité.

Cass, crim., 7 janvier 2020, n° 18-84.755, B., points 13-16

2.15 Compétence de l'autorité de contrôle

Législation nationale prévoyant une unique autorité de contrôle en application de l'article 51 du RGPD - Compétence de cette autorité pour connaître des réclamations relatives à des traitements de données à caractère personnel par la commission mise en place par le parlement de cet État membre dans l'exercice de son pouvoir de contrôle du pouvoir exécutif

L'article 77, paragraphe 1, et l'article 55, paragraphe 1, du RGPD doivent être interprétés en ce sens que lorsqu'un État membre a fait le choix, conformément à l'article 51, paragraphe 1, de ce règlement, d'instituer une seule autorité de contrôle, sans toutefois lui attribuer la compétence pour surveiller l'application dudit règlement par une commission d'enquête mise en place par le parlement de cet État membre dans l'exercice de son pouvoir de contrôle du pouvoir exécutif, ces dispositions confèrent directement à cette autorité la compétence pour connaître des réclamations relatives à des traitements de données à caractère personnel effectués par ladite commission d'enquête.

CJUE, 16 janvier 2024, Österreichische Datenschutzbehörde, C-33/22

Mise à disposition temporaire par une juridiction de pièces issues d'une procédure juridictionnelle à des journalistes – Traitements effectués dans l'exercice de sa fonction juridictionnelle – Contrôle par une autorité extérieure – Absence

L'article 55, paragraphe 3, du règlement (UE) 2016/679 doit être interprété en ce sens que le fait pour une juridiction de mettre à la disposition temporaire de journalistes des pièces issues d'une procédure juridictionnelle, contenant des données à caractère personnel, afin de leur permettre de mieux rendre compte du déroulement de cette procédure relève de l'exercice, par cette juridiction, de sa « fonction juridictionnelle », au sens de cette disposition.

La détermination, eu égard à l'objet et au contexte d'une affaire donnée, des informations issues d'un dossier de procédure juridictionnelle pouvant être fournies à des journalistes dans le but de leur permettre de rendre compte du déroulement de la procédure juridictionnelle ou d'éclairer tel ou tel aspect d'une décision rendue se rattache clairement à l'exercice, par ces juridictions, de leur « fonction juridictionnelle », dont le contrôle par une autorité extérieure serait susceptible de porter atteinte, de manière générale, à l'indépendance du pouvoir judiciaire.

CJUE, 24 mars 2022, Autoriteit Persoonsgegevens, C-245/20, points 38-39

2.16 Indépendance de l'autorité de contrôle

Risque d'influence politique des autorités de tutelle de l'État – Entrave à l'exercice indépendant des missions de l'autorité de contrôle – Obligation de respecter la durée du mandat

Le seul risque que les autorités de tutelle de l'État puissent exercer une influence politique sur les décisions des autorités de contrôle suffit pour entraver l'exercice indépendant des missions de celles-ci. En effet, d'une part, il pourrait en résulter une « obéissance anticipée » de ces autorités eu égard à la pratique décisionnelle de l'autorité de tutelle et, d'autre part, « considérant le rôle de gardiennes du droit à la vie privée qu'assument les autorités de contrôle », leurs décisions comme elles-mêmes doivent être au-dessus de tout soupçon de partialité.

En outre, mettre fin au mandat d'une autorité de contrôle avant son terme sans respecter les règles et les garanties préétablies à cette fin par la législation applicable constituerait une menace potentielle

qui « planerait alors sur cette autorité tout au long de l'exercice de son mandat » et pourrait conduire à une forme d'obéissance de celle-ci au pouvoir politique, incompatible avec l'exigence d'indépendance. Peu importe la circonstance que la fin anticipée du mandat résulte d'une restructuration ou d'un changement de modèle.

Il s'ensuit que l'exigence d'indépendance mentionnée par la directive 95/46 doit « nécessairement être interprétée comme incluant l'obligation de respecter la durée du mandat des autorités de contrôle jusqu'à son échéance et de n'y mettre fin de manière anticipée que dans le respect des règles et des garanties de la législation applicable ».

CJUE, grande chambre, 8 avril 2014, Commission / Hongrie, C-288/12, points 53-55

Régime institutionnel méconnaissant l'exigence d'indépendance

Méconnaît l'exigence d'indépendance prévue à l'article 28, paragraphe 1, second alinéa, de la directive 95/46 un régime institutionnel où :

- le membre administrateur de l'autorité de contrôle est un fonctionnaire fédéral assujetti à une tutelle de service ;
- le bureau de l'autorité est intégré aux services de la chancellerie fédérale ;
- le chancelier fédéral dispose d'un droit inconditionnel à l'information sur tous les aspects de la gestion de la Datenschutzkommission.

CJUE, grande chambre, 16 octobre 2012, Commission/ Autriche, C-614/10

Régime institutionnel méconnaissant l'exigence d'indépendance

Méconnaît l'exigence d'indépendance prévue à l'article 28, paragraphe 1, second alinéa, de la directive 95/46 un régime institutionnel où sont soumises à une tutelle administrative de l'État ou Länder les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel, quelles que soient les modalités d'exercice de ladite tutelle, dès lors qu'elle permet en principe au Gouvernement du Land concerné ou à un organe de l'administration soumise à ce Gouvernement d'influer directement ou indirectement sur les décisions des autorités de contrôle ou, le cas échéant, d'annuler et de remplacer ces décisions.

CJUE, grande chambre, 9 mars 2010, Commission / Allemagne, C-518/07

---

3. Autres règles incombant à certains responsables du traitement et sous-traitants

3.1 Obligations liées à la responsabilité conjointe

Accord de responsabilité conjointe – Collecte du consentement pour le compte de sociétés partenaires – Obligation du responsable de traitement ne collectant pas le consentement d'être en mesure de démontrer que la personne concernée a donné son consentement

En cas de responsabilité conjointe, l'article 26 du RGPD oblige les responsables de traitement conjoints à s'assurer, par le biais d'un accord, qu'ils respectent mutuellement le RGPD et notamment qu'ils organisent entre eux la meilleure façon de répondre aux droits des personnes concernées, en fonction de la nature du traitement et de leur responsabilité respective vis-à-vis de ce traitement.

En l'espèce, le fait que la collecte du consentement des internautes pour la mise en œuvre du traitement en cause revenait aux partenaires de la société mise en cause n'exonérait pas cette dernière de son obligation, en application de l'article 7 du RGPD, d'être en mesure de démontrer que la personne concernée avait donné son consentement et de procéder à certaines vérifications à cette fin. En effet, la seule clause issue de conditions générales d'utilisation aux termes desquelles la société exigeait de ses partenaires, « lorsque la loi le prévoit », que la politique de confidentialité de leur site inclue « des mentions et des mécanismes de choix conformes aux lois et réglementations applicables » ne permettait pas de garantir l'existence d'un consentement valide et il convenait à tout le moins qu'elle soit complétée pour préciser que l'organisme qui recueille le consentement doit mettre à disposition de l'autre partie la preuve du consentement.

CNIL, FR, 15 juin 2023, Sanction, Société X, n°SAN-2023-009, publié, points 52, 61, 74

3.2 Obligations en cas de sous-traitance

3.2.1 Obligations du responsable

Suivi des instructions contractuelles par le sous-traitant – Contrôle par le responsable de traitement

Si le responsable de traitement peut décider de recourir à un prestataire spécialisé, en particulier en lui confiant une mission de sous-traitance des données à caractère personnel, au sens du RGPD, il reste tenu de veiller, par des diligences raisonnables, à ce que le respect de la protection des données à caractère personnel soit effectivement assuré. Le caractère suffisant de ces diligences dépend notamment des compétences et des moyens du responsable de traitement. La responsabilité du responsable de traitement peut être retenue du fait de l'absence de mise en œuvre par celui-ci d'un contrôle régulier sur les mesures techniques et organisationnelles prises par un sous-traitant.

CNIL, FR, 11 mai 2023, Sanction, Société X, n°SAN-2023-006, publié, point 33

Voir aussi : CE, 10ème chambre, 26 avril 2022, Optical Center, n° 449284, Inédit ; CNIL, FR, 24 novembre 2022, Sanction, Société X, n° SAN-2022-021, publié

3.2.2 Obligations du sous-traitant

3.3 Analyse d'impact

3.3.1 Nécessité

Décret créant un traitement relatif à la gestion des ressources humaines d'agents de l'État – Traitement établissant des profils de personnes physiques – 1) Analyse d'impact relative à la protection des données– 2) Ouverture du traitement à d'autres services ou

institutions – Élaboration de l'étude d'impact pendant la préparation du décret – 3) Caractère suffisant de l'analyse d'impact préexistante – Conditions – Obligation de compléter l'analyse d'impact en cas d'adaptation de la mise en œuvre

Saisi d'un projet de décret portant création d'un traitement automatisé de données à caractère personnel relatif à la gestion des ressources humaines de certains agents de l'État, le Conseil d'État constate que ce traitement a fait l'objet, comme il le devait, d'une analyse d'impact relative à la protection des données à caractère personnel.

1) Il considère en premier lieu que la réalisation préalable de cette analyse d'impact est exigée par les dispositions du paragraphe 1 de l'article 35 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (dit RGPD) dans la mesure où ce traitement permet de procéder à une « évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire » au sens du a) du paragraphe 3 du même article.

Il relève à cet égard que les traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines figurent sur la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, annexée à la délibération n° 2018-327 du 11 octobre 2018 de la CNIL portant adoption de cette liste.

2) En deuxième lieu, dans la mesure où le projet de décret ouvre à des services ou institutions distincts la possibilité de recourir à ce traitement dans des conditions similaires, la dernière phrase du paragraphe 1 de l'article 35 du RGPD, selon laquelle « une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires », a logiquement conduit à élaborer cette analyse d'impact lors de la préparation du projet de décret.

3) En troisième lieu, lorsque des services ou institutions décideront d'y recourir sans adapter les modalités de mise en œuvre de ce traitement, l'analyse d'impact réalisée lors de la préparation du projet de décret pourra être regardée comme suffisante. Toutefois, compte tenu de la diversité des caractéristiques et des modes d'organisation des services ou institutions susceptibles de recourir au traitement en cause et des adaptations qu'ils décident de lui apporter en fonction de leurs besoins, il appartiendra à chaque responsable, préalablement à la mise en œuvre du traitement, de compléter le cas échéant l'analyse d'impact produite initialement par l'autorité compétente, en fonction des spécificités propres à cette mise en œuvre.

CE, Section de l'administration (section de l'intérieur), 23 mai 2019, Avis n°396435, Projet de décret portant création d'un traitement automatisé relatif à la gestion des ressources humaines de certains agents de l'État

---

L'analyse d'impact n'est pas une modalité de la procédure consultative et ne conditionne pas la légalité d'un décret. Elle est en revanche une obligation de fond s'imposant au responsable de traitement.

Le Conseil d'État (section de l'intérieur) saisi d'un projet de décret portant transposition en droit interne des principes du code mondial antidopage et de diverses modifications relatives à la procédure disciplinaire lui donne un avis favorable. Ce projet modifie les dispositions réglementaires du code du sport relatives au traitement automatisé de données à caractère personnel visant à mettre en œuvre l'établissement du profil biologique des sportifs, ainsi que celles relatives aux modalités d'utilisation d'un algorithme prédictif pour les besoins de l'établissement de ce même profil biologique.

Le Conseil d'État considère, eu égard au caractère sensible des données médicales qui font l'objet d'un traitement pour l'établissement du profil biologique des sportifs, au grand nombre de sportifs concernés, ainsi qu'aux modalités de réalisation de ce traitement, au moyen d'un algorithme prédictif, et à ses finalités, notamment de sanction, que le traitement permettant l'établissement du profil

biologique des sportifs impose de conduire l'analyse d'impact prévue par l'article 35 du règlement général sur la protection des données.

Si la réalisation de cette dernière n'est pas une modalité de la procédure consultative de la CNIL et ne conditionne pas la légalité du décret modifiant les dispositions règlementaires relatives à ce traitement, elle n'en n'est pas moins une obligation de fond s'imposant au responsable dudit traitement. Aussi le Conseil d'État attire-t-il l'attention du Gouvernement sur la nécessité pour le responsable du traitement de réaliser cette analyse d'impact dans les plus brefs délais.

CE, Section de l'intérieur, 19 mars 2019, Avis n° 396817, Projet de décret portant transposition des principes du code mondial antidopage et diverses modifications relatives à la procédure disciplinaire

---

Traitement nécessaire à l'organisation d'un vote électronique – Traitement à grande échelle de données sensibles – Obligation pour le responsable du traitement d'effectuer une analyse d'impact qui doit être achevée pour la mise en œuvre du traitement

Un traitement nécessaire à l'organisation d'un vote électronique pour l'élection des membres des chambres d'agriculture, eu égard, d'une part, à la nature des données collectées et analysées et, d'autre part, au fait que ces données portent sur un électorat d'environ trois millions de personnes, remplit les critères posés par le point b) du paragraphe 3 de l'article 35 du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD) pour caractériser les traitements à grande échelle de données sensibles.

Par suite, sa mise en œuvre doit être précédée de l'analyse d'impact prévue par ces stipulations. Cette obligation d'effectuer une analyse d'impact est d'application immédiate et directe. Le paragraphe 4 du même article 35 dispose que : « L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68 ». Toutefois, cette liste ne saurait être regardée comme une mesure nationale d'application nécessaire à l'entrée en vigueur de l'obligation faite au responsable du traitement d'effectuer une analyse d'impact qui découle directement du point b) du paragraphe 3 de l'article 35 du règlement.

La circonstance que le responsable du traitement (le ministre de l'agriculture) n'ait pas, au moment où le Conseil d'État (section des travaux publics) a examiné un projet de décret comportant la mise en œuvre de traitements relevant de la procédure prévue au b) du paragraphe 3 de l'article 35 du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD), achevé l'analyse d'impact qui lui incombe ne faisait obstacle ni à cet examen, ni à ce que le Conseil d'État lui donnât un avis favorable, dès lors qu'en vertu du paragraphe 1 de cet article, cette analyse doit être effectuée « avant le traitement », c'est-à-dire avant la mise en œuvre concrète de celui-ci.

CE, Section des travaux publics, 3 juillet 2018, Avis n° 395077, Projet de décret comportant la mise en œuvre de traitement relevant de la procédure prévue au b) du règlement (UE) n°2016/679 du 27 avril 2016 (RGPD)

3.3.2 Contenu

Directive 2016/680 – Possibilité de mener une unique analyse d'impact sur « un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires » – Existence même si aucune disposition de la directive ne le prévoit

À l'occasion de l'examen d'un projet de décret relatif à la mise en œuvre de traitements de données à caractère personnel provenant des caméras individuelles des agents de la police municipale, le Conseil

d'État (section de l'intérieur) estime qu'il résulte tant des finalités poursuivies par les dispositifs en cause que des missions confiées aux agents de police municipale, que les traitements projetés relèvent des dispositions de la directive (UE) n° 2016/680 du 27 avril 2016 telle que transposée aux articles 70-1 et suivants de la loi du 6 janvier 1978 modifiée.

Compte tenu de leurs finalités ils doivent être regardés comme mis en œuvre pour le compte de l'État. Le traitement étant mis en œuvre au niveau des collectivités locales ou des établissements de coopérations intercommunales, le ministre de l'intérieur ne peut être regardé comme le responsable du traitement au sens du premier alinéa de l'article 70-4, alors même que cette mise en œuvre est faite pour le compte de l'État.

Le Conseil d'État (section de l'intérieur) estime cependant possible que, dans le cadre de l'élaboration du texte régissant les caractéristiques essentielles du traitement, le ministre réalise une étude d'impact d'ensemble, bien que la directive ne prévoit pas, quant à elle, qu'une seule et même analyse puisse « porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires », à l'instar de l'article 35 du règlement (UE) 2016/679.

CE, Section de l'intérieur, 8 janvier 2019, Avis n° 396340, Projet de décret relatif à la mise en œuvre de traitements provenant des caméras individuelles des agents de la police municipale

---

3.3.3 Consultation de l'autorité de contrôle sur une AIPD

Dans le champ du RGPD

Dans le champ de la directive

Traitement relevant de la directive « Police-Justice » susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques et mis en œuvre pour le compte de l'État – Analyse d'impact devant être réalisée et transmise à la CNIL avant l'édiction de l'acte définissant le traitement

Il résulte de l'article 90 de la loi n° 78-17 du 6 janvier 1978, applicable aux traitements de données à caractère personnel relevant de la directive (UE) 2016/80 du 27 avril 2016, mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, que, lorsqu'est exigée une analyse d'impact préalablement à la création ou à la modification d'un tel traitement mis en œuvre pour le compte de l'État, il appartient à l'administration, à peine d'irrégularité de l'acte instituant ou modifiant ce traitement, de la réaliser et de la transmettre à la Commission nationale de l'informatique et des libertés (CNIL) dans le cadre de la demande d'avis prévue à l'article 33 de la loi du 6 janvier 1978.

CE, 10ème–9ème chambres réunies, 24 décembre 2021, Ligue des droits de l'homme et autres, n° 447513, T., point 12

Voir aussi : CE, 10ème–9ème chambres réunies, 24 décembre 2021, Ligue des droits de l'homme et autres, n° 447515, Inédit

---

3.4 Code de conduite

3.5 Certification

3.5.1 Traitements

3.5.2 Produits et personnes

3.6 Délégué à la protection des données

Interdiction de relèvement de ses fonctions pour l'exercice de ses missions – Exigence d'indépendance fonctionnelle – 1) Réglementation nationale interdisant le relèvement de ses fonctions d'un DPO en l'absence de motif grave – Licéité – 2) Conflit d'intérêts – Critères

1) L'article 38, paragraphe 3, deuxième phrase, du RGPD doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale prévoyant qu'un responsable du traitement ou un sous-traitant ne peut révoquer un délégué à la protection des données qui est membre de son personnel que pour un motif grave, même si la révocation n'est pas liée à l'exercice des missions de ce délégué, pour autant qu'une telle réglementation ne compromette pas la réalisation des objectifs de ce règlement.

2) Un « conflit d'intérêts », au sens de l'article 38, paragraphe 6 du RGPD est susceptible d'exister lorsqu'un délégué à la protection des données se voit confier d'autres missions ou tâches, qui conduiraient ce dernier à déterminer les finalités et les moyens du traitement de données à caractère personnel auprès du responsable du traitement ou de son sous-traitant, ce qu'il incombe au juge national de déterminer au cas par cas, sur la base d'une appréciation de l'ensemble des circonstances pertinentes, notamment de la structure organisationnelle du responsable du traitement ou de son sous-traitant et à la lumière de l'ensemble de la réglementation applicable, y compris des éventuelles règles internes de ces derniers.

CJUE, 9 février 2023, X-FAB Dresden, C-453/21

Protection du délégué à la protection des données contre toute décision défavorable en relation avec ses missions – 1) Portée – a) Protection garantissant l'effectivité du RGPD– Existence – b) Obstacle au licenciement d'un délégué – Absence, par elle-même – c) Protection régissant globalement ses relations de travail avec le responsable du traitement – Absence – 2) Conséquence – Possibilité pour le délégué de faire l'objet d'une sanction ou d'un licenciement – Conditions

1) a) Il résulte du paragraphe 3 de l'article 38 du RGPD, éclairé par la Cour de justice de l'Union européenne (CJUE) dans son arrêt du 22 juin 2022 (C-534/20), Leistritz AG c/ LH, qu'en protégeant le délégué à la protection des données contre toute décision qui mettrait fin à ses fonctions, lui ferait subir un désavantage ou qui constituerait une sanction, lorsqu'une telle décision serait en relation avec l'exercice de ses missions, ces dispositions visent essentiellement à préserver l'indépendance fonctionnelle du délégué à la protection des données et, partant, à garantir l'effectivité du RGPD.

b) En revanche, elles ne font pas obstacle au licenciement d'un délégué qui ne posséderait plus les qualités professionnelles requises pour exercer ses missions ou qui ne s'acquitterait pas de celles-ci conformément au RGPD.

c) Il ressort également de cet arrêt que ces dispositions n'ont pas pour objet de régir globalement les relations de travail entre un responsable du traitement ou un sous-traitant et des membres de son personnel, lesquelles ne sont susceptibles d'être affectées que de manière accessoire, dans la mesure strictement nécessaire à la réalisation des objectifs du RGPD.

2) Il en résulte clairement que l'article 38 du RGPD ne fait pas obstacle à ce que le salarié exerçant les fonctions de délégué au sein de l'entreprise fasse l'objet d'une sanction ou d'un licenciement à raison de manquements aux règles internes à l'entreprise applicables à tous ses salariés, sous réserve que ces dernières ne soient pas incompatibles avec l'indépendance fonctionnelle qui lui est garantie par le RGPD.

CE,10ème-9ème chambres réunies, 21 octobre 2022, Mme A... C..., n° 459254, Rec., point 10

---

4 Droits des personnes

4.1 Généralités sur les modalités d'exercice des droits

Obligation de faciliter l'exercice des droits (art. 12 RGPD) – Cas d'un responsable de traitement mettant à disposition des adresses électroniques erronées, sans diligence pour les corriger, et une adresse postale – Manquement

Le caractère erroné des adresses électroniques communiquées sur le site web d'un responsable de traitement et destinées à recueillir les demandes relatives à l'exercice des droits conférés à la personne en vertu des articles 15 à 22 du RGPD, lorsqu'il n'a été pleinement réparé qu'à l'issue d'un délai de plus de six mois, et postérieurement à un contrôle diligenté par les services de la CNIL, ainsi qu'une procédure d'exercice de ces mêmes droits effectuée par voie postale par un prestataire du responsable du traitement ne permettant pas de faciliter les démarches des personnes concernées, en l'absence de transmission directe des demandes de droit d'accès du responsable de traitement à son prestataire, sont de nature à caractériser un manquement aux dispositions de l'article 12 du RGPD.

CE, 10ème chambre, 26 avril 2022, Optical Center, n°449284, Inédit., point 7

4.1.1 Limitations en application de l'article 23 RGPD

Traitement de données à caractère personnel à des fins fiscales – 1) «Mesure législative» limitant la portée des obligations et des droits au sens du RGPD – Mesure nécessairement adoptée par un parlement – Absence – Conditions – Clarté, précision et prévisibilité de la limitation pour les justiciables – 2) Demande de communication d'informations relatives à des annonces de vente de véhicules mises en ligne – a) Application des principes de l'article 5 du RGPD – Application, en l'absence de mention expresse inverse dans le droit national – b) Licéité – Existence

1) Il ressort du considérant 41 du RGPD, que la référence, dans ce règlement, à une « mesure législative » n'implique pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée.

Toute mesure adoptée en vertu de l'article 23 du RGPD doit, ainsi que le législateur de l'Union l'a, au demeurant, souligné au considérant 41 de ce règlement, être claire et précise et son application être prévisible pour les justiciables. En particulier, ces derniers doivent être en mesure d'identifier les circonstances et les conditions dans lesquelles la portée des droits que leur confère ledit règlement est susceptible de faire l'objet d'une limitation.

Il découle des considérations qui précèdent que l'administration fiscale d'un État membre ne saurait déroger aux dispositions de l'article 5, paragraphe 1), du RGPD en l'absence d'une base juridique claire et précise du droit de l'Union ou du droit national, dont l'application est prévisible pour les justiciables, prévoyant les circonstances et les conditions dans lesquelles la portée des obligations et des droits prévus à cet article 5 peut être limitée.

2) a) Les dispositions du RGPD doivent être interprétées en ce sens que l'administration fiscale d'un État membre ne saurait déroger aux dispositions de l'article 5, paragraphe 1, de ce règlement, qui fixe les principes à respecter par tout traitement, alors qu'un tel droit ne lui a pas été octroyé par le droit national, au sens de l'article 23, paragraphe 1, de ce même texte.

b) Les dispositions du RGPD doivent être interprétées en ce sens qu'elles ne s'opposent pas à ce que l'administration fiscale d'un État membre impose à un prestataire de services d'annonces publiées sur internet de lui communiquer des informations relatives aux contribuables ayant publié des annonces

dans l'une des rubriques de son portail en ligne, dès lors que cela est nécessaire à la mission d'intérêt public poursuivie par cette administration. Néanmoins, les données demandées doivent être nécessaires au regard des finalités spécifiques pour lesquelles elles sont collectées et la période sur laquelle porte leur collecte ne saurait excéder la durée strictement nécessaire pour atteindre l'objectif d'intérêt général visé.

CJUE, 24 février 2022, Valsts ieņēmumu dienests , C-175/20, points 52, 56-57

---

1) Administration fiscale – Traitement aux fins d'obtenir le droit de procéder à une mesure d'enquête – Fraude fiscale – Champ d'application matériel du RGPD – 2) Contrôle du juge – Obligation d'informations pesant sur le responsable de traitement, exemptions ou limitations – Conditions – 3) Limitation de la portée de l'obligation d'informer – Conditions

1) Le traitement de données à caractère personnel mis en œuvre par l'administration fiscale aux fins d'obtenir l'autorisation de procéder à des opérations de visite et saisies sur le fondement de l'article L. 16 B du livre des procédures fiscales, qui a pour finalité d'obtenir le droit de procéder à une mesure d'enquête pouvant donner lieu à la constatation d'une infraction ou d'un manquement à la législation fiscale, dans le but de percevoir l'impôt et de lutter contre la fraude fiscale, entre dans le champ d'application matériel du RGPD.

2) Dès lors, le juge doit notamment vérifier si, dans le litige qui lui est soumis, le responsable du traitement est tenu de fournir à la personne concernée les informations prévues à son article 14 ou si sont réunies les conditions des exceptions ou limitations à cette obligation d'information qu'il prévoit. En effet, si l'article 14 du RGPD soumet le responsable du traitement à l'obligation de fournir un certain nombre d'informations à la personne concernée lorsque les données à caractère personnel n'ont pas été collectées auprès d'elle, il résulte du paragraphe 5 de ce texte que cette obligation ne s'applique pas dans la mesure où elle est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement.

3) En outre, l'article 23 du RGPD prévoit que le droit de l'État membre auquel le responsable du traitement est soumis peut, par la voie de mesures législatives, limiter la portée de l'obligation d'informer la personne concernée par le traitement de données à caractère personnel prévue à l'article 14 du RGPD lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la prévention et la détection d'infractions pénales, les enquêtes et les poursuites en la matière et d'autres objectifs importants d'intérêt public général d'un État membre, notamment un intérêt économique ou financier important, y compris dans les domaines monétaire, budgétaire et fiscal.

Ainsi, l'administration fiscale n'a pas l'obligation de fournir à la personne concernée les informations prévues à l'article 14 de ce règlement si sont réunies les conditions de l'exception prévue au paragraphe 5 de ce texte ou des limitations prévues à l'article 23.

Cass, com., 1er juin 2023, n°21-18.558, B., points 10-15

Décret du Premier ministre autorisant la collecte de données nécessaires au développement d'un algorithme pour l'indemnisation du préjudice corporel– « Mesure législative » pour la limitation des droits au sens du RGPD – Inclusion

Le Premier ministre est compétent pour l'adoption d'un décret se bornant à autoriser la collecte de données nécessaires au développement d'un algorithme en matière d'indemnisation du préjudice corporel sans déroger à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui n'a ni pour objet, ni pour effet de fixer des règles relatives aux garanties fondamentales

accordées aux citoyens pour l'exercice des libertés publiques, y compris en ce qu'il exclut l'exercice des droits d'information et d'opposition des personnes dont les données personnelles sont collectées.

L'article 23 du RGPD selon lequel le droit de l'Union ou le droit d'un État membre peut apporter des limitations aux droits prévus par le règlement « par la voie de mesures législatives », ne saurait être entendu comme imposant l'intervention du législateur, le droit de l'Union européenne ne régissant pas la répartition des compétences au sein des États membres.

CE, 10ème–9ème chambres réunies, 30 décembre 2021, Société B... Avocat Victimes et Préjudices et autres, n° 440376, Inédit., points 5, 28

Voir aussi : CE, 10ème – 9ème chambres réunies, 18 octobre 2018, M. K... et autres, n° 404996, Rec. ; CE, 10ème/9ème SSR, 11 mars 2013, Association SOS racisme – Touche pas à mon pote, n° 348613, Rec.

« Mesure législative » limitant ou excluant le droit d'opposition (art. 23 RGPD) – 1) Autorités pouvant écarter le droit d'opposition – Collectivités territoriales et établissements publics – Inclusion – 2) Conditions et garanties

1) L'article 23 du RGPD permet de limiter ou d'écarter le droit d'opposition à un traitement, à certaines conditions, par une « mesure législative ». Le considérant 41 du RGPD précise que cette « mesure législative » n'est pas nécessairement un acte adopté par le Parlement, mais doit être déterminée par le droit national de chaque État membre. En France, il peut en particulier s'agir d'un acte réglementaire. La CNIL estime que, s'agissant des traitements participant de l'exécution d'une mission d'intérêt public, tant l'État que les collectivités territoriales ou les établissements publics peuvent, dans leurs domaines de compétence respectifs et s'ils disposent d'un pouvoir réglementaire, limiter ou exclure le droit d'opposition.

2) Cependant, l'exercice de cette faculté est soumis à une double limite : d'une part, s'agissant de la compétence, il convient de ne pas empiéter sur le domaine réservé à la loi en application de l'article 34 de la Constitution ; d'autre part, de veiller à ce que les conditions prévues à l'article 23 soient respectées. Dans ses lignes directrices 10/2020 du 13 octobre 2021 sur l'article 23, le Comité européen pour la protection des données a notamment rappelé l'obligation pour le responsable de traitement de veiller au caractère strictement nécessaire et proportionné de la limitation envisagée au regard de l'objectif poursuivi. Il a également souligné que l'acte écartant l'opposition doit faire l'objet d'une publicité suffisante et être accessible.

CNIL, SP, 16 février 2023, Avis sur un projet de décision, Création d'un fichier central des titres permanents du permis de chasser, n°2023-015, publié, point 16

4.2 Information

Procédure de préinscription à l'entrée en premier cycle Parcoursup – Publication obligatoire à l'issue de la procédure des critères d'examen des candidatures sous la forme d'un rapport indiquant dans quelle mesure des traitements algorithmiques ont été utilisés

Les dispositions du dernier alinéa du paragraphe I de l'article L. 612-3 du code de l'éducation ne sauraient, sans méconnaître le droit d'accès aux documents administratifs garanti par l'article 15 de la Déclaration de 1789, être interprétées comme dispensant chaque établissement d'enseignement supérieur de publier, à l'issue de la procédure nationale de préinscription à l'entrée en premier cycle et dans le respect de la vie privée des candidats, le cas échéant sous la forme d'un rapport, les critères

en fonction desquels les candidatures ont été examinées et précisant, le cas échéant, dans quelle mesure des traitements algorithmiques ont été utilisés pour procéder à cet examen.

CC, 2020-834 QPC, 3 avril 2020, UNEF, point 17

Caractérisation du délit de collecte de données à caractère personnel par un moyen déloyal dans le cadre de rapports employeur/employés - Données disponibles en accès libre sur internet – Utilisation sans rapport avec l'objet de leur mise en ligne – Collecte à l'insu des personnes concernées – Méconnaissance de l'obligation d'information des personnes et de leur droit d'opposition

Dans le cadre de rapports employeur/employés, le fait d'effectuer des recherches sur des personnes portant sur des données à caractère personnel telles qu'antécédents judiciaires, renseignements bancaires et téléphoniques, véhicules, propriétés, qualité de locataire ou de propriétaire, situation matrimoniale, santé, déplacement à l'étranger est susceptible de constituer un moyen de collecte déloyal dès lors que, issues de la capture et du recoupement d'informations diffusées sur des sites publics tels que sites web, annuaires, forums de discussion, réseaux sociaux, sites de presse régionale, de telles données ont fait l'objet d'une utilisation sans rapport avec l'objet de leur mise en ligne et ont été recueillies à l'insu des personnes concernées, ainsi privées du droit d'opposition institué par la loi informatique et libertés.

En effet, le fait que les données à caractère personnel collectées en l'espèce par le prévenu aient été pour partie en accès libre sur internet ne retire rien au caractère déloyal de cette collecte, dès lors qu'une telle collecte, de surcroît réalisée à des fins dévoyées de profilage des personnes concernées et d'investigation dans leur vie privée, à l'insu de celles-ci, ne pouvait s'effectuer sans qu'elles en soient informées.

Cass, crim., 30 avril 2024, n°23-80.962, B., points 8,10

Décret du 30 janvier 2019 relatif aux modalités d'évaluation des personnes se déclarant mineures – Personne se déclarant mineure et privée de la protection de sa famille – Demande de protection – Information effective et adaptée – Exigence de clarté (article 12 RGPD)

L'article R. 221-15-8 du code de l'action sociale et des familles créé par le décret attaqué dispose que, préalablement à la collecte de ses données, la personne se déclarant mineure et privée temporairement ou définitivement de la protection de sa famille est informée de la nature des données et informations collectées et des conséquences d'un refus de les communiquer ou d'une évaluation concluant à sa majorité et reçoit des informations relatives à la protection des données personnelles. Cette information est assurée par un formulaire dédié et rédigé dans une langue qu'elle comprend ou dont il est raisonnable de supposer qu'elle la comprend. À défaut, notamment lorsque l'intéressé ne sait pas lire, l'information est donnée sous forme orale. Le décret attaqué a ainsi prévu une information effective et adaptée des personnes sollicitant une protection en qualité de mineur, qui doit en outre satisfaire, sans que le pouvoir réglementaire ait eu à le rappeler, à l'exigence de clarté et de simplicité prévue par l'article 12 du RGPD.

CE, 1ère–4ème chambres réunies, 5 février 2020, Unicef France et autres, n°428478, T., point 23

4.2.1 Dans le champ du RGPD

En cas de collecte directe

Cookies – 1) Information claire et complète devant être donnée par le fournisseur de services – Durée de fonctionnement des cookies – Possibilité ou non pour des tiers d'avoir accès aux cookies – 2) Non exhaustivité de la liste des informations que le responsable de traitement doit fournir en application de l'article 10 de la directive 95/46 – Durée de fonctionnement des cookies – Exigence d'un traitement loyal

1) L'article 5, paragraphe 3, de la directive 2002/58 doit être interprété en ce sens que les informations que le fournisseur de services doit donner à l'utilisateur d'un site internet incluent la durée de fonctionnement des cookies ainsi que la possibilité ou non pour des tiers d'avoir accès à ces cookies.

2) L'article 10 de la directive 95/46, à laquelle fait référence l'article 5, paragraphe 3, de la directive 2002/58, ainsi que l'article 13 du RGPD énoncent les informations que le responsable du traitement doit fournir à la personne auprès de laquelle il collecte des données la concernant. Ces informations comprennent notamment, en vertu de l'article 10 de la directive, outre l'identité du responsable du traitement et les finalités du traitement auquel les données sont destinées, toute information supplémentaire telle que les destinataires ou les catégories de destinataires des données, dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

Si la durée du traitement des données ne figure pas parmi ces informations, il ressort toutefois de l'expression « au moins » figurant à l'article 10 de la directive 95/46 que celles-ci ne sont pas énumérées de manière exhaustive. Or, l'information sur la durée de fonctionnement des cookies doit être considérée comme répondant à l'exigence d'un traitement loyal des données prévue par ledit article, en ce que, dans une situation telle que celle en cause au principal, une durée longue, voire illimitée, implique la collecte de nombreuses informations sur les habitudes de navigation et la fréquence des visites éventuelles de l'utilisateur sur les sites des partenaires publicitaires de l'organisateur du jeu promotionnel.

Cette interprétation est corroborée par l'article 13, paragraphe 2, sous a), du règlement 2016/679, qui prévoit que le responsable du traitement doit fournir à la personne concernée, pour garantir un traitement équitable et transparent, une information portant, notamment, sur la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée.

Quant à la possibilité ou non pour des tiers d'avoir accès aux cookies, il s'agit d'une information comprise dans les informations mentionnées à l'article 10, sous c), de la directive 95/46, ainsi qu'à l'article 13, paragraphe 1, sous e), du règlement 2016/679, dès lors que ces dispositions mentionnent explicitement les destinataires ou les catégories de destinataires des données.

CJUE, grande chambre, 1er octobre 2019, Planet49, C-673/17, points 76-80

Directive 95/46 – Exceptions à l'obligation d'information de l'article 13, paragraphe 1 – Transposition en droit national – Faculté des États membres

L'article 13, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 doit être interprété en ce sens que les États membres ont non pas l'obligation, mais la faculté de transposer dans leur droit national une ou plusieurs des exceptions qu'il prévoit à l'obligation d'informer les personnes concernées du traitement de leurs données à caractère personnel.

CJUE, 7 novembre 2013, IPI, C-473/12

Exigence d'accessibilité de l'information - Politique de confidentialité disponible uniquement en anglais – Illicéité.

L'information fournie au moyen d'une politique de confidentialité disponible uniquement en anglais, relative à des traitements de données ciblant majoritairement un public francophone, ne permet pas aux personnes concernées d'apprécier à l'avance la portée et les conséquences des traitements et n'est par conséquent pas conforme aux exigences de transparence de l'information posées par l'article 12 du RGPD. Il en va de même du renvoi opéré vers une politique de confidentialité uniquement en anglais depuis un formulaire de création de compte.

CNIL, FR, 29 décembre 2023, Sanction, Société X, n° SAN-2023-023, publié

Prospection téléphonique non soumise au consentement préalable de la personne – 1) Obligation d'informer au plus tard lors de l'appel téléphonique – 2) Forme de l'information prévue par le RGPD

1) Il résulte de l'article 14 du RGPD que, lorsqu'un prospecteur récupère un numéro de téléphone d'un tiers, par exemple un fournisseur d'accès à internet (FAI), à des fins de prospection par voie téléphonique, il doit informer la personne prospectée du traitement de ces données pour cette finalité, au plus tard lors de l'appel téléphonique.

2) Lorsqu'une information prévue par le RGPD est fournie dans le cadre d'échanges téléphoniques, il est admis que cette information puisse se limiter aux éléments les plus importants pour l'interlocuteur, afin de rester brève, à condition d'indiquer un moyen d'obtenir les informations complètes (exemples : touche à activer sur le téléphone, courriel reçu par l'interlocuteur, renvoi vers une page web). L'information sur le traitement des données transmises par les FAI, notamment les coordonnées téléphoniques des personnes, à des fins de prospection téléphonique, en application de l'article 14 du RGPD, et celle relative à l'enregistrement de la conversation, en application de l'article 13 du RGPD, peuvent par ailleurs être fusionnées.

CNIL, FR, 12 octobre 2023, Sanction, Société X, n° SAN-2023-015, publié, point 59

Voir aussi : CNIL, FR, 23 juin 2022, Sanction, n° SAN-2022-011, publié

Prospection commerciale – Information sur la source des données – Nature – Indication de l'acquisition des données auprès d'un « organisme spécialisé dans l'enrichissement de données » – Insuffisance

Un courrier de prospection commerciale doit être suffisamment précis dans l'indication de la source d'où proviennent les données du prospect, cette information étant de nature à garantir un traitement équitable et transparent à son égard, en particulier dans un contexte de reventes successives de données entre de multiples acteurs et dans l'hypothèse où le prospect souhaiterait exercer ses droits auprès du courtier en données dont il ignore l'identité.

La seule mention que les données ont été collectées auprès d'un « organisme spécialisé dans l'enrichissement de données » n'est pas suffisamment précise et est susceptible de caractériser un manquement à l'information des personnes, au sens de l'article 14 du RGPD.

CNIL, FR, 24 novembre 2022, Sanction, Société X, n° SAN-2022-021, publié, point 41

Attentes raisonnables de l'utilisateur – Recours à un symbole couramment utilisé en

informatique pour un usage inhabituel – Illicéité en l'absence d'information spécifique de l'utilisateur ou d'activation par défaut

Dans la symbolique couramment utilisée en informatique, le fait de cliquer sur « X » en haut à droite de la dernière fenêtre visible d'une application permet généralement de la quitter. En l'espèce, le fait de cliquer sur « X » ne fait en réalité que mettre l'application en arrière-plan et non la quitter. Eu égard au fait que des données à caractère personnel de l'utilisateur peuvent être communiquées à des tiers sans qu'il en ait nécessairement conscience, soit l'utilisateur doit se voir délivrer une information spécifique sur ce point, soit le comportement de réduction en arrière-plan ne doit pas être activé par défaut et c'est à l'utilisateur de le paramétrer manuellement.

Tout autre fonctionnement ne saurait correspondre aux attentes de l'utilisateur.

CNIL, FR, 10 novembre 2022, Sanction, Société X, n° SAN-2022-020, publié, points 59-63

Prospection commerciale – Modalités de délivrance de l'information aux personnes concernées – Insuffisance de liens insérés au pied de formulaires de collecte sur Internet

L'information aux personnes concernées ne figurant pas sur un support distinct des mentions légales et conditions générales mais étant uniquement accessible via des liens intitulés « Conditions générales » ou « Mentions légales », insérés au pied de formulaires de collecte des données à caractère personnel mis en ligne sur un site internet, ne permet pas à l'utilisateur de bénéficier d'une information suffisamment claire et accessible sur le traitement de ses données.

Une telle modalité de délivrance de l'information aux personnes concernées ne répond pas aux exigences de transparence et d'accessibilité prévues par le RGPD.

CNIL, P, 1er décembre 2021, Mise en demeure, Société X, n° MED-2021-131, non publié

En cas de collecte indirecte

Données n'ayant pas été collectées directement auprès de la personne concernée – Informations à fournir – Exception à l'obligation d'information – Données générées par le responsable du traitement dans le cadre de son propre processus – Inclusion

L'article 14, paragraphe 5, sous c), du règlement général sur la protection des données doit être interprété en ce sens que l'exception à l'obligation d'information de la personne concernée par le responsable du traitement, prévue à cette disposition, concerne indistinctement toutes les données à caractère personnel que le responsable du traitement n'a pas collectées directement auprès de la personne concernée, que ces données aient été obtenues par le responsable du traitement auprès d'une personne autre que la personne concernée ou qu'elles aient été générées par le responsable du traitement lui-même, dans le cadre de l'exercice de ses missions.

CJUE, 28 novembre 2024, Másdi, C-169/23

Transfert par une administration publique d'un État membre de données à caractère personnel en vue de leur traitement par une autre administration publique de ce même État sans information de la personne – Illicite

Les articles 10, 11 et 13 de la directive 95/46/CE du 24 octobre 1995 doivent être interprétés en ce sens qu'ils s'opposent à des mesures nationales qui permettent à une administration publique d'un État

membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement.

CJUE, 1er octobre 2015, Bara e.a, C-201/14

---

1) Administration fiscale – Traitement aux fins d'obtenir le droit de procéder à une mesure d'enquête – Fraude fiscale – Champ d'application matériel du RGPD – 2) Contrôle du juge – Obligation d'informations pesant sur le responsable de traitement, exemptions ou limitations – Conditions – 3) Limitation de la portée de l'obligation d'informer – Conditions

1) Le traitement de données à caractère personnel mis en œuvre par l'administration fiscale aux fins d'obtenir l'autorisation de procéder à des opérations de visite et saisies sur le fondement de l'article L. 16 B du livre des procédures fiscales, qui a pour finalité d'obtenir le droit de procéder à une mesure d'enquête pouvant donner lieu à la constatation d'une infraction ou d'un manquement à la législation fiscale, dans le but de percevoir l'impôt et de lutter contre la fraude fiscale, entre dans le champ d'application matériel du RGPD.

2) Dès lors, le juge doit notamment vérifier si, dans le litige qui lui est soumis, le responsable du traitement est tenu de fournir à la personne concernée les informations prévues à son article 14 ou si sont réunies les conditions des exceptions ou limitations à cette obligation d'information qu'il prévoit. En effet, si l'article 14 du RGPD soumet le responsable du traitement à l'obligation de fournir un certain nombre d'informations à la personne concernée lorsque les données à caractère personnel n'ont pas été collectées auprès d'elle, il résulte du paragraphe 5 de ce texte que cette obligation ne s'applique pas dans la mesure où elle est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement.

3) En outre, l'article 23 du RGPD prévoit que le droit de l'État membre auquel le responsable du traitement est soumis peut, par la voie de mesures législatives, limiter la portée de l'obligation d'informer la personne concernée par le traitement de données à caractère personnel prévue à l'article 14 du RGPD lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la prévention et la détection d'infractions pénales, les enquêtes et les poursuites en la matière et d'autres objectifs importants d'intérêt public général d'un État membre, notamment un intérêt économique ou financier important, y compris dans les domaines monétaire, budgétaire et fiscal.

Ainsi, l'administration fiscale n'a pas l'obligation de fournir à la personne concernée les informations prévues à l'article 14 de ce règlement si sont réunies les conditions de l'exception prévue au paragraphe 5 de ce texte ou des limitations prévues à l'article 23.

Cass, com., 1er juin 2023, n°21-18.558, B., points 10-15

Annuaires – Indexation de données à caractère personnel issues des réseaux sociaux – Information délivrée via un avertissement dans la politique de confidentialité – Insuffisance en l'espèce

Cas d'un annuaire ayant enrichi ses données en collectant les données publiquement accessibles sur des réseaux sociaux.

La circonstance que, dans le cadre de leur politique de confidentialité, certains réseaux sociaux auraient averti leurs membres de la possible indexation de leurs données par des moteurs de

recherche ne saurait les faire regarder comme déjà informés, au sens de la loi du 6 janvier 1978, de la possible agrégation de leurs données à caractère personnel à un service d'annuaire.

Eu égard à l'intérêt qui s'attache au respect des libertés et droits fondamentaux des vingt-cinq millions de personnes touchées par le traitement litigieux, et notamment au respect de leur vie privée, la société responsable de traitement n'est pas fondée à soutenir que l'information de ces personnes, dont elle avait les coordonnées dans son annuaire, exigeait des efforts disproportionnés par rapport à l'intérêt de la démarche au sens des dispositions du III de l'article 32 de la loi du 6 janvier 1978.

CE, 10ème/9ème SSR, 12 mars 2014, Société Pages Jaunes Groupe, n° 353193, T., point 9

Système de vidéoprotection installé dans une ville – Demande de communication d'une carte avec l'emplacement des caméras et des zones surveillées - Exclusion

Il résulte des articles 13 et 15 du RGPD, des dispositions des titres II et III de la loi informatique et libertés relatives aux obligations d'information et au droit d'accès, et des dispositions du code de la sécurité intérieure régissant spécifiquement la vidéoprotection, notamment l'article R. 253-6, que le responsable de traitement, s'il est tenu d'informer, d'une façon adaptée au contexte et aux objectifs poursuivis, sur l'existence de la vidéoprotection d'un territoire, d'une zone ou d'un bâtiment, et de fournir l'ensemble des mentions et informations prévues par ces textes, n'est pas tenu à ce titre de communiquer l'emplacement exact de chaque caméra. Ainsi, en l'espèce, la commune n'était pas tenue de fournir à la personne concernée une carte avec l'emplacement des caméras et des zones surveillées.

CNIL, P, 29 mai 2024, Courrier présidente, Commune de X, 27412, non publié

Droit d'accès au dossier médical du mineur – Conditions

Le droit d'accès au dossier médical du mineur fondé sur l'article L. 1111-7 du code de la santé publique peut être exercé par chacun des titulaires de l'autorité parentale, dans les conditions précisées par ce texte et après occultation des éventuelles mentions relatives à la vie privée de l'autre titulaire, aux données médicales. Le parent ne perd ce droit d'accès qu'en cas de retrait de la qualité de titulaire de l'autorité parentale prévus aux articles 378 et suivants du code civil.

CNIL, P, 1er juillet 2021, Mise en demeure, n°MED-2021-042, non publié

Exception d'efforts disproportionnés

Annuaires – Réutilisation de données publiées sur internet – Information des personnes au moyen de courriels lorsque les adresses électroniques des personnes concernées figurent dans la base de données utilisée – Effort disproportionné - Absence

Dans le cadre d'une collecte indirecte de données à caractère personnel, la CNIL considère, conformément à la délibération n°2024-041 du 25 janvier 2024 portant adoption de deux recommandations relatives à la réutilisation de données à caractère personnel publiées sur internet, que ce n'est que dans des hypothèses limitées que les éditeurs doivent pouvoir se prévaloir des dispositions de l'article 14.5.b du RGPD, autorisant les organismes ne collectant pas les données directement auprès des personnes concernées à ne pas informer celles-ci lorsqu'une telle information exigerait des « efforts disproportionnés ». En particulier, dès lors qu'une information individuelle peut être effectuée au moyen de l'envoi automatisé de courriels à chacune des adresses présentes dans la base de données, la Commission considère que l'effort à fournir pour y procéder n'est en principe

pas « disproportionné » et ce même lorsque les risques associés à la mise en œuvre du traitement sont faibles.

CNIL, P, 24 juillet 2024, mise en demeure, Société X, décision n° MED-2024-107, non publié

Traitement visant à recenser les personnes influentes à des fins de représentation d'intérêts – Intérêt légitime – Obligation d'information individuelle des personnes concernées – Absence d'efforts disproportionnés pour le responsable du traitement

Lorsqu'un traitement de données à caractère personnel, consistant en la collecte d'informations visant à recenser les personnes influentes auprès desquelles une entreprise souhaite représenter ses intérêts pour une opération d'influence spécifique est réalisé sur le fondement de l'intérêt légitime poursuivi par le responsable de traitement, le fait que les données en question étaient publiques et que les personnes concernées pouvaient raisonnablement s'attendre à ce que leurs données fassent l'objet d'un tel traitement ne constituent pas des motifs de nature à exempter le responsable de traitement de son obligation d'information des personnes concernées.

La responsabilité de s'assurer que l'information a bien été délivrée individuellement aux personnes concernées incombe au responsable de traitement et non au sous-traitant. La fourniture de cette information ne saurait constituer des efforts disproportionnés pour le responsable du traitement, dès lors qu'il dispose, en l'espèce, des informations utiles pour contacter les personnes concernées.

CNIL, FR, 26 juillet 2021, Sanction, Société X, n° SAN-2021-012, publié, points 74-85

Voir aussi : CE, 10ème/9ème SSR, 12 mars 2014, Société Pages Jaunes Groupe, n° 353193, T.

Collecte indirecte à partir de sources publiques – Éléments d'appréciation des efforts requis pour la fourniture de l'information

Lorsque des données à caractère personnel sont collectées par un responsable de traitement de manière indirecte à partir de sources publiques, il résulte de l'article 14 du RGPD que le responsable de traitement est tenu d'en informer individuellement les personnes concernées, sauf notamment si la fourniture de cette information est impossible en pratique ou requiert des efforts disproportionnés.

Pour apprécier le caractère proportionné des efforts requis pour la fourniture de l'information, il y a lieu d'apprécier notamment les ressources financières et humaines dont dispose le responsable du traitement, les moyens et renseignements dont dispose déjà le responsable du traitement pour procéder à cette information, ainsi que l'intérêt pour les personnes concernées de disposer de cette information, en prenant en compte le volume de données traitées, les usages qui peuvent en être fait et les éventuelles atteintes à la vie privée qui pourraient en résulter.

CNIL, P, 8 juillet 2021, Mise en demeure, Société X, n° MED-2021-043, non publié

Voir aussi : CE, 10ème/9èmeSSR, 12 mars 2014, Société Pages Jaunes Groupe, n°353193, T.

4.3 Accès

4.3.1 Généralités

1) Fourniture d'une première copie des données – Obligation du responsable de traitement – Demande motivée par un but étranger à ceux visés au considérant 63 RGPD – Inclusion – Application au dossier médical d'un patient – 2) Législation mettant à la charge de la personne concernée les frais d'une première copie de ses données – Illicéité

1) L'article 12, paragraphe 5, et l'article 15, paragraphes 1 et 3, du RGPD doivent être interprétés en ce sens que l'obligation de fournir à la personne concernée, à titre gratuit, une première copie de ses données à caractère personnel faisant l'objet d'un traitement s'impose au responsable du traitement même lorsque cette demande est motivée dans un but étranger à ceux visés au considérant 63, première phrase, dudit règlement.

L'article 15, paragraphe 3, première phrase, du RGPD doit être interprété en ce sens que dans le cadre d'une relation médecin/patient, le droit d'obtenir une copie des données à caractère personnel faisant l'objet d'un traitement implique qu'il soit remis à la personne concernée une reproduction fidèle et intelligible de l'ensemble de ces données. Ce droit suppose celui d'obtenir la copie intégrale des documents figurant dans son dossier médical qui contiennent, entre autres, lesdites données, si la fourniture d'une telle copie est nécessaire pour permettre à la personne concernée d'en vérifier l'exactitude et l'exhaustivité ainsi que pour garantir leur intelligibilité. S'agissant de données relatives à la santé de la personne concernée, ce droit inclut en tout état de cause celui d'obtenir une copie des données de son dossier médical contenant des informations telles que des diagnostics, des résultats d'examens, des avis de médecins traitants et tout traitement ou intervention administrés à celle-ci.

2) L'article 23, paragraphe 1, sous i), du règlement 2016/679 doit être interprété en ce sens qu'est susceptible de relever du champ d'application de cette disposition une législation nationale adoptée avant l'entrée en vigueur de ce règlement. Toutefois, une telle faculté ne permet pas d'adopter une législation nationale qui, en vue de protéger les intérêts économiques du responsable du traitement, met à la charge de la personne concernée les frais d'une première copie de ses données à caractère personnel faisant l'objet de ce traitement.

CJUE, 26 octobre 2023, FT, C-307/22

---

1) Opérations de traitement antérieures à la date d'entrée en application du RGPD – Application du RGPD – Conditions – 2) Informations communicables – Journaux de consultation – Inclusion – Identité des salariés ayant consulté les données – Exclusion en principe – 3) Qualité de cliente et d'ancienne salariée du RT de la personne concernée – Activité bancaire dans le cadre d'une mission réglementée – Absence d'incidence sur l'étendue du droit d'accès

L'article 15 du RGPD être interprété en ce sens que :

1) Il est applicable à une demande d'accès aux informations visées par cette disposition lorsque les opérations de traitement concernées par cette demande ont été effectuées avant la date d'entrée en application dudit règlement, mais que la demande a été présentée après cette date.

2) Le droit d'accès prévu à l'article 15 doit permettre à la personne concernée de s'assurer que les données à caractère personnel la concernant sont exactes et qu'elles sont traitées de manière licite. Pour ce faire, la copie que le responsable du traitement est tenu de fournir à la personne concernée doit contenir toutes les données à caractère personnel faisant l'objet d'un traitement, présenter l'ensemble des caractéristiques lui permettant d'exercer effectivement ses droits au titre dudit règlement et, par conséquent, reproduire intégralement et fidèlement ces données. Afin de garantir que les informations ainsi fournies soient faciles à comprendre, la reproduction d'extraits de documents, voire de documents entiers ou encore d'extraits de bases de données, qui contiennent, entre autres, les données à caractère personnel faisant l'objet d'un traitement peut s'avérer indispensable dans le cas où la contextualisation des données traitées est nécessaire pour en assurer l'intelligibilité. Les opérations de consultation des données par les salariés du responsable de traitement constituant un traitement, la personne dont les données personnelles sont consultées a droit à l'accès à ses données mais également aux informations en lien avec ces opérations telles qu'elles sont mentionnées à l'article 15 du RGPD. La date des consultations est de nature à permettre à la personne concernée d'obtenir confirmation que ses données à caractère personnel ont effectivement fait l'objet d'un traitement à un moment donné et constitue un élément permettant de vérifier sa licéité à cette date. En outre, l'article 15 prévoit la possibilité d'accéder à la finalité du traitement de consultation et les éventuels destinataires des données consultées.

Il en résulte que la cour dit pour droit que les informations relatives à des opérations de consultation des données à caractère personnel d'une personne, portant sur les dates et les finalités de ces opérations, constituent des informations que cette personne a le droit d'obtenir du responsable du traitement en vertu de cette disposition. En revanche, ladite disposition ne consacre pas un tel droit s'agissant des informations relatives à l'identité des salariés dudit responsable ayant procédé à ces opérations sous son autorité et conformément à ses instructions, à moins que ces informations soient indispensables pour permettre à la personne concernée d'exercer effectivement les droits qui lui sont conférés par ce règlement et à condition qu'il soit tenu compte des droits et des libertés de ces salariés.

3) La circonstance que le responsable du traitement exerce une activité bancaire dans le cadre d'une mission réglementée et que la personne dont les données à caractère personnel ont été traitées en sa qualité de cliente du responsable du traitement a été également l'employée de ce responsable est, en principe, sans incidence sur l'étendue du droit dont bénéficie cette personne en vertu de cette disposition.

CJUE, 22 juin 2023, Pankki S, C-579/21, points 57, 61-62, 65-66

Voir aussi : CJUE, 4 mai 2023, Österreichische Datenschutzbehörde, C-487/21, points 21, 32, 39 ; CE, 10ème chambre, 24 février 2022, M. A... B..., n° 447495, Inédit.

Droit d'accès de la personne concernée à ses données faisant l'objet d'un traitement – Fourniture d'une copie des données – Notion de « copie » – Notion d'« informations »

L'article 15, paragraphe 3, première phrase, du RGPD doit être interprété en ce sens que le droit d'obtenir de la part du responsable du traitement une copie des données à caractère personnel faisant l'objet d'un traitement implique qu'il soit remis à la personne concernée une reproduction fidèle et intelligible de l'ensemble de ces données. Ce droit suppose celui d'obtenir la copie d'extraits de documents voire de documents entiers ou encore d'extraits de bases de données qui contiennent, entre autres, lesdites données, si la fourniture d'une telle copie est indispensable pour permettre à la personne concernée d'exercer effectivement les droits qui lui sont conférés par ce règlement, étant souligné qu'il doit être tenu compte, à cet égard, des droits et libertés d'autrui.

L'article 15, paragraphe 3, troisième phrase, du RGPD doit être interprété en ce sens que la notion d'« informations » qu'il vise se rapporte exclusivement aux données à caractère personnel dont le responsable du traitement doit fournir une copie en application de la première phrase de ce paragraphe.

CJUE, 4 mai 2023, Österreichische Datenschutzbehörde, C-487/21

Droit d'accès à l'information sur les destinataires et les catégories de destinataires des données – Obligation de fournir l'identité même des destinataires, sauf impossibilité ou demande abusive

Le droit d'accès de la personne concernée aux données à caractère personnel la concernant, prévu par l'article 15, paragraphe 1, sous c) du RGPD, implique, lorsque ces données ont été ou seront communiquées à des destinataires, l'obligation pour le responsable du traitement de fournir à cette personne l'identité même de ces destinataires, à moins qu'il ne soit impossible de les identifier ou que ledit responsable du traitement ne démontre que les demandes d'accès de la personne concernée sont manifestement infondées ou excessives, au sens de l'article 12, paragraphe 5, du RGPD, auxquels cas celui-ci peut indiquer à cette personne uniquement les catégories de destinataires en cause.

CJUE, 12 janvier 2023, Österreichische Post, C-154/21

Directive 95/46/CE – Article 2, sous a) – Réponses écrites fournies par le candidat lors d'un examen professionnel – Annotations de l'examinateur relatives à ces réponses – Article 12, sous a) et b) – Étendue des droits d'accès et de rectification de la personne concernée

Les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examinateur relatives à ces réponses constituent des données à caractère personnel. Le candidat a, en principe, un droit d'accès à ces données.

CJUE, 20 décembre 2017, Nowak, C-434/16

Directive 95/46/CE – Facturation de la communication de données personnelles par une autorité publique – Admissible si le montant est inférieur ou égal au coût de la communication

L'article 12, sous a), de la directive 95/46/CE du 24 octobre 1995 (relatif au droit d'accès) ne s'oppose pas à la perception de frais à l'occasion de la communication par une autorité publique de données à caractère personnel.

En revanche, afin de garantir que les frais perçus à l'occasion de l'exercice du droit d'accès ne soient pas excessifs, leur montant ne doit pas excéder le coût de la communication de ces données. Il appartient à la juridiction nationale d'effectuer, au regard des circonstances de l'affaire au principal, les vérifications nécessaires.

CJUE, 12 décembre 2013, X, C-486/12

Directive 95/46/CE – Droit d'accès à l'information sur les destinataires et les catégories de destinataires des données – Durée de conservation de l'information sur les destinataires ou les catégories de destinataires

L'article 12, sous a), de la directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, impose aux États membres de prévoir un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Il appartient aux États membres dans la transposition de la directive 95/46/CE de fixer un délai de conservation de cette

information ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive 95/46, et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement.

Une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêt et obligation en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement. Il appartient à la juridiction nationale d'effectuer les vérifications nécessaires.

CJUE, 7 mai 2009, Rijkeboer, C-553/07

Contravention d'opposition à l'exercice du droit d'accès – Caractérisation de l'infraction

La contravention d'opposition à l'exercice du droit d'accès à une information nominative, prévue et réprimée par les articles 35 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction antérieure à la loi du 6 août 2004, 1er 3° du décret du 23 décembre 1981 et consistant dans la fourniture de données présentées sous une forme non directement intelligible, constitue une infraction instantanée, consommée à la date d'envoi de l'information à la personne titulaire du droit d'accès. Ne caractérisent pas la réitération de cette infraction, les réponses faites ultérieurement aux réclamations du titulaire du droit d'accès se plaignant de l'absence de clarté des informations données.

Justifie, dès lors, sa décision, la cour d'appel qui constate l'extinction de l'action publique par la prescription après avoir retenu qu'il s'était écoulé plus d'une année entre l'envoi des informations au titulaire du droit d'accès et la plainte adressée par lui au procureur de la République.

Cass, crim., 6 mai 2008, n° 07-82.000, B., points 2-3

Demande présentée de manière non précise compte tenu de la quantité de données personnelles traitées par un fichier – Restriction de l'accès– Licéité - Conditions

Il résulte, d'une part, des dispositions du RGPD, telles qu'elles sont en particulier commentées notamment par les § 62 et 63 du préambule de ce règlement ou par les lignes directrices du Comité européen de la protection des données personnelles, que des restrictions à l'accès peuvent être prononcées lorsqu'en particulier, les demandes sont présentées de manière non précise compte tenu de la quantité de données personnelles traitées par un fichier et, d'autre part, des articles 49 et 107 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, que d'autres restrictions peuvent être apportées à ce droit d'accès compte tenu notamment des caractéristiques des données en cause.

CE, 10ème, 31 décembre 2024, n° 488201, Inédit, point 5

Droit d'accès de toute personne physique aux données la concernant (art. 39 de la loi Informatique et Libertés) – Obligation du responsable du traitement de transmettre ces données, sauf demande abusive – Communication faite préalablement au

mandataire de la personne – Circonstance ne levant pas l'obligation de donner accès à la personne concernée

Aux termes de l'article 39 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés, toute personne peut à tout moment avoir accès aux données à caractère personnel la concernant contenues dans un fichier. Cet article fait obligation au responsable du traitement de transmettre au demandeur les données dont il sollicite la communication, sauf si la demande présente un caractère abusif. La circonstance que le responsable du traitement a auparavant répondu favorablement à une demande de l'avocat de l'intéressé, formulée dans le cadre d'un litige avec son employeur, est sans influence sur l'existence de l'obligation.

CE, 10ème/9ème SSR, 20 octobre 2010, Société Centrapel, n°327916, T., point 3

Demande d'accès à une information détenue par la société employeur du demandeur et par la société à laquelle la mise en œuvre du traitement automatisé a été confiée – Demande pouvant être adressée à cette dernière, sans que la clause de confidentialité figurant dans la convention entre ces deux sociétés puisse être opposée

Le requérant qui demandait l'accès à une information nominative le concernant dans l'exercice de sa profession, était en droit d'adresser cette demande soit auprès de la société qui l'employait soit à la société à laquelle la mise en œuvre du traitement automatisé avait été confiée en vertu d'un contrat de prestation de service passé entre les deux sociétés, sans que la clause de confidentialité figurant dans la convention entre ces deux sociétés puisse lui être opposée.

CE, Section, 14 juin 1999, Société TVF, n° 197751, T., point 5

Système de vidéoprotection installé dans une ville – Demande de communication d'une carte avec l'emplacement des caméras et des zones surveillées - Exclusion

Il résulte des articles 13 et 15 du RGPD, des dispositions des titres II et III de la loi informatique et libertés relatives aux obligations d'information et au droit d'accès, et des dispositions du code de la sécurité intérieure régissant spécifiquement la vidéoprotection, notamment l'article R. 253-6, que le responsable de traitement, s'il est tenu d'informer, d'une façon adaptée au contexte et aux objectifs poursuivis, sur l'existence de la vidéoprotection d'un territoire, d'une zone ou d'un bâtiment, et de fournir l'ensemble des mentions et informations prévues par ces textes, n'est pas tenu à ce titre de communiquer l'emplacement exact de chaque caméra. Ainsi, en l'espèce, la commune n'était pas tenue de fournir à la personne concernée une carte avec l'emplacement des caméras et des zones surveillées.

CNIL, P, 29 mai 2024, Courrier présidente, Commune de X, 27412, non publié

Droit d'accès au dossier médical du mineur – Conditions

Le droit d'accès au dossier médical du mineur fondé sur l'article L. 1111-7 du code de la santé publique peut être exercé par chacun des titulaires de l'autorité parentale, dans les conditions précisées par ce texte et après occultation des éventuelles mentions relatives à la vie privée de l'autre titulaire, aux données médicales. Le parent ne perd ce droit d'accès qu'en cas de retrait de la qualité de titulaire de l'autorité parentale prévus aux articles 378 et suivants du code civil.

CNIL, P, 1er juillet 2021, Mise en demeure, n°MED-2021-042, non publié

Délai

Délai d'exercice du droit d'accès – Exigence d'équilibre entre l'intérêt de la personne à protéger sa vie privée et la charge que l'obligation de conservation représente pour le responsable de traitement – Illustration

Il appartient aux États membres de fixer un délai de conservation des informations détenues sur les destinataires de données ainsi qu'un accès corrélatif à celles-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive 95/46, et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement.

Une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêts et obligations en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement. Il appartient à la juridiction nationale d'effectuer les vérifications nécessaires.

CJUE, 7 mai 2009, Rijkeboer, C-553/07

4.3.2 Droit d'accès aux traitements ne relevant pas du droit de l'Union

Fichier intéressant la sûreté de l'État ou la défense – Ayant droit d'une personne décédée – Qualité de personne concernée – Absence – Droit d'accès ou possibilité de solliciter un accès indirect aux données à caractère personnel figurant dans le traitement – Absence

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés n'ouvre la possibilité de demander la communication de données à caractère personnel figurant dans un traitement automatisé ou de solliciter un accès indirect à de telles données qu'à la personne concernée par celles-ci. La seule qualité d'ayant droit de son père décédé dont se prévaut une personne ne lui confère pas la qualité de personne concernée par les données susceptibles de concerner son père dans un fichier intéressant la sûreté de l'État ou la défense.

CE, Formation spécialisée, 2 décembre 2019, M. B... A..., n° 420917, Inédit., point 4

Droit d'accès indirect aux données à caractère personnel contenues dans des fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique (art. 41 de la loi du 6 janvier 1978) – Mise en œuvre – 1) Principe – Modalités de communication des informations au demandeur définies par le responsable de traitement (art. 88 du décret du 20 octobre 2005) – 2) Application – Obligation de remettre au demandeur une copie de ces informations – Absence

Il ressort des articles 41 de la loi n°78-17 du 6 janvier 1978 et 88 du décret n° 2005-1309 du 20 octobre 2005 dans leur rédaction applicable au litige que, dans le cadre du droit d'accès indirect aux données à caractère personnel contenues dans l'un des fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique, le responsable du traitement communique les informations sollicitées à la personne concernée selon les modalités qu'il définit.

Le ministre de l'intérieur, qui n'était pas tenu de remettre au requérant une copie des documents consultés, a pu valablement exécuter l'injonction qui lui était faite en s'assurant que le requérant puisse consulter les données sollicitées en préfecture. Il s'ensuit qu'en jugeant que le ministre de l'intérieur n'avait pas complètement exécuté l'injonction qui lui était faite en ne délivrant pas au requérant une copie des documents consultés, une cour administrative d'appel entache son arrêt d'erreur de droit.

CE, 10ème–9ème chambres réunies, 24 octobre 2019, M. B., n° 427204, T., point 3

Fichier intéressant la sûreté de l'État, la défense et la sécurité publique (article 39) – 1) Divisibilité des informations contenues dans ces fichiers – Existence – 2) Possibilité d'accéder directement aux informations contenues dans les fichiers – Existence – Informations ne remettant pas en cause les fins assignées au traitement

1) Un fichier intéressant la sûreté de l'État, la défense et la sécurité publique au sens de l'article 39 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés, peut comprendre, d'une part, des informations dont la communication à l'intéressé serait susceptible de mettre en cause les fins assignées à ce traitement et, d'autre part, des informations dont la communication ne mettrait pas en cause ces mêmes fins.

2) Pour l'accès aux informations susceptibles de mettre en cause les fins assignées au traitement, il incombe, en application de l'article 39 de la loi Informatique et Libertés, à la Commission nationale de l'informatique et des libertés, saisie par la personne visée par ces informations, de l'informer qu'il a été procédé aux vérifications nécessaires. Pour l'accès aux informations qui ne sont pas susceptibles de mettre en cause les fins assignées au traitement, il appartient au gestionnaire du traitement ou à la Commission nationale de l'informatique et des libertés, saisie par la personne visée, de lui en donner communication avec, pour la commission, l'accord du gestionnaire du traitement.

CE, Section, 6 novembre 2002, M.X, n° 194295, Rec., point 5

4.3.3 Limitations du fait des droits des tiers

Article 15, paragraphe 4, RGPD – Droit d'obtenir copie de ses données à caractère personnel – Limite

Il résulte clairement des dispositions du paragraphe 4 de l'article 15 du RGPD que le droit, pour une personne dont les données à caractère personnel sont traitées, d'obtenir une copie de ces dernières, ne doit pas porter atteinte aux droits et libertés d' « autrui », c'est-à-dire d'autres personnes que le demandeur. En particulier, aucune disposition de ce règlement n'exclut de cette catégorie les destinataires des données qui ont eux-mêmes la qualité de personne concernée à l'égard des données demandées.

CE, 10ème chambre, 24 février 2022, M. A... B..., n° 447495, Inédit., point 7

Contexte d'exercice du droit d'accès – Litige – Procédure judiciaire

Le droit d'accès peut être exercé dans un contexte litigieux ou en parallèle d'une procédure judiciaire, sous réserve, notamment, des limites prévues par le RGPD et le code de la santé publique.

CNIL, P, 1er juillet 2021, Mise en demeure, Pharmacie de X, n°MED-2021-042, non publié

La confirmation de la présence ou non dans un traitement ne porte en principe pas atteinte aux droits et libertés d'autrui. – Application dans le cadre d'un contrat d'assurance-vie

Le droit d'accès de la personne concernée comprend plusieurs composantes : la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées, l'accès auxdites données le cas échéant et la fourniture d'informations sur le traitement concerné. Les limitations à l'exercice du droit d'accès rendues nécessaires par les dispositions de l'article 15.4 du RGPD, qui prévoient que le droit d'obtenir une copie des données ne porte pas atteinte aux droits et libertés d'autrui, ne peuvent pas en principe concerner la confirmation que des données font ou non l'objet d'un traitement.

Il s'ensuit que le bénéficiaire non acceptant ou n'étant pas en mesure d'apporter la preuve de son acceptation du bénéfice du contrat d'assurance-vie doit pouvoir recevoir confirmation ou non de sa présence dans le traitement de gestion du fichier des contrats de capitalisation et d'assurance vie dénommé FICOVIE, quand bien même des restrictions concernant l'accès aux données enregistrées dans ce traitement peuvent être appliquées à ces catégories de personnes en application de l'article 15.4 du RGPD.

CNIL, SP, 25 février 2021, Avis sur projet d'arrêté, FICOVIE, n° 2021-025, publié, points 10-12

4.3.4 Droit d'accès des tiers

Possibilité de communication orale à toute personne de données relatives à des condamnations pénales d'une personne physique figurant dans un fichier– 1) Illicéité – 2) Nature du demandeur de société commerciale ou un particulier – Indifférence

1) Les dispositions du règlement 2016/679, notamment l'article 6, paragraphe 1, sous e), et l'article 10 de celui-ci, doivent être interprétées en ce sens qu'elles s'opposent à ce que des données relatives à des condamnations pénales d'une personne physique figurant dans un fichier tenu par une juridiction puissent être communiquées oralement à toute personne aux fins de garantir un accès du public à des documents officiels, sans que la personne demandant la communication ait à justifier d'un intérêt spécifique à obtenir lesdites données.

2) La circonstance que cette personne soit une société commerciale ou un particulier n'ayant pas d'incidence à cet égard.

CJUE, 7 mars 2024, Endemol Shine Finland, C-740/22, point 59

Directive 95/46/CE – Demande de communication des données personnelles d'une personne responsable d'un accident de la circulation afin d'exercer un droit en justice – Obligation du responsable du traitement de faire droit à une telle demande – Absence

L'article 7, sous f), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 doit être interprété en ce sens qu'il n'impose pas l'obligation de communiquer des données à caractère personnel à un tiers afin de lui permettre d'introduire un recours en indemnisation devant une juridiction civile pour un dommage causé par la personne concernée par la protection de ces données. Toutefois, l'article 7, sous f), de cette directive ne s'oppose pas à une telle communication sur la base du droit national.

CJUE, 4 mai 2017, Rīgas satiksme, C-13/16

Directive 95/46/CE – Article 6, paragraphe 1, sous e) – Données soumises à la publicité au registre des sociétés – Première directive 68/151/CEE – Article 3 – Dissolution de la société concernée – Limitation de l'accès des tiers à ces données – Exception – Compétence des États membres

L'ingérence dans le droit à la vie privée et à la protection des données à caractère personnel qu'emporte la publicité des données nominatives contenues dans le registre des sociétés n'est pas disproportionnée eu égard au nombre de données concernées et au fait qu'elle vise à assurer la sécurité juridique dans les rapports entre les sociétés et les tiers ainsi qu'à protéger les intérêts des tiers par rapport aux sociétés par actions et aux sociétés à responsabilité limitée.

Il ne peut donc être garanti aux personnes physiques dont les données sont inscrites dans le registre des sociétés le droit d'obtenir, après un certain délai à compter de la dissolution de la société, l'effacement des données à caractère personnel les concernant.

En revanche, les États membres peuvent exceptionnellement déroger à cette exigence de publicité. Il leur appartient de déterminer si les personnes physiques, visées à l'article 2, paragraphe 1, sous d) et j) de la directive 68/151/CEE, à savoir, d'une part, les personnes qui ont le pouvoir d'engager une société à l'égard des tiers et de la représenter en justice et celles qui participent à l'administration, à la surveillance ou au contrôle de la société et, d'autre part, les liquidateurs d'une société, peuvent demander à l'autorité chargée de la tenue, respectivement, du registre central, du registre du commerce ou du registre des sociétés de vérifier, sur la base d'une appréciation au cas par cas, s'il est exceptionnellement justifié, pour des raisons prépondérantes et légitimes tenant à leur situation particulière, de limiter, à l'expiration d'un délai suffisamment long après la dissolution de la société concernée, l'accès aux données à caractère personnel les concernant, inscrites dans ce registre, aux tiers justifiant d'un intérêt spécifique à la consultation de ces données.

CJUE, 9 mars 2017, Manni, C-398/15

Mesure de communication de bulletins de salaire par le juge sur le fondement des articles 6 et 8 de la CESDH, de l'article 9 du code civil et de l'article 9 du code de procédure civile – Communication nécessaire à l'exercice ou à la défense d'un droit en justice – Licéité – Conditions

Il résulte du point (4) de l'introduction du RGPD, que le droit à la protection des données à caractère personnel n'est pas un droit absolu et doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité, en particulier le droit à un recours effectif et à accéder à un tribunal impartial. Selon l'article 145 du code de procédure civile, s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé. Il résulte par ailleurs des articles 6 et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 9 du code civil et 9 du code de procédure civile, que le droit à la preuve peut justifier la production d'éléments portant atteinte à la vie personnelle à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi. Doit en conséquence être approuvé l'arrêt qui ordonne à l'employeur de communiquer à une salariée les bulletins de salaires d'autres salariés occupant des postes de niveau comparable au sien avec occultation des données personnelles à l'exception des noms et prénoms, de la classification conventionnelle et de la rémunération, après avoir relevé que cette communication d'éléments portant atteinte à la vie personnelle d'autres salariés était indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, soit la défense de l'intérêt légitime de la salariée à l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail.

Cass, soc., 8 mars 2023, n° 21-12.492, points 5-10

4.4 Rectification

Droit de libre circulation et de libre séjour sur le territoire des États membres –- Obligation de reconnaissance du changement de prénom et d'identité de genre dans un autre Etat membre – Rectification de l'acte d'état civil

L'article 20 et l'article 21, paragraphe 1, TFUE, lus à la lumière des articles 7 et 45 de la charte des droits fondamentaux de l'Union européenne doivent être interprétés en ce sens qu'ils s'opposent à une réglementation d'un État membre qui ne permet pas de reconnaître et d'inscrire dans l'acte de naissance d'un ressortissant de cet État membre le changement de prénom et d'identité de genre légalement acquis dans un autre État membre lors de l'exercice de sa liberté de circulation et de séjour, avec pour conséquence de le contraindre à engager une nouvelle procédure, de type juridictionnel, de changement d'identité de genre dans ce premier État membre, laquelle fait abstraction de ce changement déjà légalement acquis dans cet autre État membre.

CJUE, 4 octobre 2024, Mirin, C-4/23

Fichiers de police – Refus de rectification – Absence de justification de l'exactitude des mentions – Faute susceptible d'engager la responsabilité de l'État

Le refus de l'administration de rectifier des fiches de police communiquées à d'autres services constitue, en l'absence de preuve de faits susceptibles de justifier l'exactitude des mentions figurant dans ces fiches, une faute de nature à engager la responsabilité de l'État.

CE, Section, 13 mai 1987, M. X, n° 51779, T., point 3

4.5 Effacement

4.5.1 Portée

Absence d'accord déterminant la responsabilité conjointe du traitement et de la tenue du registre des activités de traitement – Conséquences – Droit à l'effacement – Absence

L'article 17, paragraphe 1, sous d), et l'article 18, paragraphe 1, sous b), du RGPD doivent être interprétés en ce sens que la méconnaissance, par le responsable du traitement, des obligations prévues aux articles 26 et 30 de ce règlement, relatives, respectivement, à la conclusion d'un accord déterminant la responsabilité conjointe du traitement et à la tenue d'un registre des activités de traitement, ne constitue pas un traitement illicite conférant à la personne concernée un droit à l'effacement ou à la limitation du traitement, dès lors qu'une telle méconnaissance n'implique pas, en tant que telle, une violation par le responsable du traitement du principe de « responsabilité » tel qu'énoncé à l'article 5, paragraphe 2, dudit règlement, lu conjointement avec l'article 5, paragraphe 1, sous a), et l'article 6, paragraphe 1, premier alinéa, de ce dernier.

CJUE, 4 mai 2023, Bundesrepublik Deutschland, C-60/22

Recherche effectuée à partir du nom d'une personne sur un moteur de

recherche – 1) Affichage d'un lien menant vers des articles contenant des informations prétendument inexactes dans la liste de résultats – Demande de déréférencement – Conditions – 2) Résultats d'une recherche d'images de cette personne – Demande de déréférencement – Conditions

1) L'article 17, paragraphe 3, sous a), du RGPD doit être interprété en ce sens que dans le cadre de la mise en balance qu'il convient d'opérer entre les droits visés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, d'une part, et ceux visés à l'article 11 de la Charte des droits fondamentaux, d'autre part, aux fins de l'examen d'une demande de déréférencement adressée à l'exploitant d'un moteur de recherche et tendant à ce que soit supprimé de la liste de résultats d'une recherche le lien menant vers un contenu comportant des allégations que la personne ayant introduit la demande estime inexactes, ce déréférencement n'est pas soumis à la condition que la question de l'exactitude du contenu référencé ait été résolue, au moins à titre provisoire, dans le cadre d'un recours intenté par cette personne contre le fournisseur de contenu.

2) L'article 17, paragraphe 3, sous a), du RGPD doit être interprété en ce sens que dans le cadre de la mise en balance qu'il convient d'opérer entre les droits visés aux articles 7 et 8 de la Charte des droits fondamentaux, d'une part, et ceux visés à l'article 11 de la Charte des droits fondamentaux, d'autre part, aux fins de l'examen d'une demande de déréférencement adressée à l'exploitant d'un moteur de recherche et tendant à ce que soient supprimées des résultats d'une recherche d'images effectuée à partir du nom d'une personne physique des photographies affichées sous la forme de vignettes qui représentent cette personne, il y a lieu de tenir compte de la valeur informative de ces photographies indépendamment du contexte de leur publication sur la page internet d'où elles sont extraites, mais en prenant en considération tout élément textuel qui accompagne directement l'affichage de ces photographies dans les résultats de recherche et qui est susceptible d'apporter un éclairage sur la valeur informative de celles-ci.

CJUE, grande chambre, 8 décembre 2022, Google, C-460/20

Moteurs de recherche sur Internet – Traitement des données contenues dans des sites web – Catégories de données spécifiques visées à l'article 8 de cette directive et aux articles 9 et 10 de ce règlement – Applicabilité de ces articles à l'exploitant du moteur de recherche – 1) Portée des obligations de cet exploitant au regard desdits articles – 2) Publication des données sur des sites web aux seules fins de journalisme ou d'expression artistique ou littéraire – 3) Incidence sur le traitement d'une demande de déréférencement

1) Les dispositions de l'article 8, paragraphes 1 et 5, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doivent être interprétées en ce sens que l'interdiction ou les restrictions relatives au traitement des catégories particulières de données à caractère personnel, visées par ces dispositions, s'appliquent, sous réserve des exceptions prévues par cette directive, également à l'exploitant d'un moteur de recherche dans le cadre de ses responsabilités, de ses compétences et de ses possibilités en tant que responsable du traitement effectué lors de l'activité de ce moteur, à l'occasion d'une vérification opérée par cet exploitant, sous le contrôle des autorités nationales compétentes, à la suite d'une demande introduite par la personne concernée.

2) Les dispositions de l'article 8, paragraphes 1 et 5, de la directive 95/46 doivent être interprétées en ce sens que, en vertu de celles-ci, l'exploitant d'un moteur de recherche est en principe obligé, sous réserve des exceptions prévues par cette directive, de faire droit aux demandes de déréférencement portant sur des liens menant vers des pages web sur lesquelles figurent des données à caractère personnel qui relèvent des catégories particulières visées par ces dispositions.

L'article 8, paragraphe 2, sous e), de la directive 95/46 doit être interprété en ce sens que, en application de celui-ci, un tel exploitant peut refuser de faire droit à une demande de déréférencement

lorsqu'il constate que les liens en cause mènent vers des contenus comportant des données à caractère personnel qui relèvent des catégories particulières visées à cet article 8, paragraphe 1, mais dont le traitement est couvert par l'exception prévue audit article 8, paragraphe 2, sous e), à condition que ce traitement réponde à l'ensemble des autres conditions de licéité posées par cette directive et à moins que la personne concernée n'ait, en vertu de l'article 14, premier alinéa, sous a), de ladite directive, le droit de s'opposer audit traitement pour des raisons prépondérantes et légitimes tenant à sa situation particulière.

Les dispositions de la directive 95/46 doivent être interprétées en ce sens que, lorsque l'exploitant d'un moteur de recherche est saisi d'une demande de déréférencement portant sur un lien vers une page web sur laquelle des données à caractère personnel relevant des catégories particulières visées à l'article 8, paragraphe 1 ou 5, de cette directive sont publiées, cet exploitant doit, sur la base de tous les éléments pertinents du cas d'espèce et compte tenu de la gravité de l'ingérence dans les droits fondamentaux de la personne concernée au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, vérifier, au titre des motifs d'intérêt public important visés à l'article 8, paragraphe 4, de ladite directive et dans le respect des conditions prévues à cette dernière disposition, si l'inclusion de ce lien dans la liste de résultats, qui est affichée à la suite d'une recherche effectuée à partir du nom de cette personne, s'avère strictement nécessaire pour protéger la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page web au moyen d'une telle recherche, consacrée à l'article 11 de cette charte.

3) Les dispositions de la directive 95/46 doivent être interprétées en ce sens que,

a) d'une part, les informations relatives à une procédure judiciaire dont une personne physique a été l'objet ainsi que, le cas échéant, celles relatives à la condamnation qui en a découlé constituent des données relatives aux « infractions » et aux « condamnations pénales », au sens de l'article 8, paragraphe 5, de cette directive, et

b) d'autre part, l'exploitant d'un moteur de recherche est tenu de faire droit à une demande de déréférencement portant sur des liens vers des pages web, sur lesquelles figurent de telles informations, lorsque ces informations se rapportent à une étape antérieure de la procédure judiciaire en cause et ne correspondent plus, compte tenu du déroulement de celle-ci, à la situation actuelle, dans la mesure où il est constaté, dans le cadre de la vérification des motifs d'intérêt public important visés à l'article 8, paragraphe 4, de ladite directive, que, eu égard à l'ensemble des circonstances de l'espèce, les droits fondamentaux de la personne concernée, garantis par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, prévalent sur ceux des internautes potentiellement intéressés, protégés par l'article 11 de cette charte.

CJUE, grande chambre, 24 septembre 2019, GC e.a, C-136/17

Portée territoriale du déréférencement – Exploitant d'un moteur de recherche faisant droit à une demande de déréférencement – Obligation d'opérer le déréférencement sur ses versions correspondant à l'ensemble des États membres – Mesures complémentaires en cas de nécessité

L'article 12, sous b), et l'article 14, premier alinéa, sous a), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ainsi que l'article 17, paragraphe 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46 (règlement général sur la protection des données), doivent être interprétés en ce sens que, lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement en application de ces dispositions, il est tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur, mais sur les versions de celui-ci correspondant à l'ensemble des États membres, et ce, si

nécessaire, en combinaison avec des mesures qui, tout en satisfaisant aux exigences légales, permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des États membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès aux liens qui font l'objet de cette demande.

CJUE, grande chambre, 24 septembre 2019, Google, C-507/17

Directive 95/46, articles 12 et 14 – 1) Droit d'accès de la personne concernée aux données à caractère personnel et droit d'opposition à leur traitement – Droit de demander la suppression de la liste de résultats des liens vers des pages web – 2) Conditions

1) Les articles 12 b), et 14 a), de la directive 95/46, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doivent être interprétés en ce sens que, afin de respecter les droits prévus à ces dispositions et pour autant que les conditions prévues par celles-ci sont effectivement satisfaites, l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite.

À cet égard, dans la mesure où l'inclusion dans la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, d'une page web et des informations qui y sont contenues relatives à cette personne facilite sensiblement l'accessibilité de ces informations à tout internaute effectuant une recherche sur la personne concernée et peut jouer un rôle décisif pour la diffusion desdites informations, le traitement des données réalisé par l'exploitant d'un moteur de recherche est susceptible de constituer une ingérence plus importante dans le droit fondamental au respect de la vie privée de la personne concernée que la publication par l'éditeur de cette page web.

2) Les articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46 doivent être interprétés en ce sens que, dans le cadre de l'appréciation des conditions d'application de ces dispositions, il convient notamment d'examiner si la personne concernée a un droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne. Cette dernière pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander que l'information en question ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats, ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question.

CJUE, 13 mai 2014, Google Spain, C-131/12, points 87-88

Données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté – Demande de déréférencement – Conditions d'appréciation du bien-fondé de la demande – Application

Il résulte des articles 9, 38 et 40 de la loi n°78-17 du 6 janvier 1978, dite loi informatique et libertés, qui doivent être interprétés à la lumière de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, et de l'arrêt rendu le 24 septembre 2019 par la Cour de justice de l'Union européenne (GC e.a. contre Commission nationale de l'informatique et des libertés, C-136/17) que, lorsqu'une juridiction est saisie d'une demande de déréférencement portant sur un lien vers une page internet sur laquelle des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté sont publiées, elle doit, pour porter une appréciation sur son bien-fondé, vérifier, de façon concrète, si l'inclusion du lien litigieux dans la liste des résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, répond à un motif d'intérêt public important, tel que le droit à l'information du public, et si elle est strictement nécessaire pour assurer la préservation de cet intérêt.

Dès lors, ne donne pas de base légale à sa décision une cour d'appel qui rejette une demande de déréférencement portant sur des liens permettant d'accéder à des comptes-rendus d'audience relatant une condamnation pénale, publiés sur le site internet d'un journal, sans rechercher, comme il le lui incombait, si, compte tenu de la sensibilité des données en cause et, par suite, de la particulière gravité de l'ingérence dans les droits de l'intéressé au respect de sa vie privée et à la protection de ses données à caractère personnel, l'inclusion des liens litigieux dans la liste des résultats était strictement nécessaire pour protéger la liberté d'information des internautes potentiellement intéressés à avoir accès aux pages internet concernées.

Cass, 1re civ., 27 novembre 2019, n° 18-14.675, B., points 9, 11

Appréciation du bien-fondé d'une demande de déréférencement – Mise en balance des intérêts – Illégalité d'une injonction d'ordre général

La juridiction saisie d'une demande de déréférencement est tenue de porter une appréciation sur son bien-fondé et de procéder, de façon concrète, à la mise en balance des intérêts en présence, de sorte qu'elle ne peut ordonner une mesure d'injonction d'ordre général conférant un caractère automatique à la suppression de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages internet contenant des informations relatives à cette personne.

Dès lors, viole les articles 38 et 40 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le second dans sa rédaction applicable au litige issue de la loi n° 2004-801 du 6 août 2004, ensemble l'article 5 du code civil, une cour d'appel qui, saisie d'une telle demande, prononce une injonction d'ordre général et sans procéder, comme il le lui incombait, à la mise en balance des intérêts en présence.

Cass, 1re civ., 14 février 2018, n° 17-10.499, B., points 6, 9

Consultation du registre paroissial et publicité limitée – Refus d'effacement – Absence d'atteinte au droit au respect de la vie privée

La consultation du registre paroissial portant mention du baptême d'une personne, à l'âge de deux ans, et de son reniment en 2001 n'est ouverte, l'intéressé mis à part, qu'aux ministres du culte, eux-mêmes tenus au secret. En outre, la seule publicité donnée à ces deux événements émanait de la personne elle-même. Dans ces circonstances, la cour d'appel a pu retenir que cette dernière ne pouvait

invoquer aucune atteinte au droit au respect de sa vie privée du fait du refus d'effacement de la mention de son baptême sur le registre paroissial.

Cass, 1re civ., 19 novembre 2014, n° 13-25.156, B., points 3, 5

Droit au déréférencement – Portée territoriale – 1) Portée des obligations pesant sur l'exploitant d'un moteur de recherche en vertu du droit de l'UE – Obligation de déréférencement à l'échelle de l'UE – Existence – Obligation de déréférencement mondial – Absence – 2) Faculté de la CNIL d'imposer un déréférencement mondial – a) Absence, faute de disposition législative prévoyant un déréférencement excédant le champ couvert par le droit de l'UE – b) En tout état de cause, exercice d'une telle faculté subordonné par la CJUE à une mise en balance entre le droit au respect de la vie privée et à la protection des données à caractère personnel et le droit à la liberté d'information

Exploitant d'un moteur de recherche demandant l'annulation de la délibération de la formation restreinte de la CNIL le sanctionnant pour ne s'être pas conformé à la mise en demeure qui lui avait été adressée de faire droit aux demandes de déréférencement de personnes physiques en supprimant de la liste des résultats affichés l'ensemble des liens menant vers les pages web litigieuses sur toutes les extensions de nom de domaine de son moteur de recherche.

1) Par un arrêt du 24 septembre 2019, Google LLC contre CNIL (C-507/17), la CJUE a dit pour droit que l'article 17, paragraphe 1, du règlement (UE) 2016/679 du 27 avril 2016 doit être interprété en ce sens que, lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement en application de ces dispositions, il est tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur, mais sur les versions de celui-ci correspondant à l'ensemble des États membres et ce, si nécessaire, en combinaison avec des mesures qui, tout en satisfaisant aux exigences légales, permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des États membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès aux liens qui font l'objet de cette demande.

Il en résulte que la formation restreinte de la CNIL a entaché sa délibération d'erreur de droit en sanctionnant l'exploitant au motif que seule une mesure de déréférencement s'appliquant à l'intégralité du traitement lié au moteur de recherche, sans considération des extensions interrogées et de l'origine géographique de l'internaute effectuant une recherche, est à même de répondre à l'exigence de protection telle qu'elle a été consacrée par la CJUE.

2) a) Si la CNIL soutient en défense que la sanction contestée trouve son fondement dans la faculté que la Cour de justice a reconnue aux autorités de contrôle d'ordonner de procéder à un déréférencement portant sur l'ensemble des versions d'un moteur de recherche, il ne résulte, en l'état du droit applicable, d'aucune disposition législative qu'un tel déréférencement pourrait excéder le champ couvert par le droit de l'Union européenne pour s'appliquer hors du territoire des États membres de l'Union européenne.

b) Au surplus, il résulte en tout état de cause des énonciations du point 72 de l'arrêt de la CJUE du 24 septembre 2019 qu'une telle faculté ne peut être ouverte qu'au terme d'une mise en balance entre, d'une part, le droit de la personne concernée au respect de sa vie privée et à la protection des données à caractère personnel la concernant et, d'autre part, le droit à la liberté d'information. Or, il ressort des termes mêmes de la délibération attaquée que, pour constater l'existence de manquements persistants et reprocher à la société requérante d'avoir méconnu l'obligation de principe de procéder au déréférencement portant sur l'ensemble des versions d'un moteur de recherche, la formation restreinte de la CNIL n'a pas effectué une telle mise en balance.

CE, 10ème-9ème chambres réunies, 27 mars 2020, Société Google Inc, n° 399922, Rec., points 7-10

Évaluation de la minorité de personnes étrangères – Dispositif d'effacement des données du traitement en cas d'établissement de la nationalité française

À l'occasion de l'examen d'un projet de décret relatif aux modalités d'évaluation des personnes se déclarant mineures et privées temporairement ou définitivement de la protection de leur famille et autorisant la création d'un traitement de données à caractère personnel relatif à ces personnes, le Conseil d'État (section de l'intérieur) introduit, à l'article R. 221-15-5 du code de l'action sociale et des familles, une disposition visant à effacer les données à caractère personnel relatives à des personnes dont il serait établi au cours de la procédure d'évaluation de la minorité qu'elles sont de nationalité française.

En effet dès qu'il est établi que l'intéressé est français, l'effacement des données du traitement, au regard de ses finalités, s'impose en tant que la vocation du traitement est l'aide à l'évaluation de la minorité de personnes étrangères.

CE, Section de l'intérieur, 18 décembre 2018, Avis n°396168, Projet de décret relatif aux modalités d'évaluation des personnes se déclarant mineures et privées temporairement ou définitivement de la protection de leur famille et autorisant la création d'un traitement de données à caractère personnel relatif à ces personnes

Décision de justice publiée sur internet – 1) Possibilité d'anonymiser la décision sans la rendre incompréhensible ou diminuer sa valeur doctrinale pour le public – Effacement en principe de droit – 2) Autres cas - Mise en balance des droits et intérêts en présence

1) Dans le cas particulier d'une demande d'effacement, fondée sur une opposition au traitement, relative à certains éléments figurant dans une décision de justice publiée sur internet, il y a lieu de tenir compte de la possibilité d'anonymiser la décision sans la rendre incompréhensible ou diminuer sa valeur doctrinale pour le public. Si tel est le cas et si la publication porte atteinte à la vie privée du demandeur, il doit en principe être procédé à l'effacement des données à caractère personnel publiées.

2) Dans les autres cas, il y a lieu de mettre en balance l'atteinte que cette publication porte à la vie privée du demandeur avec les droit et intérêts du responsable de traitement, ainsi que l'intérêt du public à connaître cette décision, au regard notamment de son apport jurisprudentiel.

CNIL, P, 22 janvier 2024, mise en demeure, Société X, décision n° MED-2024-016, non publié

4.5.2 Office de la CNIL

Effacement des données à caractère personnel ayant fait l'objet d'un traitement illicite – Pouvoir de l'autorité nationale de contrôle d'ordonner au responsable du traitement ou au sous-traitant d'effacer ces données 1) sans demande préalable de la personne concernée 2) que les données aient été collectées auprès de la personne concernée ou qu'elles proviennent d'une autre source

1) L'article 58, paragraphe 2, sous d) et g), du règlement général sur la protection des données doit être interprété en ce sens que l'autorité de contrôle d'un État membre est habilitée, dans l'exercice de son pouvoir d'adoption des mesures correctrices prévues à ces dispositions, à ordonner au responsable du traitement ou au sous-traitant d'effacer des données à caractère personnel ayant fait l'objet d'un traitement illicite, et ce alors qu'aucune demande n'a été présentée à cet effet par la

personne concernée en vue d'exercer ses droits en application de l'article 17, paragraphe 1, de ce règlement.

2) L'article 58, paragraphe 2, du règlement 2016/679 doit être interprété en ce sens que le pouvoir de l'autorité de contrôle d'un État membre d'ordonner l'effacement de données à caractère personnel ayant fait l'objet d'un traitement illicite peut viser tant des données collectées auprès de la personne concernée que des données provenant d'une autre source.

CJEU, 14 mars 2024, Újpesti Polgármesteri Hivatal, C-46/23

Droit au déréférencement – CNIL saisie d'une plainte formée à la suite d'une décision de refus de déréférencement opposée par l'exploitant d'un moteur de recherche – Méthode d'appréciation – Données ne relevant pas de catégories particulières 1) a) Principe – Déréférencement, sauf intérêt prépondérant du public à accéder à l'information – b) Éléments à prendre en compte – c) Illustration – 2) Données sensibles (art. 9 du RGPD) – a) Principe – Déréférencement, sauf si l'accès à ces données par le nom de l'intéressé est strictement nécessaire à l'information du public – b) Éléments à prendre en compte – c) Cas où les données ont été manifestement rendues publiques par l'intéressé – d) Illustration

1) a) Il appartient en principe à la Commission nationale de l'informatique et des libertés (CNIL), saisie par une personne d'une demande tendant à ce qu'elle mette l'exploitant d'un moteur de recherche en demeure de procéder au déréférencement de liens vers des pages web publiées par des tiers et contenant des données personnelles ne relevant pas de catégories particulières la concernant, d'y faire droit. Toutefois, il revient à la CNIL d'apprécier, compte tenu du droit à la liberté d'information, s'il existe un intérêt prépondérant du public à avoir accès à une telle information à partir d'une recherche portant sur le nom de cette personne de nature à faire obstacle au droit au déréférencement.

b) Pour procéder ainsi à une mise en balance entre le droit au respect de la vie privée et à la protection des données à caractère personnel et le droit à la liberté d'information et apprécier s'il peut être légalement fait échec au droit au déréférencement, il lui incombe de tenir notamment compte, d'une part, de la nature des données en cause, de leur contenu, de leur caractère plus ou moins objectif, de leur exactitude, de leur source, des conditions et de la date de leur mise en ligne et des répercussions que leur référencement est susceptible d'avoir pour la personne concernée et, d'autre part, de la notoriété de cette personne, de son rôle dans la vie publique et de sa fonction dans la société. Il lui incombe également de prendre en compte la possibilité d'accéder aux mêmes informations à partir d'une recherche portant sur des mots-clés ne mentionnant pas le nom de la personne concernée ainsi que le rôle qu'a, le cas échéant, joué cette dernière dans la publicité conférée aux données la concernant. 2) a) Lorsque des liens mènent vers des pages web contenant des données à caractère personnel relevant des catégories particulières visées à l'article 8 paragraphe 1 de la directive 95/46/CE du 24 octobre 1995, abrogé et remplacé par l'article 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD), l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel de la personne concernée est susceptible d'être particulièrement grave en raison de la sensibilité de ces données. Il s'ensuit qu'il appartient en principe à la CNIL, saisie par une personne d'une demande tendant à ce qu'elle mette l'exploitant d'un moteur de recherche en demeure de procéder au déréférencement de liens vers des pages web, publiées par des tiers et contenant des données personnelles relevant de catégories particulières la concernant, de faire droit à cette demande. Il n'en va autrement que s'il apparaît, compte tenu du droit à la liberté d'information, que l'accès à une telle information à partir d'une recherche portant sur le nom de cette personne est strictement nécessaire à l'information du public.

b) Pour apprécier s'il peut être légalement fait échec au droit au déréférencement au motif que l'accès à des données à caractère personnel relevant de catégories particulières à partir d'une recherche

portant sur le nom de la personne concernée est strictement nécessaire à l'information du public, il lui incombe de tenir notamment compte, d'une part, de la nature des données en cause, de leur contenu, de leur caractère plus ou moins objectif, de leur exactitude, de leur source, des conditions et de la date de leur mise en ligne et des répercussions que leur référencement est susceptible d'avoir pour la personne concernée et, d'autre part, de la notoriété de cette personne, de son rôle dans la vie publique et de sa fonction dans la société. Il lui incombe également de prendre en compte la possibilité d'accéder aux mêmes informations à partir d'une recherche portant sur des mots-clés ne mentionnant pas le nom de la personne concernée.

c) Dans l'hypothèse particulière où les données litigieuses ont manifestement été rendues publiques par la personne qu'elles concernent, il appartient à la CNIL de procéder comme s'il s'agissait de données non sensibles afin d'apprécier s'il existe ou non un intérêt prépondérant du public de nature à faire obstacle au droit au déréférencement, une telle circonstance n'empêchant pas l'intéressé de faire valoir, à l'appui de sa demande de déréférencement, des « raisons tenant à sa situation particulière », ainsi que l'a relevé la Cour de justice de l'Union européenne dans son arrêt AF, BH et ED contre CNIL (C-136/17) du 24 septembre 2019.

d) Requérante demandant à la CNIL d'ordonner à un exploitant de moteur de recherche de procéder au déréférencement de liens renvoyant vers des articles de blogs, un forum de discussion et une vidéo disponible sur une plateforme faisant état d'une relation extraconjugale qu'elle aurait entretenue avec l'ancien président d'un pays étranger et mentionnant l'existence alléguée d'une vidéo intime en témoignant.

Eu égard à la nature et au contenu des informations litigieuses, qui touchent à l'intimité de la requérante et qui proviennent de rumeurs et au fait que, à la date de la présente décision, il est possible d'accéder par d'autres liens à des informations faisant état des relations amicales entre l'intéressée et cet ancien président, la CNIL n'a pu, en dépit du rôle que joue la requérante dans la vie économique et sociale du pays, légalement estimer que le maintien des liens permettant d'avoir accès à ces informations à partir d'une recherche effectuée sur le nom de la requérante était strictement nécessaire à l'information du public.

CE, 6 décembre 2019, Mme X, n° 395335, Rec., points 11, 15-16

Voir aussi : CE, 6 décembre 2019, Mme A, n°403868, 403869, T. ; CE, 6 décembre 2019, M. A, n° 405910, T. ; CE, 6 décembre 2019, M. A, n°409212 , T. ; CE, 6 décembre 2019, M. A, n° 393769, T.

Droit au déréférencement – CNIL saisie d'une plainte formée à la suite d'une décision de refus de déréférencement opposée par l'exploitant d'un moteur de recherche – Méthode d'appréciation – 1) Données personnelles relatives à des procédures pénales (art. 10 du RGPD) – a) Principe – Déréférencement, sauf si l'accès à ces données par le nom de l'intéressé est strictement nécessaire à l'information du public – b) Éléments à prendre en compte – 2) Cas où les données ne sont plus à jour – 3) Illustration

1) a) Lorsque des liens mènent vers des pages web contenant des données à caractère personnel relatives à des procédures pénales visées à l'article 8 paragraphe 5 de la directive 95/46/CE du 24 octobre 1995 abrogé et remplacé par l'article 10 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 du 27 avril 2016 (RGPD), l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel de la personne concernée est susceptible d'être particulièrement grave en raison de la sensibilité de ces données. Il s'ensuit qu'il appartient en principe à la CNIL, saisie d'une demande tendant à ce qu'elle mette l'exploitant d'un moteur de recherche en demeure de procéder au déréférencement de liens vers des pages web, publiées par des tiers et contenant de telles données, de faire droit à cette demande. Il n'en va autrement que s'il apparaît, compte tenu du droit à la liberté d'information, que l'accès à une telle information à partir d'une recherche portant sur le nom de la personne concernée est strictement nécessaire à l'information du public.

b) Pour apprécier s'il peut être légalement fait échec au droit au déréférencement au motif que l'accès à des données à caractère personnel relatives à une procédure pénale à partir d'une recherche portant sur le nom de la personne concernée est strictement nécessaire à l'information du public, il lui incombe de tenir notamment compte, d'une part, de la nature des données en cause, de leur contenu, de leur caractère plus ou moins objectif, de leur exactitude, de leur source, des conditions et de la date de leur mise en ligne et des répercussions que leur référencement est susceptible d'avoir pour la personne concernée et, d'autre part, de la notoriété de cette personne, de son rôle dans la vie publique et de sa fonction dans la société. Il lui incombe également de prendre en compte la possibilité d'accéder aux mêmes informations à partir d'une recherche portant sur des mots-clés ne mentionnant pas le nom de la personne concernée.

2) Dans l'hypothèse particulière où le lien mène vers une page web faisant état d'une étape d'une procédure judiciaire ne correspondant plus à la situation judiciaire actuelle de la personne concernée mais qu'il apparaît, au terme de la mise en balance effectuée dans les conditions énoncées au point précédent, que le maintien de son référencement est strictement nécessaire à l'information du public, l'exploitant d'un moteur de recherche est tenu, au plus tard à l'occasion de la demande de déréférencement, d'aménager la liste de résultats de telle sorte que les liens litigieux soient précédés sur cette liste de résultats d'au moins un lien menant vers une ou des pages web comportant des informations à jour afin que l'image qui en résulte reflète exactement la situation judiciaire actuelle de la personne concernée.

3) Requérant ayant exercé, de 2003 à 2008, les fonctions de surveillant et animateur scolaire. À la suite d'attouchements sexuels sur mineurs, il a été mis en examen puis condamné par un jugement du tribunal correctionnel du 2 juin 2010 à une peine de sept ans d'emprisonnement, qui a été exécutée, assortie d'un suivi socio-judiciaire de dix ans et d'une interdiction d'exercer une activité impliquant un contact avec des enfants.

Eu égard à la nature et au contenu des informations litigieuses, qui donnent au public un accès direct et permanent à la condamnation dont a fait l'objet le requérant alors même que, en application du code de procédure pénale, l'accès à des données relatives aux condamnations pénales d'un individu n'est en principe possible que dans des conditions restrictives et pour des catégories limitées de personnes, à l'absence de notoriété de la personne qu'elles concernent, à l'ancienneté des faits et de la condamnation pénale ainsi qu'aux répercussions qu'est susceptible d'avoir sur la réinsertion du requérant, qui allègue avoir perdu deux emplois du fait du référencement en cause, le maintien des liens permettant d'y avoir accès à partir d'une recherche effectuée sur son nom, la CNIL n'a pu légalement estimer, alors même que ces informations proviennent d'articles de presse dont l'exactitude n'est pas contestée, que le maintien des liens litigieux était strictement nécessaire à l'information du public au motif que les chroniques judiciaires permettent d'exercer un droit de regard sur le fonctionnement de la justice pénale, sans qu'ait d'incidence la circonstance que la mesure de suivi socio-judiciaire dont fait l'objet l'intéressé est, à la date de la présente décision, toujours en cours.

CE, 6 décembre 2019, M. A, n° 401258, Rec., points 12-13

Voir aussi : CE, 6 décembre 2019, Mme X, n° 429154 T. ; CE, 6 décembre 2019, M. A, n°405464, T.

Droit au déréférencement – 1) Compétence de la CNIL pour connaître de plaintes formées à la suite d'une décision de refus de déréférencement opposée par l'exploitant d'un moteur de recherche – Existence, sans préjudice des voies de recours ouvertes devant le juge judiciaire – 2) Contrôle du juge administratif de l'excès de pouvoir – Contrôle entier

1) Il résulte des dispositions de l'article 11 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés que, sans préjudice des voies de recours ouvertes devant le juge judiciaire s'agissant des litiges opposant des particuliers aux exploitants d'un moteur de recherche, la CNIL est compétente pour connaître des plaintes formées sur le fondement de l'article 51 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans sa rédaction actuellement en

vigueur à la suite d'une décision de refus de déréférencement opposée par l'exploitant d'un moteur de recherche et, le cas échéant, pour mettre en demeure celui-ci de faire droit à la demande de déréférencement.

2) Ce pouvoir s'exerce, eu égard à la nature des droits individuels en cause, sous l'entier contrôle du juge administratif de l'excès de pouvoir.

CE, Assemblée, 24 février 2017, Mme G...C, n° 391000, Rec., point 9

4.6 Droit à la limitation

Absence d'accord déterminant la responsabilité conjointe du traitement et de la tenue du registre des activités de traitement – Conséquences – Droit à la limitation du traitement

L'article 17, paragraphe 1, sous d), et l'article 18, paragraphe 1, sous b), du RGPD doivent être interprétés en ce sens que la méconnaissance, par le responsable du traitement, des obligations prévues aux articles 26 et 30 de ce règlement, relatives, respectivement, à la conclusion d'un accord déterminant la responsabilité conjointe du traitement et à la tenue d'un registre des activités de traitement, ne constitue pas un traitement illicite conférant à la personne concernée un droit à l'effacement ou à la limitation du traitement, dès lors qu'une telle méconnaissance n'implique pas, en tant que telle, une violation par le responsable du traitement du principe de « responsabilité » tel qu'énoncé à l'article 5, paragraphe 2, dudit règlement, lu conjointement avec l'article 5, paragraphe 1, sous a), et l'article 6, paragraphe 1, premier alinéa, de ce dernier.

CJUE, 4 mai 2023, Bundesrepublik Deutschland, C-60/22

4.7 Droit d'opposition

1) Opposition au traitement d'une donnée relative aux opinions politique, philosophique ou religieuse – Légitimité sans avoir à justifier d'un motif spécifique

Justifie sa décision l'arrêt qui, pour déclarer l'Association spirituelle de l'église de scientologie d'Ile-de-France et son président coupables de traitement d'informations nominatives malgré opposition légitime, retient que l'opposition peut être transmise à l'association par la Commission nationale de l'informatique et des libertés (CNIL), aucun formalisme n'étant prévu par la loi et qu'en matière politique, philosophique ou religieuse, la légitimité de l'opposition est remplie par le seul exercice de cette faculté.

Cass, crim., 28 septembre 2004, n° 03-86.604, B., points 14-15

---

1) Droit subordonné à l'existence de raisons légitimes – Espèce – 2) Recours en excès de pouvoir contre la décision refusant de faire droit à l'opposition à un traitement de données à caractère personnel – Données ayant cessé d'être conservées dans ce traitement – Non-lieu, sans qu'ait d'incidence le fait que les données en cause aient pu être transférées vers d'autres traitements vis-à-vis desquels s'exerce le droit d'opposition

1) Il résulte des dispositions de l'article 38 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans sa rédaction applicable que le droit qu'elles ouvrent à toute personne physique de s'opposer pour des motifs légitimes à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement est subordonné à l'existence de raisons légitimes tenant de manière prépondérante à sa situation particulière. Ne commet pas d'erreur de droit la cour administrative d'appel qui relève que, pour faire opposition au traitement des données concernant ses enfants, la requérante se bornait à invoquer des craintes d'ordre général concernant notamment la sécurité du fonctionnement de la base, sans faire état de considérations qui lui seraient propres ou seraient propres à ses enfants, pour en déduire qu'elle ne justifiait pas de motifs légitimes de nature à justifier cette opposition.

2) La circonstance que les données à caractère personnel ont cessé d'être conservées dans le traitement litigieux prive d'objet les conclusions à fin d'annulation pour excès de pouvoir de la décision qui avait refusé de faire droit à l'opposition à ce traitement, sans qu'ait d'incidence le fait que les données en cause aient pu être transférées vers d'autres traitements vis-à-vis desquels s'exerce le droit d'opposition.

CE, 10ème–9ème chambres réunies, 18 mars 2019, Mme B., n° 406313, T., points 10, 4

Personne auprès de qui s'exerce le droit d'opposition – 1) Principe – Responsable du traitement – Possibilité de déléguer cette compétence– Existence – 2) Application à des traitements de l'éducation nationale (BE1D et BNIE) – Compétence exercée à l'échelon départemental

1) Si la personne responsable du traitement, au sens des dispositions du I de l'article 3 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, est, en principe, celle auprès de laquelle s'exerce le droit d'opposition (prévu par l'article 38 de la loi), ni cette loi, ni le décret n° 2005-1309 du 20 octobre 2005 pris pour son application ne font obstacle à ce qu'elle délègue sa compétence en la matière.

2) La « base élève premier degré » (BE1D) a pour finalités d'assurer la gestion administrative et pédagogique des élèves du premier degré, la gestion et le pilotage de l'enseignement du premier degré dans les circonscriptions scolaires du premier degré et les inspections d'académie et le pilotage académique et national, et la « base nationale identifiant élève » (BNIE) a la finalité d'attribuer un identifiant unique à chaque élève, afin de permettre le suivi de toute sa scolarité. Ces bases concourent aux missions relatives à l'action éducatrice et à son organisation, au sens des dispositions des articles R. 222-25 et R. 222-26 du code de l'éducation et, dès lors, en application de ces dispositions, la compétence en matière d'exercice du droit d'opposition doit être regardée comme étant exercée à l'échelon départemental des services de l'éducation nationale.

CE, 10ème-9ème chambres réunies, 27 juin 2016, Ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche contre Mme B...-A..., n° 392145, T., points 3, 7

Le droit d'opposition peut être exprimé de façon générale.

Le droit d'opposition au traitement de données personnelles, contrairement à l'acceptation d'un tel usage, qui doit être spécifique, informé et dénué de toute ambiguïté, doit être considéré comme valablement exprimé même s'il l'est de façon générale. La circonstance, d'une part, que le droit d'opposition soit manifesté par un acte d'abstention plutôt que par un acte positif, d'autre part, qu'il soit exprimé d'une manière large en visant « tout démarchage commercial », est sans incidence sur la validité de l'expression du refus de prospection ultérieure.

CE, 10ème/9ème SSR, 9 novembre 2015, Société les Éditions Néressis, n° 384673, T., point 6

Inclusion – Mise en ligne sur internet d'une base de données de jurisprudence non totalement anonymisées – Conséquence – Applicabilité du droit d'opposition

Il résulte des dispositions des articles 2 et 38 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés, que la mise en ligne sur le réseau internet d'une base de données de jurisprudence non totalement anonymisée doit être regardée comme un traitement automatisé de données à caractère personnel au sens de la loi Informatique et Libertés, auquel s'applique le droit d'opposition qu'elle ouvre aux personnes concernées.

CE, 10ème/9ème SSR, 23 mars 2015, Association Lexeek pour l'accès au droit, n° 353717, T., point 8

Exclusion du droit d'opposition (art. 23 RGPD) – 1) Autorités pouvant écarter le droit d'opposition – Collectivités territoriales et établissements publics – Inclusion – 2) Conditions et garanties

1) L'article 23 du RGPD permet de limiter ou d'écarter le droit d'opposition à un traitement, à certaines conditions, par une « mesure législative ». Le considérant 41 du RGPD précise que cette « mesure législative » n'est pas nécessairement un acte adopté par le Parlement, mais doit être déterminée par le droit national de chaque État membre. En France, il peut en particulier s'agir d'un acte réglementaire. La CNIL estime que, s'agissant des traitements participant de l'exécution d'une mission d'intérêt public, tant l'État que les collectivités territoriales ou les établissements publics peuvent, dans leurs domaines de compétence respectifs et s'ils disposent d'un pouvoir réglementaire, limiter ou exclure le droit d'opposition.

2) Cependant, l'exercice de cette faculté est soumis à une double limite : d'une part, s'agissant de la compétence, ne pas empiéter sur le domaine réservé à la loi en application de l'article 34 de la Constitution ; d'autre part, veiller à ce que les conditions prévues à l'article 23 soient respectées. Dans ses lignes directrices 10/2020 du 13 octobre 2021 sur l'article 23, le Comité européen pour la protection des données a notamment rappelé l'obligation pour le responsable de traitement de veiller au caractère strictement nécessaire et proportionné de la limitation envisagée au regard de l'objectif poursuivi. Il a également souligné que l'acte écartant l'opposition doit faire l'objet d'une publicité suffisante et être accessible.

CNIL, SP, 16 février 2023, Avis sur un projet de décision, Création d'un fichier central des titres permanents du permis de chasser, n° 2023-015, publié, point 16

Notion d'acte « instaurant le traitement » permettant d'écarter le droit d'opposition au sens de l'article 56 de la loi Informatique et Libertés

La notion d'acte « instaurant le traitement » peut renvoyer, s'agissant de traitements mis en œuvre par les autorités publiques, à des normes contenant l'ensemble de la réglementation d'un traitement, notamment en application de l'article 35 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. S'agissant de traitements décidés et mis en place par des opérateurs privés, la limitation du droit d'opposition doit être prévue dans un acte législatif ou réglementaire autorisant la mise en œuvre des traitements par ces opérateurs, qui doit comporter les dispositions spécifiques prescrites par l'article 23.2 du RGPD.

CNIL, SP, 17 décembre 2020, Avis sur projet de décret, Vidéo-port du masque, n° 2020-136, publié, point 19

4.7.1 Opposition à la prospection commerciale

Prospection commerciale par SMS – Information sur l'opposition gratuite – Illégalité d'un dispositif d'opposition payant

Un SMS de prospection doit informer la personne de ce qu'elle peut s'opposer gratuitement au traitement de ses données.

Est illégal un dispositif informant la personne qu'il est possible de s'opposer au traitement en adressant un SMS ou un appel téléphonique payants dans le message de prospection reçu par SMS, ou en remplissant un formulaire sur internet, sans que cette faculté ait été mentionnée dans les SMS de prospection.

CE, 10ème/9ème SSR, 23 mars 2015, Société Groupe DSE France, n° 357556, T., point 15

Effectivité du droit d'opposition dans le temps – Liste repoussoir ou système équivalent

Il revient à la société traitant des données à caractère personnel à des fins de prospection commerciale de mettre en place un mécanisme permettant une prise en compte effective du droit d'opposition exprimé par les personnes faisant l'objet de prospection téléphonique en application de l'article 21 du RGPD. Elle doit, à ce titre, être en mesure de s'assurer, dans le temps, que l'opposition exprimée par les intéressés est respectée et que les personnes ayant fait part de leur opposition ne reçoivent plus d'appels de prospection. Un tel mécanisme peut prendre la forme d'une liste repoussoir ou d'un système équivalent.

CNIL, P, 4 mars 2020, Mise en demeure, Société X, n° MED-2020-004, non publié

4.8 Décision automatisée

Notion de décision informatisée – Calcul automatisé d'une valeur de probabilité de la solvabilité d'une personne – Inclusion – Conditions

L'article 22, paragraphe 1, du RGPD doit être interprété en ce sens que l'établissement automatisé, par une société fournissant des informations commerciales, d'une valeur de probabilité fondée sur des données à caractère personnel relatives à une personne et concernant la capacité de celle-ci à honorer des engagements de paiement à l'avenir constitue une « décision individuelle automatisée », au sens de cette disposition, lorsque dépend de manière déterminante de cette valeur de probabilité le fait qu'une tierce partie, à laquelle ladite valeur de probabilité est communiquée, établisse, exécute ou mette fin à une relation contractuelle avec cette personne.

CJUE, 7 décembre 2023, SCHUFA Holding, C-634/21

Consultation de traitements automatisés d'informations nominatives des services de police et de gendarmerie – Application de l'article 2 de la loi Informatique et Libertés – Données recueillies dans les fichiers – Élément de la décision administrative prise sous le contrôle du juge par l'autorité administrative

Est applicable à la consultation des traitements automatisés d'informations nominatives des services de police et de gendarmerie, prévue par l'article 25 de la loi pour la sécurité intérieure dans le cadre

de certaines enquêtes administratives, l'article 2 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en vertu duquel une décision administrative « impliquant une appréciation sur un comportement humain » ne peut être exclusivement fondée sur un traitement automatisé « donnant une définition du profil ou de la personnalité de l'intéressé ». Les données recueillies dans les fichiers ne constitueront donc, dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative.

CC, 2003-467 DC, 13 mars 2003, Loi pour la sécurité intérieure, point 34

4.9 Autres limitations des droits

4.9.1 Dans le champ RGPD

Traitement automatisé de données à caractère personnel pour la production des certificats de membre d'équipage sécurisés biométriques – Droit d'opposition – Absence – Objectif d'intérêt public de sécurité publique – Fondement juridique de l'absence de droit d'opposition : article 23 (1. c) du RGPD

Saisi d'un projet de décret relatif à la création d'un traitement automatisé de données à caractère personnel pour la production des certificats de membre d'équipage sécurisés biométriques, le Conseil d'État (section de l'intérieur) estime que le projet peut prévoir la non-application du droit d'opposition au traitement des données pour des raisons tenant à l'objectif d'intérêt public de sécurité publique dans un lieu aussi sensible qu'un aéroport et que le fondement juridique de cette disposition doit être non pas l'article 38 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés mais directement l'article 23 (1. c) du Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

CE, Section de l'intérieur, 5 février 2019, Avis n°396472, Projet de décret relatif à la création d'un traitement de données biométriques pour la production des certificats de membres d'équipage sécurisés biométriques

---

4.9.2 Dans le champ de la directive

Radars routiers – Limitation du droit à l'effacement pour les classements sans suite – Atteinte disproportionnée en l'espèce

Eu égard aux finalités du système de contrôle automatisé, qui a pour objet de centraliser les opérations d'identification, de gestion et de suivi des infractions routières et non routières faisant l'objet d'une amende forfaitaire, la limitation du droit à demander l'effacement des données aux seules personnes ayant bénéficié d'une décision définitive de relaxe, à l'exclusion de celles pour lesquelles la procédure a été classée sans suite, porte une atteinte disproportionnée aux droits de ces dernières.

CE, 10ème–9ème chambres réunies, 24 septembre 2021, Médecins du Monde et autres, n° 441317, Inédit., point 8

4.10 Droit à la réclamation auprès d'une autorité de contrôle

Absence de compétence prioritaire ou exclusive – Possibilité d'exercer les recours administratifs et juridictionnels prévus par le RGPD de manière concurrente et indépendante

L'article 77, paragraphe 1, l'article 78, paragraphe 1, et l'article 79, paragraphe 1, du RGPD, lus à la lumière de l'article 47 de la Charte des droits fondamentaux de l'Union européenne doivent être interprétés en ce sens qu'ils permettent un exercice concurrent et indépendant des voies de recours prévues, d'une part, à cet article 77, paragraphe 1, et à cet article 78, paragraphe 1, ainsi que, d'autre part, à cet article 79, paragraphe 1.

Il appartient aux États membres, en accord avec le principe de l'autonomie procédurale, de prévoir les modalités d'articulation de ces voies de recours afin que soient assurés l'effectivité de la protection des droits garantis par ce règlement, l'application cohérente et homogène des dispositions de ce dernier ainsi que le droit à un recours effectif devant un tribunal, visé à l'article 47 de la Charte des droits fondamentaux.

CJUE, 12 janvier 2023, Budapesti Elektromos Müvek, C-132/21

4.11 Droit d'accès aux documents administratifs

Règlement n° 1049/2001 – Accès aux documents des institutions de l'Union européenne – Document contenant des données à caractère personnel – Règlement n° 45/2001 – Mise en balance des intérêts

L'article 4, paragraphe 1, sous b) du règlement n° 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission prévoit une exception à l'accès à un document dans le cas où la divulgation porterait atteinte à la protection de la vie privée ou de l'intégrité de l'individu, notamment en conformité avec la législation de l'Union relative à la protection des données à caractère personnel.

Une demande d'accès portant sur un document contenant des données à caractère personnel doit donc toujours être examinée et appréciée en conformité avec le règlement n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (CJUE, 29 juin 2010, Commission c/ Bavarian Lager, C-28/08, points 57 et 59-64). La communication ne peut alors être refusée qu'en cas d'« atteinte concrète et effective » à l'intérêt protégé.

CJUE, 16 juillet 2015, ClientEarth et Pesticide Action Europe contre Autorité européenne de sécurité des aliments, C-615/13 P, points 69-70

Registre de contention et d'isolement des établissements de santé (art. L. 3222-5-1 du code de la santé publique) – Communication – 1) Conditions – Occultation des éléments identifiant les patients et les soignants – 2) Cas où l'identité des patients a fait l'objet d'une pseudonymisation – Contrôle du juge administratif – Risque d'atteinte à la protection de la vie privée et au secret médical – Illustration – Communicabilité à des tiers de l'identifiant dit « anonymisé » du patient – Exclusion

1) Le registre de contention et d'isolement comporte des mentions qui ne sont pas soumises à occultation préalable avant leur communication, telles que les dates, les heures et la durée de chaque mesure de contention forcée ou d'isolement. Les éléments permettant d'identifier les patients doivent, en application des articles L. 311-6 et L. 311-7 du code des relations entre le public et l'administration, être occultés préalablement à la communication du registre de contention et d'isolement, afin de ne pas porter atteinte au secret médical et à la protection de la vie privée, comme doivent également l'être celles permettant d'identifier les soignants, afin d'éviter que la divulgation d'informations les concernant puisse leur porter préjudice.

2) Dans le cas où l'identité des patients a fait l'objet d'une pseudonymisation, laquelle ne permet l'identification des personnes en cause qu'après recoupement d'informations, il appartient au juge administratif d'apprécier si, eu égard à la sensibilité des informations en cause et aux efforts nécessaires pour identifier les personnes concernées, leur communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. En l'espèce, compte tenu de la nature des informations en cause, qui touchent à la santé mentale des patients, et du nombre restreint de personnes pouvant faire l'objet d'une mesure de contention et d'isolement, facilitant ainsi leur identification, alors au demeurant que les autorités énumérées à l'article L. 3222-5-1 du code de la santé publique peuvent accéder à l'ensemble des informations figurant sur les registres et contrôler l'activité des établissements concernés, l'identifiant dit " anonymisé " figurant dans ces registres, qu'il s'agisse, selon la pratique du centre hospitalier, de " l'identifiant permanent du patient " (IPP) ou d'un identifiant spécialement défini, doit être regardé comme une information dont la communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. Cet identifiant n'est donc communicable qu'au seul intéressé en vertu des dispositions de l'article L. 311-6 du code des relations entre le public et l'administration.

CE, 10ème-9ème chambres réunies, 8 février 2023, Association « commission des citoyens pour les droits de l'homme », n°455887, T., points 5-7

Application de la loi du 17 juillet 1978 (« loi CADA ») aux données relevant de la loi Informatique et Libertés (art. 37) – Existence – Modalités

Il résulte de l'article 37 de la loi n° 78-17 du 6 janvier 1978 (loi IL) que les dispositions de cette loi ne font, en principe, pas obstacle à l'application, au bénéfice de tiers, des dispositions du titre Ier de la loi n° 78-753 du 17 juillet 1978. Lorsque des données à caractère personnel ont également le caractère de documents administratifs, elles ne sont communicables aux tiers, en vertu du III de l'article 6 de la loi du 17 juillet 1978, que s'il est possible d'occulter ou de disjoindre les mentions portant atteinte, notamment, à la protection de la vie privée ou au secret médical. Il ne peut être accédé à une demande de communication sur le fondement de la loi du 17 juillet 1978 que si le traitement nécessaire pour rendre impossible, s'agissant de données de santé, toute identification, directe ou indirecte, de l'une quelconque des personnes concernées, y compris par recoupement avec d'autres données, n'excède pas l'occultation ou la disjonction des mentions non communicables, seule envisagée par cette loi. Dans le cas contraire, sont seules applicables les dispositions de la loi du 6 janvier 1978 et des lois spéciales applicables au traitement de certaines catégories de données, notamment, en ce qui concerne les données de santé à caractère personnel, les chapitres IX et X de la loi du 6 janvier 1978.

CE, 1ère/6ème SSR, 30 décembre 2015, Société les Laboratoires Servier, n°372230, Rec., point 2

4.12 Droit à réparation

Droit à réparation et responsabilité – 1) Conditions – Existence d'un dommage causé par la violation – 2) Forme de la réparation – Excuses – Inclusion – 3) Montant de la réparation – Minoration en raison de l'attitude du responsable de traitement – Absence

1) L'article 82, paragraphe 1, du règlement général sur la protection des données (RGPD), lu à lumière de l'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'une violation de dispositions de ce règlement ne suffit pas, à elle seule, pour constituer un « dommage », au sens de cet article 82, paragraphe 1.

2) L'article 82, paragraphe 1, du RGPD doit être interprété en ce sens que la présentation d'excuses peut constituer une réparation adéquate d'un dommage moral sur le fondement de cette disposition, notamment lorsqu'il est impossible de rétablir la situation antérieure à la survenance de ce dommage, pour autant que cette forme de réparation soit de nature à compenser intégralement le préjudice subi par la personne concernée.

3) L'article 82, paragraphe 1, du RGPD doit être interprété en ce sens qu'il s'oppose à ce que l'attitude et la motivation du responsable du traitement puissent être prises en compte afin, le cas échéant, d'accorder à la personne concernée une réparation inférieure au préjudice qu'elle a concrètement subi.

CJUE, 4 octobre 2024, Patērētāju tiesību aizsardzības centrs, C-507/23

Article 82 du RGPD 1) Autorité responsable de la publicité obligatoire des actes – Refus d'effacer les données non requises – Droit à réparation – Existence d'un préjudice moral - 2) Exonération de responsabilité prévue à l'article 82 du RGPD - Interprétation

1) L'article 82, paragraphe 1, du règlement 2016/679 du 27 avril 2016 (RGPD) doit être interprété en ce sens qu'une perte de contrôle d'une durée limitée, par la personne concernée, sur ses données à caractère personnel en raison de la mise à la disposition du public de ces données, en ligne, dans le registre du commerce d'un État membre, peut suffire pour causer un « dommage moral », pour autant que cette personne démontre qu'elle a effectivement subi un tel dommage, aussi minime fût-il, sans que cette notion de « dommage moral » requière la démonstration de l'existence de conséquences négatives tangibles supplémentaires.

2) L'article 82, paragraphe 3, du règlement 2016/679 du 27 avril 2016 (RGPD) doit être interprété en ce sens qu'un avis de l'autorité de contrôle d'un État membre, émis sur le fondement de l'article 58, paragraphe 3, sous b), de ce règlement, ne suffit pas à exonérer de responsabilité, au titre de l'article 82, paragraphe 2, dudit règlement, l'autorité chargée de la tenue du registre du commerce de cet État membre ayant la qualité de « responsable du traitement » au sens de l'article 4, point 7, du même règlement.

CJUE, 4 octobre 2024, Agentsia po vpisvaniyata, C 200/23

---

1) Demande de réparation d'un préjudice moral – Cas d'une diffusion de données à caractère personnel à un tiers non autorisé 2) Condition de gravité de la violation – Absence – 3) Eléments de preuve Violation des dispositions du règlement – Existence d'un dommage matériel ou moral

1) L'article 82, paragraphe 1, du règlement 2016/679 doit être interprété en ce sens que dans l'hypothèse où un document contenant des données à caractère personnel a été remis à un tiers non autorisé dont il est établi qu'il n'a pas pris connaissance de celles-ci, un « dommage moral », au sens de cette disposition, n'est pas constitué par le simple fait que la personne concernée craint que, à la

suite de cette communication ayant rendu possible la réalisation d'une copie dudit document avant sa restitution, une diffusion, voire un usage abusif, de ses données se produise dans le futur.

Les articles 5, 24, 32 et 82 du règlement (UE) 2016/679 doivent être interprétés en ce sens que dans le cadre d'une action en réparation fondée sur cet article 82, le fait que des employés du responsable du traitement ont remis par erreur à un tiers non autorisé un document contenant des données à caractère personnel ne suffit pas, à lui seul, pour considérer que les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement en cause n'étaient pas « appropriées », au sens de ces articles 24 et 32.

2) L'article 82 du règlement 2016/679 doit être interprété en ce sens que cet article ne requiert pas que le degré de gravité de la violation commise par le responsable du traitement soit pris en compte aux fins de la réparation d'un dommage sur le fondement de cette disposition.

3) L'article 82, paragraphe 1, du règlement 2016/679 doit être interprété en ce sens que la personne demandant réparation au titre de cette disposition est tenue d'établir non seulement la violation de dispositions de ce règlement, mais également que cette violation lui a causé un dommage matériel ou moral.

CJEU, 25 janvier 2024, MediaMarktSaturn, C-687/21

---

1) Fonction compensatoire du droit à réparation – Existence – Fonction dissuasive de ce même droit– Exclusion - 2) Condition - Existence d'une faute du responsable du traitement en cas de manquement – Régime de faute présumée

1) L'article 82, paragraphe 1, du règlement 2016/679 doit être interprété en ce sens que le droit à réparation prévu à cette disposition remplit une fonction compensatoire, en ce qu'une réparation pécuniaire fondée sur ladite disposition doit permettre de compenser intégralement le préjudice concrètement subi du fait de la violation de ce règlement, et non une fonction dissuasive ou punitive.

2) L'article 82 du règlement 2016/679 doit être interprété en ce sens que d'une part, l'engagement de la responsabilité du responsable du traitement est subordonné à l'existence d'une faute commise par celui-ci, laquelle est présumée à moins que ce dernier prouve que le fait qui a provoqué le dommage ne lui est nullement imputable, et, d'autre part, cet article 82 ne requiert pas que le degré de gravité de cette faute soit pris en compte lors de la fixation du montant des dommages-intérêts alloués en réparation d'un préjudice moral sur le fondement de cette disposition.

CJUE, 21 décembre 2023, Krankenversicherung Nordrhein, C-667/21

Réglementation ou pratique nationale fixant un « seuil de minimis » afin de caractériser un dommage moral causé par une violation du RGPD – Illicéité – Obligation de démontrer que les conséquences de cette violation sont constitutives d'un préjudice – Existence

L'article 82, paragraphe 1, du RGPD doit être interprété en ce sens qu'il s'oppose à une réglementation nationale ou à une pratique nationale qui fixe un « seuil de minimis » afin de caractériser un dommage moral causé par une violation de ce règlement. La personne concernée est tenue de démontrer que les conséquences de cette violation qu'elle prétend avoir subies sont constitutives d'un préjudice qui se différencie de la simple violation des dispositions dudit règlement.

CJUE, 14 décembre 2023, Gemeinde Ummendorf, C-456/22

Demande de réparation d'un préjudice moral fondée sur la crainte d'un potentiel usage abusif de données à caractère personnel

L'article 82, paragraphe 1, du règlement 2016/679 doit être interprété en ce sens que la crainte d'un potentiel usage abusif de ses données à caractère personnel par des tiers qu'une personne concernée éprouve à la suite d'une violation de ce règlement est susceptible, à elle seule, de constituer un « dommage moral », au sens de cette disposition.

CJUE, 14 décembre 2023, Natsionalna agentsia za prihodite, C-340/21

Droit à réparation du dommage causé par le traitement de données effectué en violation du RGPD – Conditions du droit à réparation – Simple violation dudit règlement – Insuffisance – Condition de gravité minimale – Absence

L'article 82, paragraphe 1, du RGPD doit être interprété en ce sens que la simple violation des dispositions de ce règlement ne suffit pas pour conférer un droit à réparation.

L'article 82, paragraphe 1, du RGPD doit être interprété en ce sens qu'il s'oppose à une règle ou une pratique nationale subordonnant la réparation d'un dommage moral, au sens de cette disposition, à la condition que le préjudice subi par la personne concernée ait atteint un certain degré de gravité.

Il y a lieu de relever que le RGPD ne contient pas de disposition ayant pour objet de définir les règles relatives à l'évaluation des dommages-intérêts auxquels une personne concernée, au sens de l'article 4, point 1, de ce règlement, peut prétendre, en vertu de l'article 82 de celui-ci, lorsqu'une violation dudit règlement lui a causé un préjudice. Par conséquent, à défaut de règles du droit de l'Union en la matière, il appartient à l'ordre juridique de chaque État membre de fixer les modalités des actions destinées à assurer la sauvegarde des droits que les justiciables tirent de cet article 82 et, en particulier, les critères permettant de déterminer l'étendue de la réparation due dans ce cadre, sous réserve du respect desdits principes d'équivalence et d'effectivité.

CJUE, 4 mai 2023, Österreichische Post, C-300/21, point 54

4.13 Recours juridictionnel

4.13.1 Intérêt pour agir

Associations de défense des consommateurs

Possible action en justice contre l'auteur présumé d'une atteinte à la protection des données à caractère personnel

Les articles 22 à 24 de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 doivent être interprétés en ce sens qu'ils ne s'opposent pas à une réglementation nationale permettant aux associations de défense des intérêts des consommateurs d'agir en justice contre l'auteur présumé d'une atteinte à la protection des données à caractère personnel.

CJUE, 29 juillet 2019, Fashion ID, C-40/17

4.13.2 Droit à un recours effectif

Article 47 Charte des droits fondamentaux de l'Union européenne – 1) Mode de preuve d'une violation de la protection des données – Liste contenant des données à caractère personnel – Admissibilité – Obtention d'une telle liste sans le consentement, légalement requis, du responsable du traitement – Appréciation de la proportionnalité du rejet de cette liste litigieuse en tant que moyen de preuve – 2) Réglementation nationale subordonnant l'exercice d'un recours juridictionnel à l'épuisement préalable des voies de recours administratives – Conditions

1) L'article 47 de la Charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'il s'oppose à ce qu'une juridiction nationale rejette, en tant que moyen de preuve d'une violation de la protection des données à caractère personnel conférée par la directive 95/46, une liste, telle que la liste litigieuse, présentée par la personne concernée et contenant des données à caractère personnel de celle-ci, dans l'hypothèse où cette personne aurait obtenu cette liste sans le consentement, légalement requis, du responsable du traitement de ces données, à moins qu'un tel rejet soit prévu par la législation nationale et qu'il respecte à la fois le contenu essentiel du droit à un recours effectif et le principe de proportionnalité.

Ainsi, afin d'apprécier la proportionnalité d'un rejet de la liste litigeuse en tant que moyen de preuve, la juridiction de renvoi doit examiner si sa législation nationale limite ou non, par rapport aux données figurant sur cette liste, les droits d'information et d'accès énoncés aux articles 10 à 12 de la directive 95/46 et si une telle limitation est, le cas échéant, justifiée. En outre, même lorsque tel est le cas et qu'il existe des éléments plaidant en faveur d'un intérêt légitime à l'éventuelle confidentialité de la liste en cause, les juridictions nationales doivent vérifier au cas par cas si ceux-ci prévalent sur l'intérêt à la protection des droits du particulier et s'il existe, dans le cadre de la procédure devant cette juridiction, d'autres moyens pour assurer cette confidentialité, notamment en ce qui concerne les données à caractère personnel des autres personnes physiques figurant sur cette liste.

2) L'article 47 de la Charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'il ne s'oppose pas à une législation nationale qui subordonne l'exercice d'un recours juridictionnel par une personne affirmant qu'il a été porté atteinte à son droit à la protection des données à caractère personnel garanti par la directive 95/46/CE à l'épuisement préalable des voies de recours disponibles devant les autorités administratives nationales, à condition que les modalités concrètes d'exercice desdites voies de recours n'affectent pas de manière disproportionnée le droit à un recours effectif devant un tribunal visé à cette disposition. Il importe, notamment, que l'épuisement préalable des voies de recours disponibles devant les autorités administratives nationales n'entraîne pas de retard substantiel pour l'introduction d'un recours juridictionnel, qu'il entraîne la suspension de la prescription des droits concernés et qu'il n'occasionne pas de frais excessifs.

CJUE, 27 septembre 2017, Puškár, C-73/16, points 97-98

5. Transferts

Mineurs – Traitement ayant pour finalité d'améliorer la prise en charge et le parcours scolaires d'élèves à besoins éducatifs particuliers – Obligation de prévoir dans le contrat de sous-traitance l'interdiction de transférer les données en dehors de l'Union européenne

Dans le cadre d'un projet de décret autorisant la mise en œuvre par le ministère de l'éducation nationale d'un traitement ayant pour finalité d'améliorer la prise en charge et le parcours scolaire des élèves à besoins éducatifs particuliers, dont des élèves handicapés, compte tenu des données traitées,

de la minorité d'un grand nombre de personnes concernées par le traitement, du cadre dans lequel elles sont recueillies et du considérant 38 du RGPD qui indique que « Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel », la CNIL considère que le contrat de sous-traitance devrait prévoir l'interdiction de transférer les données en dehors de l'Union européenne.

CNIL, P, 15 juillet 2021, Avis sur projet de décret, Livret de parcours inclusif (LPI) n° 2021-082, publié, point 29

5.1 Notion de transfert

Inscription sur une page internet de données à caractère personnel par une personne qui se trouve dans un État membre – Transfert vers un pays tiers de données – Exclusion

Il n'existe pas de « transfert vers un pays tiers de données » au sens de l'article 25 de la directive 95/46, lorsqu'une personne qui se trouve dans un État membre inscrit sur une page internet des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à internet, y compris des personnes se trouvant dans des pays tiers.

CJUE, 6 novembre 2003, Lindqvist, C-101/01

5.2 Décision d'adéquation

5.2.1 Conditions de validité

Décision 2016/1250 constatant un niveau adéquat de protection assuré par le bouclier de protection des données Union européenne-États-Unis – 1) Transfert de données à caractère personnel vers un pays tiers – Notion de niveau de protection adéquat à assurer par le pays tiers concerné lors de tels transferts – Interprétation au regard du droit de l'Union – Critères d'appréciation – 2) Autorité nationale de contrôle saisie d'une demande mettant en cause le caractère adéquat du niveau de protection assuré dans ce pays tiers – Obligation pour cette autorité d'examiner la demande – Invalidité – a) Limitations de la protection des données à caractère personnel – Encadrement insuffisant pour répondre à des exigences substantiellement équivalentes – Méconnaissance du principe de proportionnalité – b) Absence de droits opposables aux autorités américaines devant les tribunaux – Mécanisme de médiation – Absence de garanties substantiellement équivalentes – Méconnaissance du droit à une protection juridictionnelle effective

1) L'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du RGPD doivent être interprétés en ce sens que les garanties appropriées, les droits opposables et les voies de droit effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne par ce règlement, lu à la lumière de la Charte des droits fondamentaux de l'Union européenne.

À cet effet, l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établi dans l'Union européenne et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci, notamment ceux énoncés à l'article 45, paragraphe 2, dudit règlement.

2) La décision d'exécution (UE) 2016/1250 de la Commission, du 12 juillet 2016, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, est invalide. Sont en particulier méconnus le principe de proportionnalité et le droit à une protection juridictionnelle effective.

a) La décision 2016/1250 consacre, à l'instar de la décision 2000/520, la primauté des exigences relatives à la sécurité nationale, à l'intérêt public et au respect de la législation américaine, rendant ainsi possibles des ingérences dans les droits fondamentaux des personnes dont les données sont transférées vers ce pays tiers. Les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de telles données transférées depuis l'Union vers ce pays tiers, et que la Commission a évaluées dans la décision 2016/1250, ne sont pas encadrées de manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, par le principe de proportionnalité, en ce que les programmes de surveillance fondés sur cette réglementation ne sont pas limités au strict nécessaire. En se fondant sur les constatations figurant dans cette décision, il est relevé que, pour certains programmes de surveillance, ladite réglementation ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'elle comporte pour la mise en œuvre de ces programmes, pas plus que l'existence de garanties pour des personnes non américaines potentiellement visées.

b) Par ailleurs, si la même réglementation prévoit des exigences que les autorités américaines doivent respecter, lors de la mise en œuvre des programmes de surveillance concernés, elle ne confère pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux. Quant à l'exigence de protection juridictionnelle, contrairement à ce que la Commission a considéré dans la décision 2016/1250, le mécanisme de médiation visé par cette décision ne fournit pas à ces personnes une voie de recours devant un organe offrant des garanties substantiellement équivalentes à celles requises en droit de l'Union, de nature à assurer tant l'indépendance du médiateur prévu par ce mécanisme que l'existence de normes habilitant ledit médiateur à adopter des décisions contraignantes à l'égard des services de renseignement américains.

CJUE, grande chambre, 16 juillet 2020, Facebook Ireland et Schrems, C-311/18

Accord de « Safe Harbor » – Décision 2000/520 – 1) Définition d'un niveau de protection « adéquat » – Obligations pesant sur la Commission – 2) Réglementation limitée au strict nécessaire – Exclusion – Atteinte au droit au respect de la vie privée – 3) Réglementation ne prévoyant pas de voies de droit pour accéder aux données, les rectifier ou les supprimer – Atteinte au droit à une protection juridictionnelle effective – 4) Restriction des pouvoirs de contrôle des autorités nationales – Invalidité de la décision

1) Le terme « adéquat » ne signifie pas que le pays tiers doit assurer un niveau de protection des libertés et droits fondamentaux « identique » à celui garanti dans l'ordre juridique de l'Union, mais à tout le moins « substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte ».

La Commission est tenue de vérifier si les États-Unis assurent effectivement, en raison de leur législation interne ou de leurs engagements internationaux, un niveau de protection des droits

fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive lue à la lumière de la Charte.

Or, la Commission n'a pas opéré un tel constat, mais s'est bornée à examiner le régime de la « sphère de sécurité »(« Safe Harbor »). Sans qu'il y ait besoin de vérifier si ce régime assure un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union, la Cour relève que ce régime est uniquement applicable aux entreprises américaines qui y souscrivent, sans que les autorités publiques des États-Unis y soient elles-mêmes soumises. Les exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des États-Unis l'emportent sur le régime de la « sphère de sécurité », si bien que les entreprises américaines sont tenues d'écarter, sans limitation, les règles de protection prévues par ce régime, lorsqu'elles entrent en conflit avec de telles exigences.

Le régime américain de la « sphère de sécurité » rend ainsi possible des ingérences, par les autorités publiques américaines, dans les droits fondamentaux des personnes, la décision de la Commission ne faisant état ni de l'existence, aux États-Unis, de règles destinées à limiter ces éventuelles ingérences ni de l'existence d'une protection juridique efficace contre ces ingérences. La Cour considère que cette analyse du régime est corroborée par deux communications de la Commission, d'où il ressort notamment que les autorités des États-Unis pouvaient accéder aux données à caractère personnel transférées à partir des États membres vers ce pays et traiter celles-ci d'une manière incompatible, notamment, avec les finalités de leur transfert et au-delà de ce qui était strictement nécessaire et proportionné à la protection de la sécurité nationale. De même, la Commission a constaté qu'il n'existait pas, pour les personnes concernées, de voies de droit administratives ou judiciaires permettant, notamment, d'accéder aux données les concernant et, le cas échéant, d'obtenir leur rectification ou leur suppression.

2) S'agissant du niveau de protection substantiellement équivalent avec les libertés et droits fondamentaux garanti au sein de l'Union, la Cour constate que, en droit de l'Union, une réglementation n'est pas limitée au strict nécessaire, dès lors qu'elle autorise de manière généralisée la conservation de toutes les données à caractère personnel de toutes les personnes dont les données sont transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception ne soient opérées en fonction de l'objectif poursuivi et sans que des critères objectifs ne soient prévus en vue de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure.

La Cour ajoute qu'une règlementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée.

3) De même, la Cour relève qu'une règlementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, porte atteinte au contenu essentiel du droit fondamental à une protection juridictionnelle effective, une telle possibilité étant inhérente à l'existence d'un État de droit.

4) Enfin, la Cour constate que la décision de la Commission du 26 juillet 2000 prive les autorités nationales de contrôle de leurs pouvoirs, dans le cas où une personne remet en cause la compatibilité de la décision avec la protection de la vie privée et des libertés et droits fondamentaux des personnes. La Cour considère que la Commission n'avait pas la compétence de restreindre ainsi les pouvoirs des autorités nationales de contrôle.

Pour toutes ces raisons, la décision 2000/520 du 26 juillet 2000 est invalide.

CJUE, grande chambre, 6 octobre 2015, Schrems, C-362/14

5.2.2 Contrôle des autorités nationales

Contrôle des transferts de données à caractère personnel vers des pays tiers – Obligation de suspendre ou d'interdire de tels transferts en cas de violation du niveau de protection adéquat dans le pays tiers concerné – Conditions

L'article 58, paragraphe 2, sous f) et j), du RGPD doit être interprété en ce sens que, à moins qu'il existe une décision d'adéquation valablement adoptée par la Commission européenne, l'autorité de contrôle compétente est tenue de suspendre ou d'interdire un transfert de données vers un pays tiers fondé sur des clauses types de protection des données adoptées par la Commission, lorsque cette autorité de contrôle considère, à la lumière de l'ensemble des circonstances propres à ce transfert, que ces clauses ne sont pas ou ne peuvent pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union, en particulier par les articles 45 et 46 de ce règlement et par la Charte des droits fondamentaux, ne peut pas être assurée par d'autres moyens, à défaut pour le responsable du traitement ou son sous-traitant établis dans l'Union d'avoir lui-même suspendu le transfert ou d'avoir mis fin à celui-ci.

CJUE, grande chambre, 16 juillet 2020, Facebook Ireland et Schrems, C-311/18

Transfert de données à caractère personnel – Plainte d'une personne physique dont les données ont été transférées depuis l'Union européenne vers les États-Unis – Décision de la Commission constatant un niveau adéquat de protection – Office des autorités nationales de contrôle

Une décision de la Commission constatant un niveau adéquat de protection assuré par un pays tiers, autorisant le transfert des données à caractère personnel vers ce pays, ne saurait « ni annihiler ni réduire les pouvoirs expressément reconnus aux autorités nationales de contrôle par l'article 8 paragraphe 3 de la Charte ».

Les autorités nationales de contrôle, saisies par une personne d'une demande relative à la protection de ses droits et libertés à l'égard du traitement des données à caractère personnel la concernant, doivent pouvoir examiner, en toute indépendance, si le transfert de ces données respecte les exigences posées par la directive.

L'article 25, paragraphe 6, de la directive 95/46/CE du 24 octobre 1995, lu à la lumière des articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'une décision adoptée au titre de cette disposition, telle que la décision 2000/520/CE de la Commission, du 26 juillet 2000 (« Safe Harbor »), conformément à la directive 95/46 relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, par laquelle la Commission européenne constate qu'un pays tiers assure un niveau de protection adéquat, ne fait pas obstacle à ce qu'une autorité de contrôle d'un État membre, au sens de l'article 28 de cette directive, examine la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant qui ont été transférées depuis un État membre vers ce pays tiers, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans celui-ci n'assurent pas un niveau de protection adéquat.

Dans l'hypothèse, où ladite autorité estime fondés les griefs avancés par la personne l'ayant saisie d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de ses données à caractère personnel, cette même autorité doit, conformément à l'article 28, paragraphe 3, premier alinéa, troisième tiret, de la directive 95/46, lu à la lumière notamment de l'article 8, paragraphe 3, de la Charte, pouvoir ester en justice. À cet égard, il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision.

CJUE, grande chambre, 6 octobre 2015, Schrems, C-362/14, points 53, 57, 64

5.3 Clauses contractuelles types

Transfert de données à caractère personnel vers les États-Unis – 1) Évaluation du niveau de protection d'un pays tiers après l'arrêt dit Schrems II et avant l'adoption du Data Privacy Framework – 2) Efficacité des « mesures additionnelles » de protection – Notification aux utilisateurs, rapports de transparence ou de politique de gestion des demandes d'accès gouvernementales – Insuffisance – 3) Techniques de chiffrement – Importateur – Obligation d'accorder l'accès ou de fournir les données importées

1) Pour les transferts de données à caractère personnel vers les États-Unis encadrés par des garanties appropriées telles que les clauses contractuelles types, il n'est pas nécessaire d'analyser plus en détails le cadre légal applicable aux États-Unis dans la mesure où la Cour a déjà procédé à une telle analyse dans son arrêt du 16 juillet 2020 (C-311/18). En effet, la Cour a constaté, d'une part, que les programmes de surveillance en cause ne correspondaient pas aux exigences minimales attachées, en droit de l'Union, au principe de proportionnalité, si bien qu'il n'était pas permis de considérer que les programmes de surveillance fondés sur ces dispositions sont limités au strict nécessaire. D'autre part, la Cour a constaté que le cadre juridique en cause ne conférait pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux, si bien que ces personnes ne disposaient pas d'un droit au recours effectif.

2) En ce qui concerne les « mesures juridiques et organisationnelles » adoptées par un responsable du traitement en complément de clauses contractuelles types pour le transfert de données vers les États-Unis, ni la notification des utilisateurs, ni la publication d'un rapport de transparence ou d'une politique de gestion des demandes d'accès gouvernementales ne permet concrètement d'empêcher ou de réduire l'accès des services de renseignement américains.

3) En ce qui concerne les techniques de chiffrement, telles que celles pour les données entreposées dans des centres de données transférées vers les États-Unis, un importateur établi aux États-Unis a dans tous les cas l'obligation d'accorder l'accès ou de fournir les données importées qui sont en sa possession, y compris les clés de chiffrement nécessaires pour rendre les données intelligibles. Tant qu'un importateur établi aux États-Unis a la possibilité d'accéder aux données des personnes physiques en texte clair, de telles mesures techniques ne peuvent être considérées comme efficaces en l'espèce.

CNIL, P, 3 février 2022, Mise en demeure, Société X, n° MED-2022-005, non publié

5.3.1 Conditions de validité

Décision 2010/87/UE instituant des clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers – Validité – Conditions d'examen – Insuffisance de la seule circonstance que les autorités du pays tiers ne sont pas liées – Existence de mécanismes permettant d'assurer un niveau de protection requis par le droit de l'Union et de suspendre ou d'interdire de tels transferts en cas de violation desdites clauses

L'examen de la décision 2010/87/UE de la Commission, du 5 février 2010, relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, telle que modifiée par la décision d'exécution (UE) 2016/2297 de la Commission, du 16 décembre 2016, au

regard des articles 7, 8 et 47 de la Charte des droits fondamentaux n'a révélé aucun élément de nature à affecter la validité de cette décision.

La validité de cette décision n'est pas remise en cause par le seul fait que les clauses types de protection des données figurant dans celle-ci ne lient pas, en raison de leur caractère contractuel, les autorités du pays tiers vers lequel un transfert des données pourrait être opéré. En revanche, cette validité dépend du point de savoir si ladite décision comporte des mécanismes effectifs permettant, en pratique, d'assurer que le niveau de protection requis par le droit de l'Union soit respecté et que les transferts de données à caractère personnel, fondés sur de telles clauses, soient suspendus ou interdits en cas de violation de ces clauses ou d'impossibilité de les honorer.

Or, la décision 2010/87 met en place de tels mécanismes. Cette décision instaure notamment une obligation pour l'exportateur des données et le destinataire du transfert de vérifier, au préalable, que ce niveau de protection soit respecté dans le pays tiers concerné et qu'elle oblige ce destinataire à informer l'exportateur des données de son éventuelle incapacité de se conformer aux clauses types de protection, à charge alors pour ce dernier de suspendre le transfert de données et/ou de résilier le contrat conclu avec le premier.

CJUE, grande chambre, 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, points 136-137, 141-142

5.4 Code de conduite

5.5 Certification

5.6 Règles d'entreprise contraignantes

5.7 Dérogations

5.7.1 Consentement

Consentement au dépôt de cookies – Consentement explicite au transfert de données vers un pays tiers – Absence d'équivalence

Le consentement par la personne concernée au dépôt de traceurs lors de sa visite sur un site internet ne saurait être considéré comme équivalent au « consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées » au sens de l'article 49.1.a du RGPD.

CNIL, P, 3 février 2022, Mise en demeure, Société X, n° MED-2022-005, non publié

5.7.2 Intérêt public

5.7.3 Intérêt légitime

5.8 Transferts et divulgations non autorisés

5.9 Accords avec des pays tiers

Données PNR – Conditions de compatibilité d'un accord de transfert de données avec la Charte des droits fondamentaux

Le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers permet le transfert systématique et continu des données PNR de l'ensemble des passagers aériens à une autorité canadienne en vue de leur utilisation et de leur conservation, ainsi que de leur éventuel transfert ultérieur à d'autres autorités et d'autres pays tiers, dans le but de lutter contre le terrorisme et les formes graves de criminalité transnationale. À cet effet, l'accord envisagé prévoit, entre autres, une durée de stockage des données de cinq ans ainsi que des exigences en matière de sécurité et d'intégrité des données PNR, un masquage immédiat des données sensibles, des droits d'accès aux données, de rectification et d'effacement et la possibilité d'introduire des recours administratifs ou judiciaires.

La Cour juge que certaines stipulations du projet d'accord envisagé sont incompatibles avec les droits fondamentaux, à moins que celui-ci ne soit révisé pour mieux encadrer et préciser les ingérences. Cet accord doit, pour être compatible avec les articles 7 et 8 ainsi qu'avec l'article 52, paragraphe 1, de la Charte des droits fondamentaux :

a) déterminer de manière claire et précise les données des dossiers passagers à transférer depuis l'Union européenne vers le Canada ;

b) prévoir que les modèles et les critères utilisés dans le cadre du traitement automatisé des données des dossiers passagers seront spécifiques et fiables ainsi que non discriminatoires ; prévoir que les bases de données utilisées seront limitées à celles exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave ;

c) soumettre, hormis dans le cadre des vérifications relatives aux modèles et aux critères préétablis sur lesquels sont fondés les traitements automatisés des données des dossiers passagers, l'utilisation de ces données par l'autorité canadienne compétente pendant le séjour des passagers aériens au Canada et après leur départ de ce pays, de même que toute communication desdites données à d'autres autorités, à des conditions matérielles et procédurales fondées sur des critères objectifs ; subordonner cette utilisation et cette communication, sauf cas d'urgence dûment justifiés, à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, dont la décision autorisant l'utilisation intervient à la suite d'une demande motivée de ces autorités, notamment dans le cadre de procédures de prévention, de détection ou de poursuites pénales ;

d) limiter la conservation des données des dossiers passagers après le départ des passagers aériens à celles des passagers à l'égard desquels il existe des éléments objectifs permettant de considérer qu'ils pourraient présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave ;

e) soumettre la communication des données des dossiers passagers par l'autorité canadienne compétente aux autorités publiques d'un pays tiers à la condition qu'il existe soit un accord entre l'Union européenne et ce pays tiers équivalent à l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, soit une décision de la Commission

européenne, au titre de l'article 25, paragraphe 6, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, couvrant les autorités vers lesquelles la communication des données des dossiers passagers est envisagée ;

f) prévoir un droit à l'information individuelle des passagers aériens en cas d'utilisation des données des dossiers passagers les concernant pendant leur séjour au Canada et après leur départ de ce pays ainsi qu'en cas de divulgation de ces données par l'autorité canadienne compétente à d'autres autorités ou à des particuliers, et

g) garantir que la surveillance des règles prévues par l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, relatives à la protection des passagers aériens à l'égard du traitement des données des dossiers passagers les concernant, est assurée par une autorité de contrôle indépendante.

CJUE, grande chambre, 26 juillet 2017, Avis sur l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des passagers, Avis 1/15

Transfert de données vers un pays ne faisant pas l'objet d'une décision d'adéquation et ne présentant pas de garantie suffisante au regard du niveau de protection offert par le droit européen – La ratification d'un accord de transfert ne saurait avoir pour effet de dispenser les autorités françaises chargées de transférer ces données des obligations qui leur incombent en application du RGPD. – Conditions de vérification

L'avenant à la convention du 15 avril 1999 entre le Gouvernement de la République française et le Gouvernement de la République du Botswana en vue d'éviter les doubles impositions et de prévenir l'évasion et la fraude fiscales en matière d'impôts comporte, en son article premier, des dispositions dont la mise en œuvre peut impliquer des transferts aux autorités botswanaises de données personnelles par les autorités françaises.

La législation concernant les données personnelles dans la République du Botswana, qui n'a pas fait l'objet d'une décision d'adéquation de la Commission européenne, ne présentant pas aujourd'hui de garantie suffisante au regard du niveau de protection offert par le droit européen, le Conseil d'État (section des finances) estime que la ratification, après autorisation parlementaire, de cet accord ne saurait avoir pour effet de dispenser les autorités françaises, chargées de transférer des données contenues dans des traitements automatisés de données à caractère personnel vers un État n'appartenant pas à l'Union européenne, des obligations qui leur incombent en application des dispositions du RGPD ainsi que, le cas échéant, des articles 123 et 124 de la section 3 du chapitre II de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans sa version issue de l'ordonnance n° 2018-1125 du 12 décembre 2018.

Cette vérification devra tenir compte, à la date du transfert des données, non seulement du niveau spécifique de protection garanti par le traitement appliqué aux données objet du transfert, mais aussi de l'ensemble des circonstances qui commandent l'application effective des règles de protection définies pour ce transfert.

CE, Section des finances, 12 février 2019, Avis n° 396689, Avenant à la convention du 15 avril 1999 entre la France et le Botswana en vue d'éviter les doubles impositions et de prévenir l'évasion et la fraude fiscale en matière d'impôts

---

6. Règles spéciales et applications sectorielles

6.1 Dans le domaine de la santé

6.1.1 Champ d'application

6.1.2 Intérêt public

6.1.3 Recherche

6.1.4 Secret médical

Registre de contention et d'isolement des établissements de santé (art. L. 3222-5-1 du code de la santé publique) – Communication au titre de la loi CADA – 1) Conditions – Occultation des éléments identifiant les patients et les soignants – 2) Cas où l'identité des patients a fait l'objet d'une pseudonymisation – Contrôle du juge administratif – Risque d'atteinte à la protection de la vie privée et au secret médical – Illustration – Communicabilité à des tiers de l'identifiant dit « anonymisé » du patient – Exclusion

1) Le registre de contention et d'isolement comporte des mentions qui ne sont pas soumises à occultation préalable avant leur communication, telles que les dates, les heures et la durée de chaque mesure de contention forcée ou d'isolement. Les éléments permettant d'identifier les patients doivent, en application des articles L. 311-6 et L. 311-7 du code des relations entre le public et l'administration, être occultés préalablement à la communication du registre de contention et d'isolement, afin de ne pas porter atteinte au secret médical et à la protection de la vie privée, comme doivent également l'être celles permettant d'identifier les soignants, afin d'éviter que la divulgation d'informations les concernant puisse leur porter préjudice.

2) Dans le cas où l'identité des patients a fait l'objet d'une pseudonymisation, laquelle ne permet l'identification des personnes en cause qu'après recoupement d'informations, il appartient au juge administratif d'apprécier si, eu égard à la sensibilité des informations en cause et aux efforts nécessaires pour identifier les personnes concernées, leur communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. En l'espèce, compte tenu de la nature des informations en cause, qui touchent à la santé mentale des patients, et du nombre restreint de personnes pouvant faire l'objet d'une mesure de contention et d'isolement, facilitant ainsi leur identification, alors au demeurant que les autorités énumérées à l'article L. 3222-5-1 du code de la santé publique peuvent accéder à l'ensemble des informations figurant sur les registres et contrôler l'activité des établissements concernés, l'identifiant dit " anonymisé " figurant dans ces registres, qu'il s'agisse, selon la pratique du centre hospitalier, de " l'identifiant permanent du patient " (IPP) ou d'un identifiant spécialement défini, doit être regardé comme une information dont la communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. Cet identifiant n'est donc communicable qu'au seul intéressé en vertu des dispositions de l'article L. 311-6 du code des relations entre le public et l'administration.

CE, 10ème-9ème chambres réunies, 8 février 2023, Association « commission des citoyens pour les droits de l'homme », n°455887, T., points 5-7

Secret médical (art. L. 1110-4 du code de la santé publique) – Partage d'informations

entre professionnels de santé ne faisant pas partie de la même équipe de soins – Obligation de recueillir le consentement de l'intéressé – Existence

Il résulte de l'article L. 1110-4 du code de la santé publique que le partage d'informations couvertes par le secret médical et nécessaires à la prise en charge d'une personne, entre professionnels de santé ne faisant pas partie de la même équipe de soins, requiert le consentement préalable de cette personne, ce à quoi l'article 275 du code de procédure civile ne permet pas, en tout état de cause, de déroger.

CE, 4ème-1ère chambres réunies, 15 novembre 2022, SCP B., n°441387, T., point 5

Personnes accédant au traitement ou destinataires de données de santé – Secret médical et droit d'en connaître – Portée

Dans le cadre d'un traitement mis en œuvre pour le compte de l'État et contenant des données recueillies par des professionnels de santé et couvertes par le secret médical, il revient au responsable du traitement de s'assurer que les personnes accédant au traitement ou destinataires des données qui pourraient avoir connaissance des données couvertes par le secret médical ont bien le droit d'en connaître.

Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne portées à la connaissance d'un professionnel de santé, de tout membre du personnel d'un établissement, service ou organisme concourant à la prévention ou aux soins et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. La Commission rappelle que ce secret s'impose à tous les professionnels intervenant dans le système de santé qui pourraient être amenés à transmettre des informations afin qu'elles soient enregistrées dans le traitement.

CNIL, P, 21 avril 2022, Avis sur projet de décret, n° 2022-051, non publié

6.2 Police-Justice

6.2.1 Règles principales et obligations particulières

Les articles 13 et 54 de la directive 2016/680 (*droit à l'information et droit d'accès*), lus à la lumière de l'article 47 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux doivent être interprétés en ce sens qu'ils s'opposent à une réglementation nationale qui autorise les autorités compétentes à tenter d'accéder à des données contenues dans un téléphone portable sans informer la personne concernée, dans le cadre des procédures nationales applicables, des motifs sur lesquels repose l'autorisation d'accéder à ces données, délivrée par un juge ou une entité administrative indépendante, à partir du moment où la communication de cette information n'est plus susceptible de compromettre les missions incombant à ces autorités en vertu de cette directive.

CJUE, 28 novembre 2024, Ministerstvo na vatreshnite raboti, C-80/23

Réglementation nationale qui octroie aux autorités compétentes la possibilité d'accéder aux données contenues dans un téléphone portable, à des fins de police judiciaire - 1) Conditions - Contrôle préalable par une juridiction ou une autorité

administrative indépendante – 2) Informations à mettre à la disposition de la personne concernée ou à lui fournir

1) L'article 4, paragraphe 1, sous c), de la directive (UE) 2016/680 (directive « Police-justice) du 27 avril 2016 (*principes relatifs au traitement des données à caractère personnel*), lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale qui octroie aux autorités compétentes la possibilité d'accéder aux données contenues dans un téléphone portable, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, si cette réglementation :

-définit de manière suffisamment précise la nature ou les catégories des infractions concernées,

-garantit le respect du principe de proportionnalité, et

-soumet l'exercice de cette possibilité, sauf cas d'urgence dûment justifié, à un contrôle préalable d'un juge ou d'une entité administrative indépendante.

2) Les articles 13 et 54 de la directive 2016/680 (*droit à l'information et droit d'accès*), lus à la lumière de l'article 47 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux doivent être interprétés en ce sens qu'ils s'opposent à une réglementation nationale qui autorise les autorités compétentes à tenter d'accéder à des données contenues dans un téléphone portable sans informer la personne concernée, dans le cadre des procédures nationales applicables, des motifs sur lesquels repose l'autorisation d'accéder à ces données, délivrée par un juge ou une entité administrative indépendante, à partir du moment où la communication de cette information n'est plus susceptible de compromettre les missions incombant à ces autorités en vertu de cette directive.

CJUE, 4 octobre 2024, Bezirkshauptmannschaft Landeck, C-548/21

Directive 2014/41/UE – Transmission et utilisation de preuves dans les affaires pénales revêtant une dimension transfrontalière – Conditions - 1) Compétence du procureur – 2) Décision de transmission de preuves acquises à la suite de l'interception de télécommunications chiffrées des utilisateurs de téléphones portables – 3) Notification de l'infiltration d'appareils terminaux visant à extraire des données de trafic, de localisation et de communication – 4) Protection des droits des utilisateurs concernés par une mesure d'« interception de télécommunications » – 5) Eléments de preuve que la personne soupçonnée n'est pas en mesure de commenter efficacement ces informations

1) L'article 1er, paragraphe 1, et l'article 2, sous c), de la directive 2014/41/UE du Parlement européen et du Conseil, du 3 avril 2014, concernant la décision d'enquête européenne en matière pénale, doivent être interprétés en ce sens qu'une décision d'enquête européenne visant à la transmission de preuves déjà en la possession des autorités compétentes de l'État d'exécution ne doit pas nécessairement être prise par un juge lorsque, en vertu du droit de l'État d'émission, dans une procédure purement interne à cet État, la collecte initiale de ces preuves aurait dû être ordonnée par un juge, mais qu'un procureur est compétent pour ordonner la transmission desdites preuves.

2) L'article 6, paragraphe 1, de la directive 2014/41 doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'un procureur adopte une décision d'enquête européenne qui vise à la transmission de preuves déjà en la possession des autorités compétentes de l'État d'exécution, lorsque ces preuves ont été acquises à la suite de l'interception, par ces autorités, sur le territoire de l'État d'émission, de télécommunications de l'ensemble des utilisateurs de téléphones portables qui permettent, grâce à un logiciel spécial et à un matériel modifié, une communication chiffrée de bout en bout, pourvu qu'une telle décision respecte l'ensemble des conditions prévues, le cas échéant, par le droit de l'État d'émission pour la transmission de telles preuves dans une situation purement interne à cet État.

3) L'article 31 de la directive 2014/41 doit être interprété en ce sens qu'une mesure liée à l'infiltration d'appareils terminaux, visant à extraire des données de trafic, de localisation et de communication d'un service de communication fondé sur l'internet, constitue une « interception de télécommunications », au sens de cet article, qui doit être notifiée à l'autorité désignée à cet effet par l'État membre sur le territoire duquel se trouve la cible de l'interception. Dans l'hypothèse où l'État membre interceptant n'est pas en mesure d'identifier l'autorité compétente de l'État membre notifié, cette notification peut être adressée à toute autorité de l'État membre notifié que l'État membre interceptant juge apte à cet effet.

4) L'article 31 de la directive 2014/41 doit être interprété en ce sens qu'il vise également à protéger les droits des utilisateurs concernés par une mesure d'« interception de télécommunications », au sens de cet article.

5) L'article 14, paragraphe 7, de la directive 2014/41 doit être interprété en ce sens qu'il impose au juge pénal national d'écarter, dans le cadre d'une procédure pénale ouverte contre une personne soupçonnée d'actes de criminalité, des informations et des éléments de preuve si cette personne n'est pas en mesure de commenter efficacement ces informations ainsi que ces éléments de preuve et que ceux-ci sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

CJUE, 30 avril 2024, M. N. (EncroChat), C-670/22

Législation nationale prévoyant la conservation par les autorités de police, à des fins de prévention et de détection des infractions pénales de données à caractère personnel, y compris biométriques et génétiques, concernant des personnes ayant fait l'objet d'une condamnation pénale définitive jusqu'au décès de ces personnes - Inconventionnalité

L'article 4, paragraphe 1, sous c) et e), de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, lu en combinaison avec les articles 5 et 10, l'article 13, paragraphe 2, sous b), ainsi que l'article 16, paragraphes 2 et 3, de celle-ci, et à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'il s'oppose à une législation nationale qui prévoit la conservation, par les autorités de police, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, de données à caractère personnel, notamment de données biométriques et génétiques, concernant des personnes ayant fait l'objet d'une condamnation pénale définitive pour une infraction pénale intentionnelle relevant de l'action publique, et ce jusqu'au décès de la personne concernée, y compris en cas de réhabilitation de celle-ci, sans mettre à la charge du responsable du traitement l'obligation de vérifier régulièrement si cette conservation est toujours nécessaire, ni reconnaître à ladite personne le droit à l'effacement de ces données, dès lors que leur conservation n'est plus nécessaire au regard des finalités pour lesquelles elles ont été traitées, ou, le cas échéant, à la limitation du traitement de celles-ci.

CJUE, 30 janvier 2024, NG c./ Direktor na Glavna direktsia « Natsionalna politsia » pri Ministerstvo na vatreshnite raboti – Sofia, C-118/22

Conservation et consultation des empreintes digitales d'un individu identifié ou identifiable – Habilitation des agents pouvant les consulter – Procédure entachée d'une nullité d'ordre public en l'absence d'habilitation

Au regard de l'ingérence dans le droit au respect de la vie privée que constituent, au sens de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, la conservation dans un fichier automatisé des empreintes digitales d'un individu identifié ou identifiable et la consultation de ces données, l'habilitation des agents pouvant les consulter est une garantie institutionnelle édictée pour la protection des libertés individuelles.

S'il ne résulte pas des pièces du dossier que l'agent ayant consulté les fichiers d'empreintes était expressément habilité à cet effet, la procédure se trouve entachée d'une nullité d'ordre public, sans que l'étranger qui l'invoque ait à démontrer l'existence d'une atteinte portée à ses droits.

Cass, 1re civ., 14 octobre 2020, n° 19-19.234, B., points 5-6

Contestation de l'habilitation d'un fonctionnaire de police – Accès à des fichiers biométriques – Retenue pour vérification du droit de circulation et de séjour

Lorsqu'une contestation porte sur l'habilitation d'un fonctionnaire de police à accéder à des fichiers biométriques à l'occasion d'une retenue pour vérification du droit de circulation et de séjour, il incombe au juge de vérifier s'il résulte des actes de la procédure, notamment des mentions, faisant foi jusqu'à preuve contraire, du procès-verbal contenant le résultat de la consultation des fichiers, que le fonctionnaire de police les ayant consultés était expressément habilité à cet effet.

Cass, 1re civ., 17 octobre 2018, n° 17-16.852, B., point 10

Catégories de données

Recours à la reconnaissance faciale en temps réel à des fins de prévention des infractions pénales – Mesures particulièrement intrusives en l'espèce et traitement de données sensibles – Manifestation d'opinions politiques – Inconventionnalité

Dans une jurisprudence constante, la Cour EDH juge que la conservation de photographies par la police, combinée à la possibilité de leur appliquer des techniques de reconnaissance faciale, constitue une ingérence dans l'exercice du droit à la vie privée. La Cour rappelle également qu'il est essentiel, dans le cadre de la mise en œuvre de la technologie de reconnaissance faciale, de disposer de règles détaillées régissant la portée et l'application des mesures ainsi que de garanties solides contre le risque d'abus et d'arbitraire. La nécessité de disposer de garanties est d'autant plus grande lorsque la technologie de reconnaissance faciale est utilisée en temps réel.

En l'espèce, le requérant russe qui a manifesté pacifiquement dans le métro moscovite, et dont des photographies et une vidéo ont été publiées sur un canal public de Telegram, a été identifié à partir de ces éléments, localisé puis interpellé, au moyen d'une technologie de reconnaissance faciale en temps réel.

Partant du principe selon lequel les mesures litigieuses poursuivaient le but légitime de la prévention des infractions pénales, la Cour estime que les mesures prises contre le requérant ont été particulièrement intrusives, surtout le recours à la technologie de reconnaissance faciale en temps réel. Un niveau élevé de justification est donc nécessaire pour qu'elles puissent être considérées comme « nécessaires dans une société démocratique », le niveau de justification le plus élevé étant requis pour l'utilisation de cette technologie. De plus, les données à caractère personnel qui ont été traitées renfermant des informations sur la participation du requérant à une manifestation pacifique, elles ont par conséquent révélé les opinions politiques de l'intéressé. Elles appartenaient donc aux catégories particulières de données sensibles qui appellent un niveau de protection accru.

Le droit interne russe autorisait le traitement des données biométriques à caractère personnel dans le cadre de l'enquête et des poursuites engagées pour toute infraction, quelles qu'en fussent la nature et la gravité.

Le requérant a été poursuivi pour une infraction administrative mineure qui n'a représenté aucun risque pour l'ordre public ou la sécurité des transports. Il n'a pas été accusé d'avoir commis un acte répréhensible au cours de sa manifestation. L'utilisation d'une technologie de reconnaissance faciale très intrusive pour identifier et arrêter les participants à des actions de protestation pacifiques pourrait produire un effet dissuasif dans le domaine des droits à la liberté d'expression et de réunion.

Dans ces conditions, le traitement des données à caractère personnel du requérant au moyen de la technologie de reconnaissance faciale dans le cadre de la procédure administrative, ne répondait pas à un « besoin social impérieux » et ne pouvait être considéré comme « nécessaire dans une société démocratique ». La Cour EDH conclut donc à une violation de l'article 8.

CEDH, 4 octobre 2023, Glukhin c. Russie, n°11519/20

Personnes mineures – Durée de conservation – Conciliation entre la nécessité d'identifier les auteurs d'infractions et celle de rechercher le relèvement éducatif et moral des mineurs délinquants

S'agissant des traitements automatisés d'informations nominatives des services de police et de gendarmerie, il appartiendra au décret prévu au V de l'article 21 de la loi pour la sécurité intérieure de déterminer une durée de conservation des faits impliquant des mineurs conciliant, d'une part, la nécessité d'identifier les auteurs d'infractions et, d'autre part, celle de rechercher le relèvement éducatif et moral des mineurs délinquants.

CC, 2003-467 DC, 13 mars 2003, Loi pour la sécurité intérieure, points 36-38

6.2.2 Traitements relatifs aux documents d'identité

Article 4, paragraphe 3, règlement n°2252 /2004 – Absence d'obligation des États membres de garantir que les données biométriques ne seront pas utilisées ou conservées à d'autres fins que la délivrance d'un passeport ou d'un document de voyage

L'article 4, paragraphe 3, du règlement n° 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres n'oblige pas les États membres à garantir, dans leur législation, que les données biométriques rassemblées et conservées conformément audit règlement ne seront pas rassemblées, traitées et utilisées à des fins autres que la délivrance du passeport ou du document de voyage, un tel aspect ne relevant pas du champ d'application dudit règlement.

CJUE, 16 avril 2015, Willems e. a., C-446/12 à C-449/12

Protection des passeports contre leur utilisation frauduleuse de manière suffisamment efficace – Recueil des empreintes digitales – Proportionnalité – Existence

Il n'a pas été porté à la connaissance de la Cour l'existence de mesures susceptibles de contribuer, de manière suffisamment efficace, au but tenant à la protection des passeports contre leur utilisation frauduleuse, tout en portant des atteintes moins importantes aux droits reconnus par les articles 7 et 8

de la Charte que celles entraînées par la méthode fondée sur les empreintes digitales. Ce recueil est donc proportionné.

CJUE, 17 octobre 2013, Schwarz, C-291/12, point 53

Traitement de données notamment biométriques visant à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage – Nature, ampleur, caractéristiques techniques et conditions de consultation – Non-conformité

La création d'un traitement de données à caractère personnel destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage permet de sécuriser la délivrance de ces titres et d'améliorer l'efficacité de la lutte contre la fraude. Elle est ainsi justifiée par un motif d'intérêt général. Toutefois, compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française. Les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles. Les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne. Les dispositions de la loi relative à la protection de l'identité autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire.

Il résulte de ce qui précède qu'eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi. Par suite, les articles 5 et 10 de la loi relative à la protection de l'identité doivent être déclarés contraires à la Constitution.

CC, 2012-652 DC, 22 mars 2012, Loi relative à la protection de l'identité, points 8-11

Données adéquates, pertinentes et non excessives – Condition non remplie – Conservation dans un traitement informatisé des données à caractère personnel recueillies lors de l'établissement ou du renouvellement des passeports de huit empreintes digitales alors que le passeport n'en contient que deux

Constitution d'un traitement automatisé centralisé des données à caractère personnel (état civil, image numérisée du visage et empreintes de huit doigts) recueillies auprès des personnes âgées d'au moins six ans lors de l'établissement ou du renouvellement des passeports.

La finalité de la consultation des empreintes digitales contenues dans le traitement automatisé (confirmer que la personne présentant une demande de renouvellement d'un passeport est bien celle à laquelle le passeport a été initialement délivré ou à s'assurer de l'absence de falsification des données contenues dans le composant électronique du passeport) peut être atteinte de manière suffisamment efficace en comparant les empreintes figurant dans le composant électronique du passeport avec celles conservées dans le traitement, sans qu'il soit nécessaire que ce dernier en contienne davantage.

Dès lors, le Conseil d'État annule l'article litigieux du fait de l'inconventionnalité de la collecte et de la conservation d'un plus grand nombre d'empreintes digitales que celles figurant dans le composant électronique, ces données n'étant ni adéquates, ni pertinentes et apparaissant excessives au regard des finalités du traitement informatisé.

CE, Assemblée, 26 octobre 2011, Association pour la promotion de l'image et autres, n° 317827, Rec., points 11-12

6.2.3 Traitements relatifs aux données de ressortissants étrangers

Traitement comportant empreintes digitales et photographies de mineurs non accompagnés – Intérêt supérieur de l'enfant – OVC de lutte contre l'immigration irrégulière – Exclusion de la reconnaissance faciale – Durée de conservation limitée et respect de la loi Informatique et Libertés – Conciliation non disproportionnée

Les dispositions contestées créent un traitement automatisé comportant les empreintes digitales et la photographie des ressortissants étrangers qui se déclarent mineurs privés temporairement ou définitivement de la protection de leur famille.

En évitant la réitération par des personnes majeures de demandes de protection qui ont déjà donné lieu à une décision de refus, le traitement automatisé mis en place par les dispositions contestées vise à faciliter l'action des autorités en charge de la protection des mineurs et à lutter contre l'entrée et le séjour irréguliers des étrangers en France. Ce faisant, et alors qu'aucune norme constitutionnelle ne s'oppose par principe à ce qu'un traitement automatisé poursuive plusieurs finalités, le législateur a, en adoptant les dispositions contestées, entendu mettre en œuvre l'exigence constitutionnelle de protection de l'intérêt supérieur de l'enfant et poursuivi l'objectif de valeur constitutionnelle de lutte contre l'immigration irrégulière.

Par ailleurs, les dispositions contestées prévoient le recueil, l'enregistrement et le traitement des empreintes digitales et de la photographie des ressortissants étrangers qui sollicitent le bénéfice des dispositifs de protection de l'enfance et excluent tout dispositif de reconnaissance faciale. Ainsi, les données recueillies sont celles nécessaires à l'identification de la personne et à la vérification de ce qu'elle n'a pas déjà fait l'objet d'une évaluation de son âge. Enfin, d'une part, les dispositions contestées prévoient que la conservation des données des personnes reconnues mineures est limitée à la durée strictement nécessaire à leur prise en charge et à leur orientation, en tenant compte de leur situation personnelle. D'autre part, le fichier instauré par les dispositions contestées est mis en œuvre dans le respect de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Conciliation non disproportionnée entre la sauvegarde de l'ordre public et le droit au respect de la vie privée

CC, 2019-797 QPC, 26 juillet 2019, Unicef France et autres, points 6, 8-10

Projet de décret pour l'application des articles L. 744-6 et L. 744-7 CESEDA – Traitement de données des vulnérabilités des demandeurs d'asile – Intérêt public – Légalité – Exception des données n'ayant pas été volontairement communiquées

Le Conseil d'État (section de l'intérieur) a donné un avis favorable au projet de décret pris pour l'application des articles L. 744-6 et L. 744-7 du code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA) et portant création du traitement automatisé de données à caractère personnel prévu par ces articles sous réserve de plusieurs observations.

L'article L. 744-6 du CESEDA confie à l'Office français de l'immigration et de l'intégration (OFII) la charge d'évaluer la vulnérabilité des demandeurs d'asile et permet que les informations recueillies dans ce cadre puissent faire l'objet d'un traitement automatisé, dans les conditions fixées par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le décret mettant en œuvre ce fichier est justifié par un intérêt public et échappe, en application du IV de l'article 8 de la même loi, à l'interdiction de collecte et de traitement des données à caractère personnel relatives à la santé prévue par le I du même article.

Le Conseil d'État estime que le projet de décret pouvait légalement prévoir l'enregistrement des données de vulnérabilité, à l'exception toutefois des données de santé à caractère personnel qui

n'auraient pas été volontairement communiquées par le demandeur d'asile, ainsi que l'accès à ces données par les personnels de l'OFII, les agents chargés de l'accueil des demandeurs d'asile relevant des ministères de l'intérieur et des affaires sociales et de l'Office français de protection des réfugiés et des apatrides, dans la limite de leurs attributions et du besoin d'en connaître.

CE, Section de l'intérieur, 17 janvier 2017, Avis n° 392228, Projet de décret pris pour l'application des articles L. 744-6 et L. 744-7 du code de l'entrée et du séjour des étrangers et du droit d'asile et portant création du traitement automatisé de données à caractère personnel

---

Ministre de l'intérieur – Incompétence pour créer un fichier informatique destiné à faciliter l'éloignement des étrangers en situation irrégulière (fichier « ELOI » créé par arrêté du 30 juillet 2006)

En application des dispositions des articles L. 611-3 et L. 611-5 du code de l'entrée et du séjour des étrangers et du droit d'asile, seul un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, peut fixer les modalités de mise en œuvre, relatives notamment à la durée de conservation et aux conditions de mise à jour des informations enregistrées, à la détermination des fonctionnaires habilités à y accéder ainsi qu'à la définition des conditions dans lesquelles les personnes concernées peuvent exercer leur droit d'accès, du traitement automatisé d'un fichier dont la finalité est de faciliter l'éloignement des étrangers en situation irrégulière et comporte, parmi les informations collectées, une photographie d'identité des intéressés.

En conséquence, illégalité de la création d'un fichier de cette nature, dénommé fichier « ELOI », par arrêté ministériel en date du 30 juillet 2006.

CE, 10ème/9ème SSR, 12 mars 2007, Gisti et autres, n° 297888, Rec., point 6

6.2.4 Techniques d'enquête

1) Utilisation de dispositifs techniques permettant de recueillir les données de connexion et de localisation, d'intercepter des correspondances émises ou reçues par un équipement terminal, de capter, fixer et enregistrer des paroles ou des images dans des lieux publics ou privés – Autorisation de recourir à ces techniques spéciales pour tout crime dans le cadre d'une enquête de flagrance ou préliminaire – Absence de contrôle suffisant par le juge du maintien du caractère nécessaire et proportionné – Absence de conciliation équilibrée – 2) Dispositifs techniques permettant d'accéder à des données informatiques – Infraction relevant de la criminalité ou de la délinquance organisées – Conformité – 3) Géolocalisation – Conditions de mise en œuvre – Conformité

1) En premier lieu, les techniques spéciales d'enquête désignent plusieurs mesures d'investigation : l'utilisation d'un dispositif technique permettant de recueillir les données de connexion d'un équipement terminal, les données relatives à sa localisation, mais également l'interception des correspondances émises ou reçues par cet équipement ; l'utilisation d'un dispositif technique, éventuellement installé dans un lieu privé, ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles dans des lieux privés ou publics, ou l'image des personnes se trouvant dans un lieu privé ; l'utilisation d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues

et émises par des périphériques. Ces techniques présentent donc un caractère particulièrement intrusif.

En deuxième lieu, le législateur a prévu que le recours à ces techniques spéciales est autorisé, dans le cadre d'une enquête de flagrance ou préliminaire, pour tout crime, et non pour les seules infractions relevant de la criminalité et de la délinquance organisées. Or, si une infraction d'une particulière gravité et complexité est de nature à justifier le recours à de telles mesures, tel n'est pas nécessairement le cas d'infractions ne présentant pas ces caractères.

En troisième lieu, cette autorisation est délivrée, à la requête du procureur de la République, par le juge des libertés et de la détention. Toutefois, si le juge des libertés et de la détention peut ordonner à tout moment l'interruption des techniques spéciales d'enquête, les dispositions légales ne prévoient pas qu'il peut accéder à l'ensemble des éléments de la procédure. Ainsi, alors que son autorisation est donnée pour une durée d'un mois, il n'a pas accès aux procès-verbaux réalisés dans le cadre de l'enquête en cours autres que ceux dressés en exécution de sa décision et n'est pas informé du déroulé de l'enquête en ce qui concerne les investigations autres que les actes accomplis en exécution de sa décision.

Il résulte de ce qui précède que le législateur a autorisé le recours à des techniques d'enquête particulièrement intrusives pour des infractions ne présentant pas nécessairement un caractère de particulière complexité, sans assortir ce recours des garanties permettant un contrôle suffisant par le juge du maintien du caractère nécessaire et proportionné de ces mesures durant leur déroulé.

Le législateur n'a donc pas opéré une conciliation équilibrée entre, d'un côté, l'objectif de recherche des auteurs d'infractions et, de l'autre, le droit au respect de la vie privée et le secret des correspondances.

En outre, en prévoyant que, en cas d'urgence, l'autorisation de recourir à une de ces techniques spéciales d'enquête peut être délivrée par le procureur de la République et peut se poursuivre sans contrôle ni intervention d'un magistrat du siège pendant vingt-quatre heures, le législateur a porté une atteinte inconstitutionnelle au droit au respect de la vie privée et au secret des correspondances.

2) En autorisant, pour les nécessités d'une enquête ou d'une information relatives à une infraction relevant de la criminalité ou de la délinquance organisée, le recours à des dispositifs techniques permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre telles qu'elles sont reçues et émises par des périphériques, y compris non audiovisuels, le législateur n'a pas méconnu le droit au respect de la vie privée.

3) En premier lieu, la géolocalisation est une mesure de police judiciaire consistant à surveiller une personne au moyen de procédés techniques en suivant, en temps réel, la position géographique d'un véhicule que cette personne est supposée utiliser ou de tout autre objet, notamment un téléphone, qu'elle est supposée détenir. La mise en œuvre de ce procédé n'implique pas d'acte de contrainte sur la personne visée, ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son. L'atteinte à la vie privée qui résulte de la mise en œuvre de ce dispositif réside dans la surveillance par localisation continue et en temps réel de la personne, le suivi de ses déplacements dans tous lieux publics ou privés, ainsi que dans l'enregistrement et le traitement des données ainsi obtenues.

En second lieu, le recours à la géolocalisation est placé sous la direction et le contrôle de l'autorité judiciaire. Lorsqu'elle est autorisée pour une procédure de recherche des causes de la mort ou de blessures graves, d'une disparition, d'une personne en fuite ou dans le cadre d'une enquête pour une infraction relevant de la criminalité organisée, le procureur de la République ne peut l'autoriser que pour une durée maximale de quinze jours consécutifs. Dans les autres cas, la durée de son autorisation ne peut excéder huit jours consécutifs. À l'issue de ce délai, elle est autorisée par le juge des libertés et de la détention pour une durée maximale d'un mois renouvelable. En outre, la durée totale de l'opération ne peut excéder un an ou, s'il s'agit d'une infraction relevant de la délinquance organisée, deux ans. Lorsque, en cas d'urgence, elle est mise en place ou prescrite par un officier de police judiciaire, le procureur de la République, immédiatement informé, peut en prescrire la mainlevée.

Dès lors, en prévoyant qu'il peut être recouru à la géolocalisation lorsque les nécessités de l'enquête concernant un crime ou un délit puni d'une peine d'emprisonnement d'au moins trois ans l'exigent, le législateur a opéré une conciliation équilibrée entre l'objectif de valeur constitutionnelle de recherche des auteurs d'infraction et le droit au respect de la vie privée.

CC, 2019-778 DC, 21 mars 2019, Loi de programmation 2018-2022 et de réforme pour la justice, points 161-167, 148-150

Géolocalisation – Conditions de mise en œuvre – Conformité

Le recours à la géolocalisation ne peut avoir lieu que lorsque l'exigent les nécessités de l'enquête ou de l'instruction concernant un crime ou un délit puni d'une peine d'emprisonnement d'au moins trois ans, s'agissant d'atteinte aux personnes, d'aide à l'auteur ou au complice d'un acte de terrorisme ou d'évasion, ou d'au moins cinq ans d'emprisonnement, s'agissant de toute autre infraction, ainsi qu'à des enquêtes ou instructions portant sur la recherche des causes de la mort, des causes de la disparition d'une personne ou des procédures de recherche d'une personne en fuite.

Le recours à la géolocalisation est placé sous la direction et le contrôle de l'autorité judiciaire. Dans les cas prévus par le 1° de l'article 230-33 du code de procédure pénale, le procureur de la République ne peut l'autoriser que pour une durée maximale de 15 jours consécutifs. À l'issue de ce délai, elle est autorisée par le juge des libertés et de la détention pour une durée maximale d'un mois renouvelable. Dans les cas prévus au 2° du même article, le juge d'instruction peut l'autoriser pour une durée maximale de quatre mois renouvelable. Lorsqu'en cas d'urgence elle est mise en place ou prescrite par un officier de police judiciaire, le procureur de la République ou le juge d'instruction, immédiatement informé, peut en prescrire la mainlevée.

Il résulte de tout ce qui précède que le législateur a entouré la mise en œuvre de la géolocalisation de mesures de nature à garantir que, placées sous l'autorisation et le contrôle de l'autorité judiciaire, les restrictions apportées aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité et ne revêtent pas un caractère disproportionné au regard de la gravité et de la complexité des infractions commises.

CC, 2014-693 DC,25 mars 2014, Loi relative à la géolocalisation, points 14, 15, 17

Interceptions téléphoniques – Matériel technique fourni par un prestataire n'accomplissant aucun acte de procédure – Moyen de nullité écarté

Attendu que, pour écarter le moyen de nullité visant les interceptions téléphoniques, pris de la violation des articles 100-3 du code de procédure pénale, 4 et 26 de la loi n°78-17 du 6 janvier 1978, en raison de l'intervention d'une société, non habilitée par l'autorité de tutelle, l'arrêt attaqué relève que celle-ci met à disposition des enquêteurs et magistrats du matériel permettant l'acheminement des données, dont elle n'est pas à l'origine et qu'elle ne détient que provisoirement, de manière précaire, en fournissant des moyens techniques ; que les juges ajoutent qu'elle n'est pas chargée de retranscrire les conversations auxquelles elle n'a d'ailleurs pas accès.

Attendu qu'en statuant ainsi, dès lors qu'aucune violation des dispositions légales en matière d'interception de communications téléphoniques ne saurait résulter de la simple fourniture à un service de police du matériel technique lui permettant d'y procéder par un prestataire qui n'accomplit aucun acte de procédure, la chambre de l'instruction a justifié sa décision.

Cass, crim., 22 mars 2016, n° 15-83.207, B., points 16-17

6.2.5 Autres fichiers et traitements

FAED

FNAEG

Refus de se soumettre à un prélèvement biologique destiné à un enregistrement dans le FNAEG – Absence de suite donnée à la réserve du Conseil constitutionnel – Conservation des profils ADN dans le FNAEG – Durée et absence de possibilité d'effacement et de protection suffisante – Violation de l'article 8 CEDH

Le requérant dénonçait une atteinte à son droit au respect de sa vie privée, en raison de l'ordre qui lui avait été fait de se soumettre à un prélèvement biologique destiné à un enregistrement dans le fichier national automatisé des empreintes génétiques (FNAEG) et pour lequel son refus d'obtempérer avait donné lieu à une condamnation pénale.

1) Durée de conservation – En 2010, le Conseil constitutionnel a déclaré conformes à la Constitution les dispositions législatives relatives au fichier incriminé, sous réserve « de proportionner la durée de conservation de ces données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées ». Au jour du prononcé du jugement de la Cour, cette réserve n'avait pas reçu de suite appropriée.

Selon le code de procédure pénale, la durée de conservation des profils ADN ne peut dépasser « quarante ans » s'agissant des personnes condamnées pour l'une des infractions énumérées. Il s'agit là d'un maximum qui aurait dû être aménagé par décret. Ce décret n'ayant pas vu le jour, la durée de quarante ans n'est plus un simple maximum mais devient en pratique la norme.

Ainsi, aucune différenciation n'est actuellement prévue en fonction de la nature et de la gravité de l'infraction commise. Or les situations susceptibles d'entrer dans le champ d'application légal du fichier en cause présentent une importante disparité, pouvant aller jusqu'à des faits particulièrement graves (à l'instar notamment des infractions sexuelles, du terrorisme ou encore des crimes contre l'humanité ou de la traite des êtres humains).

La présente affaire (de simples coups de parapluie donnés dans un contexte politique et syndical en direction de gendarmes qui n'ont pas même été identifiés) se distingue clairement de celles qui concernaient spécifiquement des infractions aussi graves que la criminalité organisée ou des agressions sexuelles.

2) Procédure d'effacement – L'accès à une telle procédure n'est prévu que pour les personnes soupçonnées, et non pour celles qui ont été condamnées (à l'instar du requérant). Or, aux yeux de la Cour, les personnes condamnées devraient également se voir offrir une possibilité concrète de présenter une requête en effacement des données mémorisées.

CEDH, 22 juin 2017, Affaire Aycaguer c. France, n°8806/12

---

1) Contrôle de la CNIL et d'un magistrat – Finalité – Conservation – Procédure d'effacement – Droit d'accès direct – Conciliation – 2) Liste d'infractions de l'article 706-55 du code de procédure pénale – Rapprochements opérés avec des empreintes génétiques provenant des traces et prélèvements enregistrés au fichier – Adéquation avec l'objectif d'identification et de recherche des auteurs

1) Le FNAEG relève du contrôle de la Commission nationale de l'informatique et des libertés en application des dispositions et selon les modalités prévues par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés. Selon les dispositions de l'article 706-54 du code de procédure pénale, il est en outre placé sous le contrôle d'un magistrat.

Il est constitué en vue de l'identification et de la recherche des auteurs de certaines infractions et ne centralise que les traces et empreintes concernant les mêmes infractions. L'inscription au fichier concerne, outre les personnes condamnées pour ces infractions, celles à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles les aient commises. Pour ces dernières, les empreintes prélevées dans le cadre d'une enquête ou d'une information judiciaires sont conservées dans le fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction. Une procédure d'effacement est, dans ce cas, prévue par le législateur, lorsque la conservation des empreintes n'apparaît plus nécessaire compte tenu de la finalité du fichier. Le refus du procureur de la République de procéder à cet effacement est susceptible de recours devant le juge des libertés et de la détention dont la décision peut être contestée devant le président de la chambre de l'instruction.

Enfin, toute personne bénéficie d'un droit d'accès direct auprès du responsable du fichier en application de l'article 39 de la loi Informatique et Libertés.

Dès lors, ces dispositions sont de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée.

2) Selon l'article 706-55 du code de procédure pénale, le FNAEG centralise les traces et empreintes génétiques concernant des crimes et délits précisément et limitativement énumérés. Outre les atteintes aux intérêts fondamentaux de la nation, toutes ces infractions portent atteinte à la sécurité des personnes ou des biens, incriminent des faits en permettant la commission ou ceux qui en tirent bénéfice. À l'exception de l'infraction prévue au second alinéa de l'article 322-1 du code pénal, toutes sont au moins punies de peines d'emprisonnement.

Pour l'ensemble de ces infractions, les rapprochements opérés avec des empreintes génétiques provenant des traces et prélèvements enregistrés au fichier sont aptes à contribuer à l'identification et à la recherche de leurs auteurs. Il en résulte que la liste prévue par l'article 706-55 est en adéquation avec l'objectif poursuivi par le législateur et que cet article ne soumet pas les intéressés à une rigueur qui ne serait pas nécessaire.

CC, 2010-25 QPC, 16 septembre 2010, M. Jean-Victor C., points 16, 22

Traitement des antécédents judiciaires (TAJ)

Traitements de données recueillies au cours des enquêtes préliminaires ou de flagrance, d'investigations exécutées sur commission rogatoire – Crime, délit ou contraventions de cinquième classe – Contrôle par le procureur de la République et encadrement de l'effacement – Données particulières sensibles – Reconnaissance faciale –Absence de durée maximum de conservation – Personnes privées de leur droit d'effacement – Atteinte disproportionnée au droit au respect de la vie privée

En application de l'article 230-6 du code de procédure pénale, les services de la police nationale et de la gendarmerie nationale peuvent mettre en œuvre des traitements automatisés de données à caractère personnel recueillies au cours des enquêtes préliminaires ou de flagrance ou au cours des investigations exécutées sur commission rogatoire et concernant tout crime ou délit et certaines contraventions de la cinquième classe. En application du premier alinéa de l'article 230-7 du même code, ces traitements peuvent contenir des informations sur les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission de ces infractions.

En application du premier alinéa de l'article 230-8 du code de procédure pénale, ces traitements sont opérés sous le contrôle du procureur de la République territorialement compétent. En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien. Le procureur de la République peut également ordonner l'effacement des données personnelles en cas

de décision de non-lieu ou de classement sans suite. En application de l'article 230-9 du code de procédure pénale, un magistrat est chargé de suivre la mise en œuvre et la mise à jour de ces traitements. Il dispose des mêmes pouvoirs d'effacement que le procureur de la République. Il résulte d'une jurisprudence constante qu'aucune personne mise en cause autre que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite ne peut obtenir, sur le fondement des dispositions contestées, l'effacement des données qui la concernent. En autorisant la création de traitements de données à caractère personnel recensant des antécédents judiciaires et l'accès à ces traitements par des autorités investies par la loi d'attributions de police judiciaire et par certains personnels investis de missions de police administrative, le législateur a entendu leur confier un outil d'aide à l'enquête judiciaire et à certaines enquêtes administratives. Il a ainsi poursuivi les objectifs de valeur constitutionnelle de recherche des auteurs d'infractions et de prévention des atteintes à l'ordre public.

Toutefois, en premier lieu, en prévoyant que les fichiers d'antécédents judiciaires peuvent contenir les informations recueillies au cours d'une enquête ou d'une instruction concernant une personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait pu participer à la commission de certaines infractions, le législateur a permis que figurent dans ce fichier des données particulièrement sensibles. Ainsi, l'article R. 40-26 du code de procédure pénale prévoit que peuvent être enregistrés les éléments d'état civil, la profession ou la situation familiale de la personne et une photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale. En deuxième lieu, les fichiers d'antécédents judiciaires sont susceptibles de porter sur un grand nombre de personnes dans la mesure où y figurent des informations concernant toutes les personnes mises en cause pour un crime, un délit et certaines contraventions de la cinquième classe. En troisième lieu, le législateur n'a pas fixé la durée maximum de conservation des informations enregistrées dans un fichier d'antécédents judiciaires. Ainsi, l'article R. 40-27 du code de procédure pénale prévoit qu'elles sont conservées pendant une durée comprise entre cinq ans et quarante ans selon l'âge de l'individu et la nature de l'infraction. En dernier lieu, ces informations peuvent être consultées non seulement aux fins de constatation des infractions à la loi pénale, de rassemblement des preuves de ces infractions et de recherche de leurs auteurs, mais également à d'autres fins de police administrative. Dès lors, en privant les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le fichier des antécédents judiciaires, le premier alinéa de l'article 230-8 du code de procédure pénale porte une atteinte disproportionnée au droit au respect de la vie privée.

CC, 2017-670 QPC, 27 octobre 2017, M. Mikhail P., points 8-14

Casier judiciaire – Irresponsabilité pénale – Conditions de mention au bulletin n°1

Lorsqu'aucune mesure de sûreté n'a été prononcée par la juridiction à l'encontre d'une personne déclarée pénalement irresponsable, la déclaration d'irresponsabilité pénale n'est pas une information susceptible d'être légalement nécessaire à l'appréciation de la responsabilité pénale de la personne éventuellement poursuivie à l'occasion de procédures ultérieures. Dès lors, eu égard aux finalités du casier judiciaire, elle ne saurait, sans porter une atteinte non nécessaire à la protection de la vie privée qu'implique l'article 2 de la Déclaration de 1789, être mentionnée au bulletin n° 1 du casier judiciaire que lorsque des mesures de sûreté ont été prononcées et tant que ces interdictions n'ont pas cessé leurs effets. Réserve.

CC, 2008-562 DC, 21 février 2008, Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental, points 28-31

Consultation - Agents habilités - Recours à la technique de reconnaissance faciale - Défaut d'autorisation préalable d'un magistrat - Validité - Détermination – Portée

Les articles 230-6 et suivants et R. 40-26 et suivants du code de procédure pénale, qui permettent à des enquêteurs de recourir à la technique de reconnaissance faciale sans autorisation préalable d'un magistrat sont conformes à l'article 8 de la Convention européenne des droits de l'homme, tel qu'interprété par la Cour européenne des droits de l'homme. En effet, l'ingérence dans l'exercice du droit au respect de la vie privée résultant du recours à cette technique est justifiée par l'objectif légitime de poursuite des auteurs d'infractions, et proportionnée au but recherché, dès lors que, d'une part, seules les données personnelles des personnes déclarées coupables des infractions les plus graves peuvent être contenues dans le fichier dont dépend l'outil utilisé pour la reconnaissance faciale, d'autre part, le juge, saisi par voie de requête en nullité, peut vérifier que seuls des agents spécialement habilités à cette fin ont accédé à ce fichier

Cass, crim., 9 octobre 2024, n° 24-80.871

Refus d'agrément individuel pour effectuer des visites de sûreté portuaire (art. L. 5332-8 du code des transports) – Fichier TAJ ayant été consulté par une personne non habilitée – Incidence sur la régularité de la procédure – Absence

Il résulte du 1° du I de l'article R. 40-29 du code de procédure pénale (CPP) que les agents habilités selon les modalités prévues au 1° du I de l'article R. 40-28 peuvent consulter les données à caractère personnel figurant dans le traitement des antécédents judiciaires (TAJ), qui se rapportent à des procédures judiciaires closes ou en cours, sans autorisation du ministère public, dans le cadre des enquêtes prévues à l'article L. 114-1 du code de la sécurité intérieure (CSI), applicable en particulier à l'instruction des demandes d'agrément des personnes chargées des visites de sûreté portuaire.

Dès lors que l'article L. 5332-8 du code des transports prévoit la possibilité que certains traitements automatisés de données à caractère personnel soient consultés au cours de l'enquête conduite par l'administration dans le cadre de ses pouvoirs de police, préalablement à la délivrance d'un agrément individuel, la circonstance que l'agent ayant procédé à cette consultation n'aurait pas été, en application des articles R. 40-23, R. 40-28 et du 1° du I de l'article R. 40-29 du CPP, individuellement désigné et régulièrement habilité à cette fin, si elle est susceptible de donner lieu aux procédures de contrôle de l'accès à ces traitements, n'est pas, par elle-même, de nature à entacher d'irrégularité la décision prise sur la demande d'agrément.

CE, 5ème – 6ème chambres réunies, 22 juin 2022, M. B... A..., n°452969, T., points 3, 5

Proportionnalité d'un dispositif de reconnaissance faciale déployé à des fins policières – Conditions

Le traitement de données à caractère personnel, dans lequel est enregistrée une photographie permettant le recours à un dispositif de reconnaissance faciale, ne constitue pas un dispositif disproportionné dès lors qu'il comporte des garanties appropriées permettant d'assurer que :

- la collecte des données biométriques relatives aux personnes mises en cause ne peut avoir lieu que dans les conditions prévues aux articles R. 40-24 et R. 40-25 du code de procédure pénale ;
- le traitement est opéré sous le contrôle du procureur de la République qui, d'office ou à la demande de la personne concernée, peut ordonner l'effacement ou la rectification des données biométriques ;
- le dispositif de reconnaissance faciale ne peut être mobilisé par les services compétents qu'en cas de nécessité absolue et sous la responsabilité des agents qui l'utilisent ; seuls certains

magistrats et agents étant autorisés par décret à accéder aux données biométriques et ces accès étant soumis à des obligations de traçabilité ;
- la mise en œuvre du traitement fait l'objet d'un suivi par un magistrat désigné par le ministre de la justice et est soumise au contrôle de la CNIL ;
- le responsable de traitement prend les mesures de sécurité appropriées au regard de la sensibilité des données en cause.

CE, 10ème chambre, 26 avril 2022, La Quadrature du Net, n°442364, Inédit., points 6-7

Décisions en matière d'effacement ou de rectification prises par le procureur de la République ou par le magistrat désigné à cet effet (art. 230-8 et 230-9 du code de procédure pénale) – Nature – Mesures d'administration judiciaire – Absence – Actes de gestion administrative du fichier – Existence – Conséquence – Décisions susceptibles de recours pour excès de pouvoir devant le juge administratif

Si les données nominatives figurant dans le traitement des antécédents judiciaires (TAJ) portent sur des informations recueillies au cours d'enquêtes préliminaires ou de flagrance ou d'investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que certaines contraventions de cinquième classe, les décisions en matière d'effacement ou de rectification prises par le procureur de la République ou par le magistrat désigné à cet effet, qui ont pour objet la tenue à jour de ce fichier et sont détachables d'une procédure judiciaire, constituent non pas des mesures d'administration judiciaire, mais des actes de gestion administrative du fichier. Elles peuvent, par suite, faire l'objet d'un recours pour excès de pouvoir devant le juge administratif.

CE, 10ème/9ème SSR, 11 avril 2014, Ligue des droits de l'homme, n° 360759, T., point 19

Autres traitements judiciaires

Traitement des données figurant dans une notice rouge publiée par Interpol – Directive 2016/680 – Condition de licéité – Limite – Existence d'une décision judiciaire définitive prise dans un État partie à l'accord de Schengen ou un État membre établissant l'application du principe ne bis in idem pour les faits visés par ladite notice

Les dispositions de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016 lues à la lumière de l'article 54 de la convention d'application de l'accord Schengen du 19 juin 1990, et de l'article 50 de la Charte des droits fondamentaux, doivent être interprétées en ce sens qu'elles ne s'opposent pas au traitement des données à caractère personnel figurant dans une notice rouge émise par l'Organisation internationale de police criminelle (Interpol), tant qu'il n'a pas été établi, par la voie d'une décision judiciaire définitive prise dans un État partie à l'accord Schengen du 14 juin 1985, ou dans un État membre, que le principe ne bis in idem s'applique s'agissant des faits sur lesquels cette notice est fondée, pour autant qu'un tel traitement satisfait aux conditions prévues par cette directive, notamment en ce qu'il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, au sens de l'article 8, paragraphe 1, de ladite directive.

CJUE, grande chambre, 12 mai 2021, Bundesrepublik Deutschland, C-505/19

Logiciels de rapprochement judiciaire – Traitement général de données – Exclusion – Contrôle du procureur de la République ou de la juridiction d'instruction – Réserve – Enregistrement de données – Conservation prolongée à l'initiative de l'enquêteur – Censure

L'article 14 de la loi d'orientation et de programmation pour la performance de la sécurité intérieure insère les articles 230-20 et suivants dans le code de procédure pénale relatifs aux logiciels de rapprochement judiciaire. L'utilisation de ces logiciels permet la mise en œuvre de traitements de données à caractère personnel recueillies à l'occasion d'enquêtes judiciaires ouvertes pour toutes catégories d'infractions quelle que soit leur gravité. Il appartient au législateur d'adopter les garanties de nature à assurer la conciliation entre les objectifs de sauvegarde de l'ordre public et les libertés constitutionnellement protégées en tenant compte de la généralité de l'application de ces logiciels.

En premier lieu, les dispositions des articles 230-20 et suivants n'ont pas pour objet et ne sauraient avoir pour effet de permettre la mise en œuvre d'un traitement général des données recueillies à l'occasion des diverses enquêtes de police judiciaire. L'article 230-23 prévoit que, sans préjudice des pouvoirs de contrôle attribués à la Commission nationale de l'informatique et des libertés, le traitement de données à caractère personnel au moyen des logiciels de rapprochement judiciaire est opéré sous le contrôle du procureur de la République ou de la juridiction d'instruction compétent. Ainsi, ces logiciels ne pourront conduire qu'à la mise en œuvre, autorisée par ces autorités judiciaires, de traitements de données à caractère personnel particuliers, dans le cadre d'une enquête ou d'une procédure déterminée portant sur une série de faits et pour les seuls besoins de ces investigations. Réserve.

En second lieu, eu égard à la possibilité ouverte par ces dispositions d'un enregistrement de données même liées à des faits de faible gravité, la conservation de ces données ne saurait être prolongée à l'initiative de l'enquêteur au-delà de trois ans après leur enregistrement. Censure.

CC, 2011-625 DC, 10 mars 2011, Loi d'orientation et de programmation pour la performance de la sécurité intérieure, points 71-72

Fichier judiciaire national automatisé des auteurs d'infractions sexuelles – 1) Inscription – Mesure de police – 2) Garanties – Gravité des infractions – Conciliation n'étant pas manifestement déséquilibrée – Motif de consultation – Conformité – 3) Nécessité de rechercher le relèvement éducatif et moral des mineurs – Conformité – 4) Obligation de justifier son adresse tous les six mois en se présentant personnellement auprès d'un service de police ou de gendarmerie – Gravité de la condamnation – Critère objectif et rationnel – Mesure de police

1) L'inscription d'une personne dans ce fichier ne constitue pas une sanction mais une mesure de police qui vise à prévenir le renouvellement de ces infractions et de faciliter l'identification de leurs auteurs. Les auteurs des saisines ne sauraient dès lors utilement soutenir qu'elle méconnaîtrait le principe de nécessité des peines qui résulte de l'article 8 de la Déclaration de 1789.

2) Eu égard, d'une part, aux garanties apportées par les conditions d'utilisation et de consultation du fichier judiciaire automatisé des auteurs d'infractions sexuelles et par l'attribution à l'autorité judiciaire du pouvoir d'inscription et de retrait des données nominatives, d'autre part, à la gravité des infractions justifiant l'inscription des données nominatives dans le fichier et au taux de récidive qui caractérise ce type d'infractions, les dispositions de l'article 48 de la loi portant adaptation de la justice à l'évolution de la criminalité sont de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée. De même, en raison du motif qu'elles assignent aux consultations du fichier par des autorités administratives, et compte tenu des restrictions et prescriptions dont elles les assortissent, cet article ne porte une atteinte excessive ni au respect de la vie privée ni aux exigences de l'article 9 de la Déclaration de 1789.

3) Les adaptations apportées, en faveur des mineurs délinquants, au régime du fichier judiciaire automatisé des auteurs d'infractions sexuelles sont inspirées par la nécessité de rechercher leur relèvement éducatif et moral. Elles ne sont pas contraires au principe fondamental reconnu par les lois de la République en matière de droit pénal des mineurs.

4) L'article 706-53-5 nouveau du code de procédure pénale impose à la personne inscrite dans le fichier des auteurs d'infractions sexuelles, lorsqu'elle a été définitivement condamnée pour un crime

ou un délit puni de dix ans d'emprisonnement, de justifier de son adresse tous les six mois en se présentant à cette fin auprès d'un service de police ou de gendarmerie [...].

La gravité de la condamnation encourue, qui détermine le champ d'application de l'obligation, de se présenter personnellement constitue un critère objectif et rationnel de distinction en relation directe avec la finalité du fichier.

L'obligation faite aux personnes inscrites de faire connaître périodiquement l'adresse de leur domicile ou de leur résidence ne constitue pas une sanction, mais une mesure de police destinée à prévenir le renouvellement d'infractions et à faciliter l'identification de leurs auteurs. L'objet même du fichier rend nécessaire la vérification continue de l'adresse de ces personnes. La charge qui leur est imposée dans le but de permettre cette vérification ne constitue pas une rigueur qui ne serait pas nécessaire au sens de l'article 9 de la Déclaration de 1789.

CC, 2004-492 DC, 2 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité, points 74, 87-88, 92-95, 89-91

Impossibilité d'interconnecter des traitements portant sur le même type de données mais poursuivant des finalités différentes

Le Conseil d'État, saisi d'un projet de décret relatif au système national d'information Schengen de deuxième génération (N-SIS II), lui a donné un avis favorable, sous réserve d'observations relatives à l'enregistrement des empreintes digitales.

L'article R. 231-9 du code de la sécurité intérieure, dans sa version résultant du projet, disposait que les empreintes digitales des personnes signalées pourraient désormais figurer parmi les données enregistrées dans le traitement N-SIS II. Cet enregistrement est prévu à l'article 20 du règlement (CE) n° 1987/2006 du 20 décembre 2006 et de la décision 2007/533/JAI du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), d'application immédiate.

D'après les informations fournies au Conseil d'État, les empreintes devaient provenir pour la plupart du fichier automatisé des empreintes digitales (FAED). Si une telle utilisation de ces données n'est pas contraire aux finalités du FAED, telles qu'elles sont mentionnées au décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, ce texte ne prévoit pas que les empreintes peuvent être transmises aux services chargés du traitement N-SIS II. Le Conseil d'État (section de l'intérieur) attire donc l'attention du Gouvernement sur la nécessité de modifier ce décret dans les meilleurs délais.

Le Conseil d'État relève en revanche, comme l'avait également signalé la Commission nationale de l'informatique et des libertés, que les empreintes digitales enregistrées dans le traitement N-SIS II ne pourront en aucun cas provenir du traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité dénommé « titres électroniques sécurisés » (TES). En effet, ce traitement a pour seul objet de procéder à l'établissement, à la délivrance, au renouvellement et à l'invalidation des titres en question ainsi que de prévenir et détecter leur falsification et contrefaçon.

CE, Section de l'intérieur, 6 décembre 2016, Avis n° 392308, Projet de décret relatif au système national d'information Schengen de deuxième génération

---

LAPI

1) Utilisation en matière de vidéoprotection – Licéité – Conditions – 2) Finalité de réponse aux réquisition judiciaires – Licéité – Absence.

1) Si les articles L. 233-1 et L. 233-1-1 du code de la sécurité intérieure autorisent les seuls services des douanes, de police et de gendarmerie nationales à mettre en œuvre les dispositifs de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants pour les finalités qu'ils prévoient, ils n'ont pas pour effet d'interdire aux autorités compétentes de mettre en œuvre, sur le fondement de l'article L. 251-2 de ce même code, des dispositifs de lecture automatisée des plaques d'immatriculation des véhicules. Toutefois, ces autorités ne peuvent le faire que pour l'une des finalités énumérées par cet article et dans le respect du titre V du livre II de ce même code.

2) La mise en œuvre d'un dispositif de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants aux seules fins de répondre aux éventuelles réquisitions des forces de l'ordre pour l'exercice de leurs missions de police judiciaire ne constitue pas une finalité déterminée et n'est pas au nombre des finalités justifiant la mise en place d'un tel dispositif visées par l'article L.251-2 du CSI.

CE, 10ème–9ème chambres réunies, 30 avril 2024, °472864, Inédit, points 4 et 5

---

1) Finalités légales de la vidéoprotection (art. L. 251-2 du CSI) – Exclusion – Mise à la disposition de la gendarmerie nationale des données collectées – 2) Dispositifs de contrôle automatisé des données signalétiques des véhicules (art. L. 233-1 du CSI) – Gestionnaires autorisés – Services des douanes, de police et de gendarmerie nationales uniquement

1) L'article L. 251-2 du code de la sécurité intérieure (CSI) liste les finalités pour lesquelles la transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes. Mettre les données collectées à la disposition de la gendarmerie nationale pour l'exercice de ses missions de police judiciaire, qui n'est pas aux nombres des finalités visées par cet article, ne constitue pas, pour un dispositif de transmission et d'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection, une finalité légitime.

2) L'article L. 233-1 du CSI autorise les seuls services des douanes, de police et de gendarmerie nationales à mettre en œuvre les dispositifs de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants pour les finalités qu'il prévoit. Par suite, une commune ne saurait mettre en œuvre un tel dispositif, alors mêmes que les données collectées seraient destinées à être mises à la disposition de la gendarmerie nationale à des fins d'aide à l'identification des auteurs d'infractions.

CE, 10ème–9ème chambres réunies, 27 juin 2016, Commune de Gujan-Mestras, n°385091, Rec., points 3-4, 6

Conciliation assurée en l'espèce entre d'une part, le respect de la vie privée des personnes et la liberté d'aller et venir et, d'autre part, la répression des infractions aux règles édictées dans la ZFE pour réduire la pollution ou celle des comportements visant à éluder le paiement de la taxe

Développement des contrôles automatisés à grande échelle des véhicules à des fins de réduction des pollutions et de la congestion du trafic routier

Le projet de loi d'orientation des mobilités, dans la version dont le Conseil d'État a été saisi, prévoyait la mise en place de dispositifs de contrôle automatisé des données signalétiques des véhicules (dit « LAPI », c'est-à-dire de lecture automatique des plaques d'immatriculation) dans trois cas :

- le premier était destiné à contrôler les voies réservées à certaines catégories de véhicules, parmi lesquelles les véhicules transportant un nombre minimal d'occupants et les véhicules à très faibles émissions ;
- le deuxième avait pour objet d'assurer le respect des restrictions de circulation dans les « zones à faibles émissions » (ZFE) dont la mise en place sera obligatoire pour les collectivités sur le territoire desquelles les niveaux de pollution sont régulièrement dépassés ;
- le troisième permettait de vérifier l'acquittement, par les véhicules entrant dans un périmètre urbain défini par une autorité organisatrice de la mobilité, de la taxe appelée « tarif de congestion » instituée par cette autorité à titre de « péage urbain » afin de réduire la circulation automobile et diminuer la pollution atmosphérique.

Le recueil systématique des photographies des véhicules et par conséquent, tant de leurs plaques d'immatriculation que de leurs conducteurs et passagers, susceptibles ainsi d'être identifiés, est de nature à permettre la saisie sur une grande échelle de données personnelles relatives au déplacement des individus concernés.

Le Conseil d'État a cependant admis la possibilité, au regard des principes constitutionnels, de mettre en place de tels dispositifs de recueil de données potentiellement identifiantes en raison des motifs d'intérêt général poursuivis en termes de politique des transports et de l'environnement. La création de voies réservées comme les restrictions d'accès au profit de certains véhicules, notamment les véhicules à très faibles émissions, sont indissociables de la mise en place d'un contrôle automatisé systématique des véhicules circulant sur ces voies ou dans ces zones, seul à même d'assurer le respect de ces dispositions. Il en va de même pour le contrôle automatisé systématique des véhicules assujettis au tarif de congestion, indispensable pour vérifier le respect de l'obligation faite aux assujettis à cette imposition. En outre, s'agissant des ZFE, le projet de loi, pour préserver les libertés auxquelles l'extension de ce dispositif est susceptible de porter atteinte, encadrait strictement le déploiement et la mise en œuvre du contrôle en limitant l'étendue et les points où il est effectué, le dispositif étant soumis à autorisation préfectorale.

Pour le péage urbain, si le projet de loi ne limitait pas le nombre des points de contrôle ni ne comportait de contraintes s'agissant de leur emplacement contrairement à ce qui était prévu pour les voies réservées et les zones à faibles émissions, il prévoyait plusieurs garanties : suppression des données dès que la vérification a permis de constater l'acquittement du tarif, consultation du système d'immatriculation des véhicules aux fins d'identification du titulaire du certificat d'immatriculation du véhicule pour les seuls véhicules en infraction, conservation des données collectées subordonnée à un masquage destiné à empêcher l'identification des occupants et limitée à huit jours.

Le Conseil d'État a considéré que les limitations et précautions dont étaient ainsi assorties ces procédures de contrôle sont de nature à assurer la conciliation qu'il incombe au législateur d'effectuer entre, d'une part, le respect de la vie privée des personnes et la liberté d'aller et venir et, d'autre part, la répression des infractions aux règles édictées dans la ZFE pour réduire la pollution ou celle des comportements visant à éluder le paiement de la taxe.

CE, Assemblée générale (section des travaux publics, section sociale), 15 novembre 2018, Avis n° 395539, Projet de loi d'orientation des mobilités

---

LAPI mis en œuvre par des personnes privés - Contrôle des entrées et sorties des véhicules d'un village de vacances – Application du principe de minimisation des données - Conditions

Dans le cadre de la mise en œuvre de dispositifs de lecture automatisée de plaques d'immatriculation (LAPI), le respect du principe de minimisation impose une vigilance particulière quant au respect de la vie privée des passagers des véhicules, des passants et des riverains et proscrit la prise de vue d'individus, y compris les occupants des véhicules.

En l'espèce, la mise en oeuvre d'un tel dispositif à certaines entrées et sorties d'un village de vacances pour des finalités de sécurité des biens et des personnes (notamment dans le cadre d'évacuations d'urgence ou de la vérification d'absence d'entrée irrégulière sur le parc) apparaissait proportionnée, mais la captation de données à caractères personnel autres que les plaques minéralogiques était excessive. En particulier, la capture de l'identité des occupants du véhicule était disproportionnée au regard de la finalité du traitement.

CNIL, P, 27 mai 2024, mise en demeure, Société X, décision n° MED 2024-069, non publié

Caméras mobiles

Drones – Interdiction législative de procéder à de la reconnaissance faciale sur les images – Portée

En application du deuxième alinéa de l'article L. 242-4 du code de la sécurité intérieure, les dispositifs aéroportés ne peuvent procéder à la captation du son, ni comporter de traitements automatisés de reconnaissance faciale. Ces dispositifs aéroportés ne peuvent procéder à aucun rapprochement, interconnexion ou mise en relation automatisé avec d'autres traitements de données à caractère personnel. Toutefois, ces dispositions ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient pas placés sur ces dispositifs aéroportés.

CC, 2021-834 DC, 20 janvier 2022, Loi relative à la responsabilité pénale et à la sécurité intérieure, point 30

PARAFE

1) Élargissement des nationalités éligibles au dispositif – Modalités d'information des personnes par le responsable de traitement – 2) Suppression dans le projet de décret de la mention des traitements mis en relation avec PARAFE – Obligation de mention – Absence – Bonne pratique

1) Le projet de décret étend la liste des nationalités éligibles au dispositif PARAFE aux ressortissants de cinq États tiers à l'entrée et à l'ensemble des ressortissants de pays tiers, sans condition de nationalité, à la sortie.

La CNIL estime que ces évolutions apparaissent légitimes au regard du besoin opérationnel invoqué. Elles entrainent néanmoins une augmentation du volume de données traitées et de personnes concernées par le traitement. Dès lors, une attention particulière devra être portée aux modalités concrètes de mise en œuvre du traitement, s'agissant notamment de l'information des personnes.

La CNIL souligne que l'obligation d'informer les personnes pèse sur le responsable de traitement. Outre les mesures déjà prévues (éléments de communication comportant des mentions obligatoires, tenue d'audits…), des mesures supplémentaires devraient être déployées pour garantir que les gestionnaires fournissent, au moment de la collecte, l'ensemble des informations énumérées à l'article 13 du RGPD. Pour assurer l'effectivité des droits des personnes, l'information sur le traitement doit, en outre, être complétée d'éléments relatifs :

- au caractère facultatif, prévu par l'article R. 232-6 du CSI, du recours au sas PARAFE pour le franchissement des frontières ; et
- le cas échéant, à l'articulation de PARAFE avec d'autres dispositifs de facilitation des contrôles

Enfin, l'information fournie à la frontière et disponible sur les sites web précités devrait être traduite en plusieurs langues. La CNIL considère qu'elle devrait être traduite a minima en anglais et accompagnée de pictogrammes.

2) L'article R. 232-8 du CSI prévoit que les données collectées sont « traitées à la seule fin de permettre l'authentification biométrique du voyageur et la consultation prévue à l'article R. 232-9, permettant le contrôle aux frontières ». Autrement dit, les données alphanumériques collectées sont utilisées pour consulter, dans le cadre des contrôles prévus par le règlement (UE) 2016/399 : le fichier des personnes recherchées, le système d'information Schengen et le fichier des documents de voyage volés et perdus d'Interpol. Ces traitements font alors l'objet d'une mise en relation avec PARAFE.

Le projet de décret supprime la mention des traitements consultés et prévoit, en conséquence, que les données sont traitées non plus pour la consultation de ces derniers, mais pour « la collecte des données nécessaires aux contrôles aux frontières ».

La CNIL ne remet pas en cause l'absence d'obligation de mentionner, au sein du projet de décret, les mises en relation. Elle rappelle néanmoins que, dans certains cas particuliers, leur mention peut constituer une bonne pratique, notamment lorsque les finalités principales du traitement sont étroitement liées à quelques mises en relation particulières. La transparence vis-à-vis du public quant aux conditions de mise en œuvre de ces opérations participe également de l'équilibre entre l'objectif poursuivi par les traitements en cause et le respect de la vie privée des personnes concernées (sur ce point, v. CNIL, SP, 27 mai 2021, avis sur projet de décret, LRPGN, n° 2021-061, publié). Au regard de ces éléments, la CNIL recommande de maintenir, au niveau du décret, la mention des mises en relation. À défaut, elle recommande vivement au ministère de décrire sur son site web l'ensemble des mises en relation réalisées avec d'autres traitements.

CNIL, SP, Avis sur projet de décret, PARAFE, n°2023-045, points 6-9, 12-14, 16, 19, 24-27

PASP

PNR

Conditions de compatibilité d'un accord de transfert de données avec la Charte des droits fondamentaux

Le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers permet le transfert systématique et continu des données PNR de l'ensemble des passagers aériens à une autorité canadienne en vue de leur utilisation et de leur conservation, ainsi que de leur éventuel transfert ultérieur à d'autres autorités et d'autres pays tiers, dans le but de lutter contre le terrorisme et les formes graves de criminalité transnationale. À cet effet, l'accord envisagé prévoit, entre autres, une durée de stockage des données de cinq ans ainsi que des exigences en matière de sécurité et d'intégrité des données PNR, un masquage immédiat des données sensibles, des droits d'accès aux données, de rectification et d'effacement et la possibilité d'introduire des recours administratifs ou judiciaires.

La Cour juge que certaines stipulations du projet d'accord envisagé sont incompatibles avec les droits fondamentaux, à moins que celui-ci ne soit révisé pour mieux encadrer et préciser les ingérences. Cet

accord doit, pour être compatible avec les articles 7 et 8 ainsi qu'avec l'article 52, paragraphe 1, de la Charte des droits fondamentaux :

a) déterminer de manière claire et précise les données des dossiers passagers à transférer depuis l'Union européenne vers le Canada ;

b) prévoir que les modèles et les critères utilisés dans le cadre du traitement automatisé des données des dossiers passagers seront spécifiques et fiables ainsi que non discriminatoires ; prévoir que les bases de données utilisées seront limitées à celles exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave ;

c) soumettre, hormis dans le cadre des vérifications relatives aux modèles et aux critères préétablis sur lesquels sont fondés les traitements automatisés des données des dossiers passagers, l'utilisation de ces données par l'autorité canadienne compétente pendant le séjour des passagers aériens au Canada et après leur départ de ce pays, de même que toute communication desdites données à d'autres autorités, à des conditions matérielles et procédurales fondées sur des critères objectifs ; subordonner cette utilisation et cette communication, sauf cas d'urgence dûment justifiés, à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, dont la décision autorisant l'utilisation intervient à la suite d'une demande motivée de ces autorités, notamment dans le cadre de procédures de prévention, de détection ou de poursuites pénales ;

d) limiter la conservation des données des dossiers passagers après le départ des passagers aériens à celles des passagers à l'égard desquels il existe des éléments objectifs permettant de considérer qu'ils pourraient présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave ;

e) soumettre la communication des données des dossiers passagers par l'autorité canadienne compétente aux autorités publiques d'un pays tiers à la condition qu'il existe soit un accord entre l'Union européenne et ce pays tiers équivalent à l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, soit une décision de la Commission européenne, au titre de l'article 25, paragraphe 6, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, couvrant les autorités vers lesquelles la communication des données des dossiers passagers est envisagée ;

f) prévoir un droit à l'information individuelle des passagers aériens en cas d'utilisation des données des dossiers passagers les concernant pendant leur séjour au Canada et après leur départ de ce pays ainsi qu'en cas de divulgation de ces données par l'autorité canadienne compétente à d'autres autorités ou à des particuliers, et

g) garantir que la surveillance des règles prévues par l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, relatives à la protection des passagers aériens à l'égard du traitement des données des dossiers passagers les concernant, est assurée par une autorité de contrôle indépendante.

CJUE, grande chambre, 26 juillet 2017, Avis sur l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des passagers, Avis 1/15

Transfert, traitement et conservation des données PNR prévus par la Directive (UE) 2016/681 – 1) Conditions de mise en œuvre de nature à assurer le respect de la Charte des droits de l'Union européenne – 2) Traitement à d'autres fins que la lutte contre les infractions terroristes et les formes graves de criminalité – Conditions de licéité – 3) Autorité nationale compétente pour vérifier les conditions de mise en œuvre – 4) Durée de conservation – 5) Extension du dispositif à d'autres modes de transport à l'intérieur de l'Union

1) Le transfert, le traitement et la conservation des données PNR (transport aérien) prévus par la directive (UE) 2016/681 (directive PNR) peuvent être considérés, au regard des exigences des articles 7, 8 et 21 ainsi que de l'article 52, paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne, comme étant limités au strict nécessaire aux fins de la lutte contre les infractions terroristes et les formes graves de criminalité, à condition que les pouvoirs prévus par ladite directive fassent l'objet d'une interprétation restrictive. La Cour précise notamment que :

- le système établi par la directive PNR ne doit couvrir que les informations clairement identifiables et circonscrites dans les rubriques figurant dans l'annexe I de celle-ci, lesquelles sont en rapport avec le vol effectué et avec le passager concerné, ce qui implique, pour certaines rubriques figurant dans cette annexe, que seuls les renseignements visés expressément sont couverts,
- l'application du système établi par la directive PNR doit être limitée aux infractions terroristes et aux seules formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers. S'agissant de ces formes, l'application de ce système ne saurait être étendue à des infractions qui, bien qu'elles remplissent le critère prévu par cette directive relatif au seuil de gravité et qu'elles soient notamment visées à l'annexe II de celle-ci, relèvent de la criminalité ordinaire compte tenu des spécificités du système pénal national,
- l'éventuelle extension de l'application de la directive PNR à tout ou partie des vols intra-UE, qu'un État membre peut décider en faisant usage de la faculté prévue par cette directive, doit être limitée au strict nécessaire. À cet effet, elle doit pouvoir faire l'objet d'un contrôle effectif par une juridiction ou par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant. À cet égard, la Cour précise que :
    - dans la seule situation où ledit État membre constate qu'il fait face à une menace terroriste qui s'avère réelle et actuelle ou prévisible, l'application de cette directive à tous les vols intra-UE en provenance ou à destination dudit État membre, pour une durée limitée au strict nécessaire, mais renouvelable, n'excède pas les limites du strict nécessaire,
    - en l'absence d'une telle menace terroriste, l'application de ladite directive ne saurait s'étendre à l'ensemble des vols intra-UE, mais doit être limitée aux vols intra-UE relatifs notamment à certaines liaisons aériennes ou à des schémas de voyage ou encore à certains aéroports pour lesquels il existe des indications de nature à justifier cette application.
    - aux fins de l'évaluation préalable des données PNR, qui a pour objectif d'identifier les personnes pour lesquelles est requis un examen plus approfondi avant leur arrivée ou leur départ et qui est, dans un premier temps, effectuée au moyen de traitements automatisés, la Cour considère à la lumière de la Charte des droit fondamentaux de l'UE que l'unité d'information passager (UIP) ne peut, d'une part, confronter ces données qu'aux seules bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement. Ces bases de données doivent être non discriminatoires et exploitées, par les autorités compétentes, en rapport avec la lutte contre des infractions terroristes et des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers. S'agissant, d'autre part, de l'évaluation préalable au regard de critères préétablis, l'UIP ne saurait utiliser des technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage (machine learning), susceptibles de modifier, sans intervention et contrôle humains, le processus d'évaluation et, en particulier, les critères d'évaluation sur lesquels se fonde le résultat de l'application de ce processus ainsi que la pondération de ces critères. Lesdits critères doivent être déterminés de manière à ce que leur application cible, spécifiquement, les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou à des formes graves de criminalité et à tenir compte tant des éléments « à charge » que des éléments « à décharge », tout en ne donnant pas lieu à des discriminations directes ou indirectes.

Compte tenu du taux d'erreur inhérent à de tels traitements automatisés des données PNR et du nombre assez conséquent de résultats « faux positifs », ayant été obtenus à la suite de leur application au cours des années 2018 et 2019, l'aptitude du système établi par la directive PNR à réaliser les objectifs poursuivis dépend essentiellement du bon fonctionnement de la vérification des résultats positifs, obtenus au titre de ces traitements, que l'UIP effectue, dans un deuxième temps, par des moyens non automatisés. À cet égard, les États membres doivent prévoir des règles claires et précises de nature à guider et à encadrer l'analyse effectuée par les agents de l'UIP. Dans ce contexte, la Cour souligne que les autorités compétentes doivent s'assurer que l'intéressé peut comprendre le fonctionnement des critères d'évaluation préétablis et des programmes appliquant ces critères, de manière à ce qu'il puisse décider, en pleine connaissance de cause, s'il exerce ou non son droit à un recours juridictionnel. De même, dans le cadre d'un tel recours, le juge chargé du contrôle de la légalité de la décision adoptée par les autorités compétentes ainsi que, hormis les cas de menaces pour la sûreté de l'État, l'intéressé lui-même doivent pouvoir prendre connaissance tant de l'ensemble des motifs que des éléments de preuve sur la base desquels cette décision a été prise, y compris des critères d'évaluation préétablis et du fonctionnement des programmes appliquant ces critères.

La communication et l'évaluation postérieures des données PNR, c'est-à-dire après l'arrivée ou le départ de la personne concernée, ne peuvent être effectuées que sur la base de circonstances nouvelles et d'éléments objectifs qui soit sont de nature à fonder un soupçon raisonnable d'implication de cette personne dans des formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers, soit permettent de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre des infractions terroristes présentant un tel lien. La communication des données PNR aux fins d'une telle évaluation postérieure doit, en principe, sauf en cas d'urgence dûment justifiée, être subordonnée à un contrôle préalable effectué soit par une juridiction soit par une autorité administrative indépendante, sur demande motivée des autorités compétentes, et ce indépendamment du point de savoir si cette demande a été introduite avant ou après l'expiration du délai de six mois suivant le transfert de ces données à l'UIP.

2) La directive (UE) 2016/681 s'oppose à une législation nationale qui autorise le traitement de données PNR à d'autres fins que la lutte contre les infractions terroristes et les formes graves de criminalité. Ainsi, une législation nationale admettant de surcroît, comme finalité du traitement des données PNR, le suivi des activités visées par les services de renseignement et de sécurité est susceptible de méconnaître le caractère exhaustif des objectifs énumérés par ladite directive. De même, le système établi par la directive PNR ne peut être prévu aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration clandestine. Il s'ensuit également que les données PNR ne sauraient être conservées dans une base de données unique pouvant être consultée aux fins de la poursuite tant des finalités de la directive PNR que d'autres finalités.

3) La directive (UE) 2016/681 s'oppose à une législation nationale selon laquelle l'autorité mise en place en tant qu'UIP a également la qualité d'autorité nationale compétente, habilitée à approuver la communication des données PNR à l'expiration des six mois suivant le transfert de ces données à l'UIP.

4) L'article 12 de la directive (UE) 2016/681, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, s'oppose à une législation nationale qui prévoit une durée générale de conservation de ces données de cinq ans, applicable indifféremment à tous les passagers aériens. En effet, après l'expiration de la période de conservation initiale de six mois, la conservation des données PNR n'apparaît pas limitée au strict nécessaire en ce qui concerne les passagers aériens pour lesquels ni l'évaluation préalable, ni les éventuelles vérifications effectuées au cours de la période de conservation initiale de six mois, ni aucune autre circonstance n'ont révélé l'existence d'éléments objectifs – tels que le fait que les données PNR des passagers concernés ont donné lieu à une concordance positive vérifiée dans le cadre de l'évaluation préalable – de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le voyage aérien effectué par ces passagers. En revanche, au cours de la période initiale de six mois, la conservation des données PNR de l'ensemble des passagers aériens soumis au système instauré par cette directive ne paraît pas, par principe, excéder les limites du strict nécessaire.

5) La directive, lue à la lumière de l'article 3, paragraphe 2, TUE, de l'article 67, paragraphe 2, TFUE et de l'article 45 de la Charte, s'oppose à un système de transfert et de traitement des données PNR de l'ensemble des transports effectués par d'autres moyens (train, bateau, etc.) à l'intérieur de l'Union en l'absence de menace terroriste réelle et actuelle ou prévisible à laquelle fait face l'État membre concerné. Dans une telle situation, comme pour les vols intra-UE, l'application du système établi par la directive PNR doit être limitée aux données PNR des transports relatifs notamment à certaines liaisons ou à des schémas de voyage ou encore à certaines gares ou certains ports maritimes pour lesquels il existe des indications de nature à justifier cette application. Il appartient à l'État membre concerné de sélectionner les transports pour lesquels de telles indications existent et de réexaminer régulièrement cette application en fonction de l'évolution des conditions ayant justifié leur sélection.

CJUE, grande chambre, 21 juin 2022, Ligue des droits humains, C-817/19, points 168-174, 176, 194, 198, 124, 205, 209-211, 220, 223 231-237, 247, 261-262, 291

GendNotes

Exploitation ultérieure de données – Obligation d'indiquer la nature et l'objet des traitements ultérieurs concernés – Conditions d'exploitation – Absence d'indication – Manquement à l'exigence d'une finalité « déterminée, explicite et légitime »

Le décret n°2020-151 du 20 février 2020 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « application mobile de prise de notes » (GendNotes) autorise le ministre de l'intérieur à mettre en œuvre un traitement automatisé de données à caractère personnel dénommé GendNotes.

L'une des finalités du traitement est de « faciliter le recueil et la conservation « en vue de leur exploitation ultérieure dans d'autres traitements de données » » notamment par le biais d'un système de pré-renseignement des données collectées.

Le Conseil d'État annule ledit décret au motif que le traitement ne satisfait pas à l'exigence « déterminée, explicite et légitime ». En effet, dès lors qu'un décret prévoit, au titre des finalités du traitement, sa mise en relation avec d'autres traitements, il doit comporter des indications quant à la nature ou à l'objet des traitements concernés ou aux conditions d'exploitation, dans ces autres traitements, des données collectées par le traitement initial, afin de satisfaire pas à l'exigence d'une finalité « déterminée, explicite et légitime » énoncée au 2° de l'article 4 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

CE, 10ème-9ème chambres réunies, Ligue des droits de l'homme, 13 avril 2021, n°439360, Inédit., points 8, 14-15

Possibilité pour un traitement de données à caractère personnel de prévoir des zones de commentaires libres – Conditions

Saisi d'un projet de décret portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « application mobile de prise de notes » (GendNotes), le Conseil d'État (section de l'intérieur) lui a donné un avis favorable sous réserve des modifications qu'il lui a apportées.

Ce traitement de données a pour finalités, d'une part, de faciliter le recueil et la conservation, en vue de leur exploitation dans d'autres traitements de données, notamment par le biais d'un système de pré-renseignement, des informations collectées par les militaires de la gendarmerie nationale à l'occasion d'actions de prévention, d'investigations ou d'interventions, et nécessaires à l'exercice de leurs missions de polices judiciaire et administrative et, d'autre part, de faciliter la transmission de comptes rendus aux autorités judiciaires. Le traitement offre la possibilité à l'utilisateur de compléter, outre des champs prédéfinis, des zones de commentaires libres dans une interface « Note ». Ce

traitement, par ses finalités, relève du titre III de la loi du 6 janvier 1978 et de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016. Ces dispositions ne font pas obstacle à ce qu'un traitement comporte une zone de commentaires libres destinée à la consignation d'appréciations. Toutefois, afin d'éviter tout contournement des restrictions imposées tant par le droit de l'Union européenne que par la loi, le Conseil d'État estime que l'acte créant ce type de zone de commentaire doit respecter les principes suivants :

- une zone de commentaire libre ne doit être prévue que lorsque cela est strictement nécessaire à l'atteinte des finalités que poursuit le traitement ;
- les faits doivent y être présentés séparément des appréciations personnelles ;
- la liberté de formulation régissant ces espaces ne peut en aucune manière aboutir à collecter et traiter des données autres que celles expressément prévues par l'acte créant le traitement ;
- au regard de la difficulté de préciser le contenu de ces zones, il est nécessaire qu'une attention spécifique à celles-ci soit portée par l'analyse d'impact, qui doit en justifier l'existence et en analyser les risques.

CE, Section de l'intérieur, 4 février 2020, Avis n° 399342, Projet portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « application mobile de prise de notes » (GendNotes)

6.3 Renseignement

1) Législation nationale prévoyant une obligation extrêmement large de conservation de toutes les communications Internet de tous les utilisateurs – Violation de l'article 8 CEDH – 2) Accès direct aux communications sans présentation d'une autorisation d'interception aux fournisseurs de services – Absence de garanties adéquates et suffisantes contre les abus liés à l'accès des autorités répressives aux communications Internet et aux données de communication connexes stockées – 3) Obligation légale de déchiffrer les communications cryptées de bout en bout – Disproportion

1) La législation contestée exige la conservation et le stockage automatiques et continus du contenu de toutes les communications Internet (communications vocales, textuelles, visuelles, sonores, vidéo ou d'autres communications électroniques) pendant une durée de six mois et des données de connexion correspondantes pendant une durée d'un an. Elle concerne tous les utilisateurs, même en l'absence de soupçon raisonnable de participation à des activités criminelles ou à des activités mettant en danger la sécurité nationale, ou de toute autre raison de penser que la conservation des données peut contribuer à la lutte contre les formes graves de criminalité ou à la protection de la sécurité nationale. Il n'y a aucune limitation du champ d'application de la mesure en termes d'application territoriale ou temporelle ou de catégories de personnes susceptibles de voir leurs données à caractère personnel conservées. La Cour conclut que l'ingérence est exceptionnellement étendue et grave. La législation ne peut être considérée comme nécessaire dans une société démocratique et porte atteinte à l'essence même du droit au respect de la vie privée garanti par l'article 8 de la Convention. L'État défendeur a donc outrepassé toute marge d'appréciation acceptable à cet égard.

2) Contrairement à la législation en cause qui prévoit un accès direct aux communications Internet par les services de sécurité sans autorisation judiciaire préalable, la Cour recommande une obligation de présenter une autorisation au fournisseur de services de communication avant d'obtenir l'accès aux communications d'une personne en ce qu'elle constitue une garantie importante contre les abus des autorités répressives, en veillant à ce qu'une autorisation en bonne et due forme soit obtenue dans tous les cas de surveillance secrète.

3) L'obligation légale de déchiffrer les communications chiffrées de bout en bout risque d'équivaloir à une obligation pour les fournisseurs de tels services d'affaiblir le mécanisme de chiffrement pour tous les utilisateurs et n'est donc pas proportionnée aux buts légitimes poursuivis.

CEDH, 13 février 2024, Podchasov c. Russie, n°33696/19, points 70, 73 et 79

Directive 2002/58 – Article 15, paragraphe 1 – Utilisation de données de trafic et de localisation conservées par des fournisseurs de communications électroniques à des fins de lutte contre la criminalité grave – Utilisation ultérieure pour un objectif de moins grande importance – Enquêtes relatives à des fautes de service apparentées à la corruption –Exclusion

La possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité. En outre, la Cour a déjà jugé que l'accès à des données relatives au trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58, qui doit s'effectuer dans le plein respect des conditions résultant de la jurisprudence ayant interprété cette directive, ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 98)

Or, ces considérations s'appliquent mutatis mutandis à une utilisation ultérieure des données relatives au trafic et à des données de localisation conservées par des fournisseurs de services de communications électroniques en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 aux fins de la lutte contre la criminalité grave.

Celui-ci doit être doit être interprété en ce sens qu'il s'oppose à ce que des données à caractère personnel relatives à des communications électroniques qui ont été conservées, en application d'une mesure législative prise au titre de cette disposition, par les fournisseurs de services de communications électroniques et qui ont par la suite été mises à la disposition, en application de cette mesure, des autorités compétentes à des fins de la lutte contre la criminalité grave puissent être utilisées dans le cadre d'enquêtes relatives à des fautes de service apparentées à la corruption.

CJUE, 7 septembre 2023, Lietuvos Respublikos generalinė prokuratūra, C-162/22, points 39-41

Activation à distance d'appareils électroniques à l'insu de leur propriétaire ou possesseur – 1) Géolocalisation en temps réel – Objet de faciliter la mise en place de moyens techniques – Activation à distance dans des circonstances définies – Autorisation par le juge et pour une durée limitée – Personnes ne pouvant faire l'objet de telles mesures – Conformité – 2) Sonorisation et captation d'images – Enregistrement dans tout lieu des personnes visées et de tiers – Activation pour l'ensemble des infractions relevant de la délinquance ou de la criminalité organisées – Atteinte disproportionnée au droit au respect de la vie privée – Non-conformité

La loi déférée insère dans le code de procédure pénale des dispositions permettant, dans le cadre d'une enquête ou d'une instruction, l'activation à distance d'appareils électroniques à l'insu de leur propriétaire ou possesseur afin, d'une part, de procéder à sa localisation en temps réel et, d'autre part, de procéder à la sonorisation et à la captation d'images.

1) En premier lieu, ces dispositions ont pour objet de faciliter la mise en place ou la désinstallation des moyens techniques permettant, selon les cas, la géolocalisation ou la sonorisation et la captation d'images.

En deuxième lieu, il ne peut être recouru à l'activation à distance d'un appareil électronique, s'agissant de la géolocalisation, que lorsque les nécessités de l'enquête ou de l'instruction relative à un crime ou à un délit puni d'au moins cinq ans d'emprisonnement l'exigent et, s'agissant de la sonorisation et de la captation d'images, que si la nature et la gravité des faits le justifient.

En troisième lieu, d'une part, cette activation à distance ne peut être autorisée que par le juge des libertés et de la détention, à la requête du procureur de la République, ou par le juge d'instruction et aux seules fins de procéder à la localisation en temps réel ou à la sonorisation et à la captation d'images de la personne. La décision d'autorisation doit comporter tous les éléments permettant d'identifier l'appareil concerné. D'autre part, la durée de l'autorisation de procéder à la sonorisation et à la captation d'images, qui doit être strictement proportionnée à l'objectif recherché, ne peut excéder quinze jours renouvelable une fois, au cours d'une enquête, et deux mois renouvelable sans que la durée totale des opérations excède six mois, au cours d'une information judiciaire.

En quatrième lieu, d'une part, l'activation à distance d'un appareil électronique ne peut, à peine de nullité, concerner les appareils électroniques utilisés par un membre du Parlement, un magistrat, un avocat, un journaliste, un commissaire de justice ou un médecin. S'agissant de la sonorisation et de la captation d'images, il est en outre prévu, à peine de nullité, que ne peuvent être transcrites les données relatives aux échanges avec un avocat qui relèvent de l'exercice des droits de la défense et qui sont couvertes par le secret professionnel de la défense et du conseil, hors les cas prévus à l'article 56-1-2 du code de procédure pénale. Il en va de même des données relatives aux échanges avec un journaliste permettant d'identifier une source ou des données collectées à partir d'un appareil qui se trouvait dans l'un des lieux protégés au titre des articles 56-1, 56-2, 56-3 et 56-5 du même code. D'autre part, le juge compétent ordonne la destruction dans les meilleurs délais des données qui ne peuvent être transcrites, ainsi que des procès-verbaux et des données collectées lorsque les opérations ont été réalisées dans des conditions irrégulières.

Dès lors, les dispositions contestées, en tant qu'elles autorisent l'activation à distance d'appareils électroniques aux seules fins de géolocalisation, ne méconnaissent pas le droit au respect de la vie privée.

2) En revanche, l'activation à distance d'appareils électroniques afin de capter des sons et des images sans qu'il soit nécessaire pour les enquêteurs d'accéder physiquement à des lieux privés en vue de la mise en place de dispositifs de sonorisation et de captation, est de nature à porter une atteinte particulièrement importante au droit au respect de la vie privée dans la mesure où elle permet l'enregistrement, dans tout lieu où l'appareil connecté détenu par une personne privée peut se trouver, y compris des lieux d'habitation, de paroles et d'images concernant aussi bien les personnes visées par les investigations que des tiers. Dès lors, en permettant de recourir à cette activation à distance non seulement pour les infractions les plus graves mais pour l'ensemble des infractions relevant de la délinquance ou de la criminalité organisées, le législateur a permis qu'il soit porté au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi. Les dispositions contestées ne sont donc pas conformes à la Constitution.

CC, 2023-855 DC, 16 novembre 2023, Loi d'orientation et de programmation du ministère de la justice 2023-2027, points 63-69

Accès en temps réel aux données de trafic et de localisation (article L. 851-2 du code de la sécurité intérieure) – Garanties – Procédure s'appliquant également à l'entourage de la personne concernée – Conformité partielle

Les dispositions contestées permettent à l'autorité administrative, pour la prévention du terrorisme, d'obtenir le recueil en temps réel des données de connexion relatives, d'une part, à une personne préalablement identifiée susceptible d'être en lien avec une menace et, d'autre part, aux personnes appartenant à l'entourage de la personne concernée par l'autorisation lorsqu'il y a des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations au titre de la finalité qui

motive l'autorisation. Cette technique de recueil de renseignement est autorisée pour une durée de quatre mois renouvelable, conformément à l'article L. 821-4 du code de la sécurité intérieure.

D'une part, le recueil des données de connexion en temps réel ne peut être mis en œuvre que pour les besoins de la prévention du terrorisme. Ne peuvent, par ailleurs, être recueillis que les informations ou documents traités ou conservés par les opérateurs de télécommunication, les fournisseurs d'accès à un service de communication au public en ligne ou les hébergeurs de contenu sur un tel service.

D'autre part, cette technique de recueil de renseignement s'exerce dans les conditions prévues au chapitre Ier du titre II du livre VIII du code de la sécurité intérieure. En vertu de l'article L. 821-4 de ce code, elle est autorisée par le Premier ministre ou les collaborateurs directs auxquels il a délégué cette compétence, sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, après avis préalable de la Commission nationale de contrôle des techniques de renseignement. Elle est autorisée pour une durée de quatre mois renouvelable. En vertu du paragraphe II de l'article L. 851-2, la procédure d'urgence absolue prévue à l'article L. 821-5 de ce code n'est pas applicable. En application de l'article L. 871-6 du même code, les opérations matérielles nécessaires à la mise en place de la technique mentionnée à l'article L. 851-2 ne peuvent être exécutées, dans leurs réseaux respectifs, que par des agents qualifiés des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications.

Enfin, cette technique de renseignement est réalisée sous le contrôle de la Commission nationale de contrôle des techniques de renseignement. La composition et l'organisation de cette autorité administrative indépendante sont définies aux articles L. 831-1 à L. 832-5 du code de la sécurité intérieure dans des conditions qui assurent son indépendance. Ses missions sont définies aux articles L. 833-1 à L. 833-11 du même code dans des conditions qui assurent l'effectivité de son contrôle. Conformément aux dispositions de l'article L. 841-1 du même code, le Conseil d'État peut être saisi par toute personne souhaitant vérifier qu'aucune technique de recueil de renseignement n'est irrégulièrement mise en œuvre à son égard ou par la Commission nationale de contrôle des techniques de renseignement.

Il résulte de ce qui précède que le législateur a assorti la procédure de réquisition des données de connexion, lorsqu'elle s'applique à une personne préalablement identifiée susceptible d'être en lien avec une menace, de garanties propres à assurer une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public et celle des infractions et, d'autre part, le droit au respect de la vie privée.

En revanche, en application des dispositions contestées, cette procédure de réquisition s'applique également aux personnes appartenant à l'entourage de la personne concernée par l'autorisation, dont il existe des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation. Ce faisant, le législateur a permis que fasse l'objet de cette technique de renseignement un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit. Ainsi, faute d'avoir prévu que le nombre d'autorisations simultanément en vigueur doive être limité, le législateur n'a pas opéré une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le droit au respect de la vie privée.

CC, 2017-648 QPC, 4 août 2017, La Quadrature du Net et autres, points 5, 7-11

Procédure de réquisition administrative de donnée – Exclusion de l'accès au contenu des correspondances – Conformité

Des dispositions instituant une procédure de réquisition administrative de données de connexion excluant l'accès au contenu des correspondances ne sauraient méconnaître le droit au secret des correspondances.

CC, 2015-478 QPC, 24 juillet 2015, Association French Data Network et autres, point 17

Interceptions administratives de correspondances émises par la voie de communications électroniques (art. L.852-1 du code de la sécurité intérieure) – Conditions en cas d'extension à l'entourage de la personne concernée – Appareil ou dispositif permettant d'intercepter des paroles ou des correspondances – Conditions

Le paragraphe I de l'article L. 852-1 du code de la sécurité intérieure autorise les interceptions administratives de correspondances émises par la voie des communications électroniques, les personnes appartenant à l'entourage d'une personne concernée par l'autorisation d'interception peuvent également faire l'objet de ces interceptions lorsqu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation. Le paragraphe II de ce même article prévoit que, pour les finalités mentionnées aux 1°, 4° et a) du 5° de l'article L. 811-3, l'utilisation d'un appareil ou d'un dispositif permettant d'intercepter, sans le consentement de leur auteur, des paroles ou des correspondances émises, transmises ou reçues par la voie électronique ou d'accéder à des données informatiques peut être autorisée afin d'intercepter des correspondances émises ou reçues par un équipement terminal. Ces techniques de recueil de renseignement s'exercent, sauf disposition spécifique, dans les conditions prévues au chapitre Ier du titre II du code de la sécurité intérieure :

- elles sont autorisées par le Premier ministre, sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, après avis préalable de la Commission nationale de contrôle des techniques de renseignement et elles ne peuvent être mises en œuvre que par des agents individuellement désignés et habilités ;
- elles sont réalisées sous le contrôle de la Commission nationale de contrôle des techniques de renseignement dont la composition et l'organisation sont définies aux articles L. 831-1 à L. 832-5 dans des conditions qui assurent son indépendance et dont les missions sont définies aux articles L. 833-1 à L. 833-11 dans des conditions qui assurent l'effectivité de son contrôle ;
- conformément aux dispositions de l'article L. 841-1, le Conseil d'État peut être saisi par toute personne souhaitant vérifier qu'aucune technique de recueil de renseignement n'est irrégulièrement mise en œuvre à son égard ou par la Commission nationale de contrôle des techniques de renseignement ;
- en application des dispositions de l'article L. 871-6, les opérations matérielles nécessaires à la mise en place de ces techniques ne peuvent être exécutées, dans leurs réseaux respectifs, que par des agents qualifiés des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications.

Par ailleurs, ces techniques ne peuvent être mises en œuvre que pour les finalités énumérées à l'article L. 811-3 ; le nombre maximal des autorisations d'interception en vigueur simultanément est arrêté par le Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement ; afin de faciliter le contrôle de cette commission, l'exécution de ces interceptions est centralisée ; en outre, en ce qui concerne les interceptions réalisées au moyen de la technique prévue au paragraphe II de l'article L. 851-2, l'autorisation ne peut être délivrée que pour certaines des finalités mentionnées à l'article L. 811-3, qui sont relatives à la prévention d'atteintes particulièrement graves à l'ordre public ; les correspondances ainsi interceptées sont détruites dès qu'il apparaît qu'elles sont sans lien avec l'autorisation délivrée et au plus tard trente jours à compter de leur recueil. Il résulte de ce qui précède que le législateur n'a pas, par les dispositions précitées, opéré une conciliation manifestement déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public et celle des infractions et, d'autre part, le droit au respect de la vie privée et le secret des correspondances.

CC, 2015-713 DC, 23 juillet 2015, Loi relative au renseignement, points 51, 64-65,67

Annulation du refus d'abroger des dispositions réglementaires en tant qu'elles ne prévoient pas un réexamen périodique de l'existence d'une menace pour la sécurité nationale justifiant l'obligation pour les opérateurs de conserver de manière généralisée et indifférenciée les données de trafic et de localisation – 1) Injonction de compléter ces dispositions dans un délai de six mois – 2) Opérateurs pouvant se soustraire à cette obligation avant l'expiration de ce délai – Absence, dans la mesure où une telle menace a été constatée par le juge

Par son arrêt du 6 octobre 2020 La Quadrature du Net et autres (C-511/18, C-512/18, C-520/18), la Cour de justice de l'Union européenne (CJUE) a dit pour droit que la directive 2002/58/CE du 12 juillet 2002 ne s'opposait pas à ce que des mesures législatives permettent, aux fins de sauvegarde de la sécurité nationale, d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de trafic et des données de localisation, sous réserve qu'une décision soumise à un contrôle effectif constate l'existence d'une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, pour une durée limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. Il ressort en outre du point 135 de cet arrêt que la responsabilité des États membres en matière de sécurité nationale, au sens du droit de l'Union, correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société, et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme.

1) Ni l'article L. 34-1 du code des postes et des communications électroniques (CPCE) ni l'article 6 de la loi n° 2004-575 du 21 juin 2004 ne prévoient un réexamen périodique, au regard des risques pour la sécurité nationale, de la nécessité de maintenir l'obligation faite aux personnes concernées de conserver les données de connexion. Ces articles, ainsi, par suite, que l'article R. 10-13 du CPCE et le décret n° 2011-219 du 25 février 2011, en tant qu'ils ne subordonnent pas le maintien en vigueur de cette obligation au constat, à échéance régulière, qui ne saurait raisonnablement excéder un an, de la persistance d'une menace grave, réelle et actuelle ou prévisible, pour la sécurité nationale sont, dans cette mesure, contraires au droit de l'Union européenne. Il résulte de ce qui précède que, s'agissant de l'objectif de sauvegarde de la sécurité nationale, le refus d'abroger l'article R. 10-13 du CPCE et l'article 1er du décret du 25 février 2011 doit être annulé en tant seulement que leurs dispositions ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, s'agissant des données qu'elles mentionnent autres que celles afférentes à l'identité civile, aux comptes et aux paiements des utilisateurs et aux adresses IP. Il y a lieu d'enjoindre au Gouvernement de compléter ces dispositions dans un délai de six mois à compter de la présente décision.

2) Il ressort des pièces du dossier que la France est, à la date de la présente décision, confrontée à une menace grave, réelle et non seulement prévisible mais actuelle pour sa sécurité nationale, appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure (CSI) qui, par son intensité, revêt un caractère grave et réel. Cette menace est, à la date de la présente décision, non seulement prévisible mais aussi actuelle. Cette menace procède d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés. Par ailleurs, la France est particulièrement exposée au risque d'espionnage et d'ingérence étrangère, en raison notamment de ses capacités et de ses engagements militaires et de son potentiel technologique et économique. La France est également confrontée à des menaces graves pour la paix publique, liées à une augmentation de l'activité de groupes radicaux et extrémistes. Dans la mesure où il résulte de la présente décision que la réalité et la gravité de la menace pesant sur la sécurité nationale justifient l'obligation de conservation généralisée et indifférenciée de l'ensemble des données de connexion à cette fin, les opérateurs ne sauraient, avant l'expiration du délai de six mois laissé au Gouvernement pour compléter les dispositions litigieuses, se soustraire à cette

obligation et aux sanctions dont sa méconnaissance est assortie au motif que la durée de l'injonction qui leur est faite n'a pas été limitée dans le temps par le pouvoir réglementaire.

CE, Assemblée, 21 avril 2021, French Data Network et autres, n° 393099, Rec., points 27, 42, 46, 44

Voir aussi : 2.11.8 Données de connexion

6.4 Traitements économiques et fiscaux

Traitement de données à caractère personnel à des fins fiscales – Demande de communication d'informations relatives à des annonces de vente de véhicules mises en ligne – 1) Application des principes de l'article 5 du RGPD – Application, en l'absence de mention expresse inverse dans le droit national – 2) Licéité – Existence

1) Les dispositions du RGPD doivent être interprétées en ce sens que l'administration fiscale d'un État membre ne saurait déroger aux dispositions de l'article 5, paragraphe 1, de ce règlement, qui fixe les principes à respecter par tout traitement, alors qu'un tel droit ne lui a pas été octroyé par le droit national, au sens de l'article 23, paragraphe 1, de ce même texte.

2) Les dispositions du RGPD doivent être interprétées en ce sens qu'elles ne s'opposent pas à ce que l'administration fiscale d'un État membre impose à un prestataire de services d'annonces publiées sur internet de lui communiquer des informations relatives aux contribuables ayant publié des annonces dans l'une des rubriques de son portail en ligne, dès lors que cela est nécessaire à la mission d'intérêt public poursuivie par cette administration. Néanmoins, les données demandées doivent être nécessaires au regard des finalités spécifiques pour lesquelles elles sont collectées et la période sur laquelle porte leur collecte ne saurait excéder la durée strictement nécessaire pour atteindre l'objectif d'intérêt général visé.

CJUE, 24 février 2022, Valsts ieņēmumu dienests, C-175/20

Demande de communication d'informations par l'administration fiscale dans le cadre d'une procédure de coopération entre États membres – 1) Droit au recours contre cette décision de la personne requise – Existence – 2) Limitation du droit au recours effectif du contribuable visé par une enquête fiscale et les tiers concernés par les informations en cause – Licéité – 3) Demande portant sur des « catégories d'informations » – Licéité – Conditions

1) Le droit à un recours effectif garanti par la Charte des droits fondamentaux impose de permettre aux personnes qui sont détentrices d'informations dont l'administration nationale demande la communication, dans le cadre d'une procédure de coopération entre États membres, de former un recours direct contre cette demande.

2) En revanche, les États membres peuvent priver d'une telle voie de recours direct le contribuable visé par l'enquête fiscale et les tiers concernés par les informations en cause, dès lors qu'il existe d'autres voies de recours permettant à ces derniers d'obtenir un contrôle incident de ladite demande.

3) Par ailleurs, une demande d'informations peut valablement porter sur des catégories d'informations plutôt que sur des informations précises, si ces catégories sont délimitées au moyen de critères établissant leur caractère « vraisemblablement pertinent ».

CJUE, grande chambre, 6 octobre 2020, État luxembourgeois, C-245/19 et C/246/19, points 69, 79, 120-123

Fourniture de réseaux publics de communication et de service de communications électroniques – Traitement de données par une société tierce chargée du recouvrement des créances – Conditions de licéité – Personnes agissant sous l'autorité des fournisseurs – Traitement limité aux données nécessaires aux fins de recouvrement des créances

Les articles 6, paragraphes 2 et 5 de la directive 2002/58/CE du 12 juillet 2002 (directive vie privée et communications électroniques) doivent être interprétés en ce sens qu'ils autorisent un fournisseur de réseaux publics de communications et de services de communications électroniques accessibles au public à transmettre des données relatives au trafic au cessionnaire de ses créances portant sur la fourniture de services de télécommunications en vue du recouvrement de celles-ci, et ce cessionnaire à traiter lesdites données à condition que en premier lieu, celui-ci agisse sous l'autorité du fournisseur de services pour ce qui concerne le traitement de ces mêmes données et, en second lieu, ledit cessionnaire se limite à traiter les données relatives au trafic qui sont nécessaires aux fins du recouvrement des créances cédées.

Indépendamment de la qualification du contrat de cession, le cessionnaire est censé agir sous l'autorité du fournisseur de services, au sens de l'article 6, paragraphe 5, de la directive 2002/58, lorsque, pour le traitement des données relatives au trafic, il agit sur la seule instruction et sous le contrôle dudit fournisseur. En particulier, le contrat conclu entre eux doit comporter des dispositions de nature à garantir le traitement licite, par le cessionnaire, des données relatives au trafic et à permettre au fournisseur de services de s'assurer, à tout moment, du respect de ces dispositions par ledit cessionnaire.

CJUE, 22 novembre 2012, Probst, C-119/12

Registre public des trusts – Informations sur la manière de disposer de son patrimoine – Non-conformité

La mention, dans un registre accessible au public, des noms du constituant, des bénéficiaires et de l'administrateur d'un trust fournit des informations sur la manière dont une personne entend disposer de son patrimoine. Il en résulte une atteinte au droit au respect de la vie privée. Or, le législateur, qui n'a pas précisé la qualité ni les motifs justifiant la consultation du registre, n'a pas limité le cercle des personnes ayant accès aux données de ce registre, placé sous la responsabilité de l'administration fiscale. Dès lors, les dispositions contestées portent au droit au respect de la vie privée une atteinte manifestement disproportionnée au regard de l'objectif poursuivi.

CC, 2016-591 QPC, 21 octobre 2016, Mme Helen S, point 6

Registre national des crédits aux particuliers – Conditions du traitement – Non-conformité

L'article 67 de la loi n°2021-344 du 17 mars 2014 relative à la consommation crée un traitement de données à caractère personnel recensant les crédits à la consommation accordés aux personnes physiques n'agissant pas pour des besoins professionnels, dénommé « registre national des crédits aux particuliers ».

Par la création de ce registre, le législateur a poursuivi un motif d'intérêt général de prévention du surendettement. Toutefois, ce registre est destiné à comprendre des données à caractère personnel d'un très grand nombre de personnes (plus de 12 millions), la durée de conservation est de plusieurs années (toute la durée du crédit ou du plan de surendettement), les motifs de consultation sont très nombreux (octroi d'un crédit à la consommation mais également d'un prêt sur gage corporel, reconduction d'un contrat de crédit renouvelable, vérification triennale de solvabilité de

l'emprunteur, vérification relative aux personnes se portant caution d'un prêt à la consommation...) et plusieurs dizaines de milliers d'agents des établissements de crédit seront habilités à consulter le registre.

Compte tenu de la nature des données enregistrées, de l'ampleur du traitement de données, de la fréquence de son utilisation, du grand nombre de personnes susceptibles d'y avoir accès et de l'insuffisance des garanties relatives à l'accès au registre, la création du registre national des crédits aux particuliers porte une atteinte au droit au respect de la vie privée qui ne peut être regardée comme proportionnée au but poursuivi.

CC, 2014-690 DC, 13 mars 2014, Loi relative à la consommation, points 51-57

Traitement relevant du RGPD ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou des mesures de sûreté (art. 31 de la loi du 6 janvier 1978) – Notion – Traitement ayant pour finalité le transfert de données fiscales vers l'administration fiscale américaine – Inclusion

Accord conclu le 14 novembre 2013 entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et de mettre en œuvre la loi relative au respect des obligations fiscales concernant les comptes étrangers (dite « loi FATCA »). Traitement d'échange automatique d'informations organisant notamment la collecte et le transfert de données à caractère personnel aux autorités fiscales américaines créé pour la mise en œuvre de cet accord.

Si le traitement créé par l'arrêté du 5 octobre 2015 a pour finalité de lutter contre la fraude et l'évasion fiscales et relève à ce titre du RGPD et non de la directive n° 2016/680, il doit être regardé comme ayant parmi ses objets la prévention, la recherche, la constatation ou la poursuite des infractions pénales. Il s'ensuit, eu égard à cet objet, qu'il est au nombre des traitements visés à l'article 31 de la loi n° 78-17 du 6 janvier 1978.

CE, Assemblée, 19 juillet 2019, Association des Américains accidentels, n°424216, Rec., point

---

Traitement mis en œuvre par l'administration fiscale, permettant à des tiers de consulter les données fiscales d'un particulier pour vérifier l'authenticité des données que celui-ci leur a fournies – Définition insuffisamment précise des personnes susceptibles de consulter ce traitement – Conséquence – Méconnaissance de l'article 29 de la loi du 6 janvier 1978 dans sa rédaction applicable au litige

Arrêté créant un traitement ayant pour objet de permettre à des tiers à qui un contribuable a communiqué une copie de son avis d'impôt sur le revenu ou de son justificatif d'impôt sur le revenu, de vérifier l'authenticité des données qui y figurent au moyen d'une consultation directe du justificatif d'impôt sur le revenu du contribuable certifié par l'administration fiscale.

Les destinataires du traitement ne sont définis, par les dispositions de l'arrêté attaqué, que comme les personnes ayant besoin, dans le cadre de leurs activités, de connaître et de vérifier l'authenticité des informations contenues dans le justificatif d'impôt sur le revenu d'un contribuable. Une telle définition ne peut être regardée, eu égard à l'importance des données en cause, comme précisant suffisamment les destinataires ou catégories de destinataires habilités à en recevoir communication, comme l'exige l'article 29 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés. Dès lors que les dispositions en cause ne sont pas divisibles du reste de l'arrêté attaqué, celui-ci doit être déclaré illégal.

CE, 10ème-9èmechambres réunies, 24 avril 2019, Caisse d'épargne et de prévoyance Languedoc-Roussillon, n°419498, T., point 8

---

1) Consultation obligationre du fichier des incidents de remboursement des crédits aux particuliers (FICP) – Obligation légale – 2) Consultation facultative du FICP – Base légale – Intérêt légitime – Mise en balance des intérêts

1) Le II de l'article 2 de l'arrêté du 26 octobre 2010 relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) combiné aux articles L.751-2 et L. L312-16 du code de la consommation prévoient les cas obligatoires de consultation du FICP par les établissements et organismes dans le cadre de l'octroi d'un crédit. Les traitements de données à caractère personnel mis en œuvre dans le cadre des opérations de consultation obligatoires du FICP, telles que définies par ces dispositions, ne peuvent être fondés que sur la base légale prévue à l'article 6, paragraphe 1, point c) du RGPD, à savoir le respect d'une obligation légale.

2) Le III de l'article 2 de l'arrêté du 26 octobre 2010 relatif au fichier national des incidents de remboursement des crédits aux particuliers (FICP) prévoit les cas de consultations facultatives. Les traitements de données à caractère personnel mis en œuvre dans ce cadre peuvent, à certaines conditions, reposer sur la base légale de l'intérêt légitime poursuivi par le responsable de traitement (art. 6, §1, f). Dans ce cas, le responsable de traitement est tenu de réaliser, au cas par cas, une mise en balance entre l'intérêt légitime poursuivi et les intérêts et libertés et droits fondamentaux des personnes concernées afin de s'assurer que la consultation n'est pas de nature à porter une atteinte disproportionnée à leur vie privée.

CNIL, P, 1er août 2024, Rappel aux obligations légales, Société X, n°ROL231090, non publié

6.5 Directive ePrivacy et chapitre III loi Informatique et Libertés, sauf prospection

6.5.1 Champ d'application

Directive vie privée et communications électroniques (dite ePrivacy)– Dispositions législatives nationales encadrant l'exploitation des données de trafic et de localisation – Exclusion

Les dispositions du code de la sécurité intérieure encadrant l'exploitation des données de trafic et de localisation collectées par les services de renseignement, sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques, ne relèvent pas du champ d'application de la directive 2002/58/CE (directive vie privée et communications électroniques).

CE, Assemblée, 21 avril 2021, French Data Network et autres, n° 393099, Rec., point 93

6.5.2 Articulation RGPD/ePrivacy

« Guichet unique » applicable aux traitements transfrontaliers (art. 56) – 1) Champ d'application – Exclusion – Mesures de mise en œuvre et de contrôle de la directive 2002/58/CE – Conséquence – 2) Compétence de la CNIL pour le contrôle des opérations d'accès et d'inscription d'informations dans les terminaux des utilisateurs en France d'un service de communications électroniques

1) Il résulte des paragraphes 1 des articles 55 et 56 du RGPD et de l'article 15 bis de la directive 2002/58/CE du 12 juillet 2002, tels qu'interprétés par la CJUE dans son arrêt du 1er octobre 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände Verbraucherzentrale Bundesverband eV/Planet49 GmbH (C-673/17) et son arrêt du 15 juin 2021, Facebook Ireland Ltd e.a. (C-645/19), que si les conditions de recueil du consentement de l'utilisateur prévues par le RGPD sont applicables aux opérations de lecture et d'écriture dans le terminal d'un utilisateur, il n'a pas été prévu l'application du mécanisme dit du « guichet unique » applicable aux traitements transfrontaliers, défini à l'article 56 de ce règlement, pour les mesures de mise en œuvre et de contrôle de la directive 2002/58/CE, qui relèvent de la compétence des autorités nationales de contrôle en vertu de l'article 15 bis de cette directive.

2) Il s'ensuit que, pour ce qui concerne le contrôle des opérations d'accès et d'inscription d'informations dans les terminaux des utilisateurs en France d'un service de communications électroniques, même procédant d'un traitement transfrontalier, les mesures de contrôle de l'application des dispositions ayant transposé les objectifs de la directive 2002/58/CE relèvent de la compétence conférée à la Commission nationale de l'informatique et des libertés par la loi n° 78-17 du 6 janvier 1978.

CE, 10ème–9ème chambres réunies, 28 janvier 2022, Sociétés Google LLC et Google Ireland Limited, n°449209, Rec., point 12

Articles 5-3, 9 et 13 de la directive 2002/58/CE prévoyant un consentement – 1) Lex specialis prévalant sur l'article 6 du RGPD pour ces opérations – 2) Compétence des autorités ePrivacy et des autorités RGPD – Articulation – 3) Mécanismes de coopération et de cohérence

1) De manière générale, le consentement préalable est nécessaire pour le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur. Dans la mesure où les informations stockées sur l'appareil de l'utilisateur final constituent des données à caractère personnel, l'article 5, paragraphe 3, de la directive « vie privée et communications électroniques » prime sur l'article 6 du RGPD pour ce qui relève des activités consistant à stocker ce type d'informations ou à y accéder. Il en va de même en ce qui concerne les interactions entre l'article 6 du RGPD et les articles 9 (traitement des données de géolocalisation) et 13 (prospection électronique) de la directive vie privée et communications électroniques. Lorsque ces articles exigent un consentement pour les actions spécifiques qu'ils décrivent, le responsable du traitement ne peut pas se fonder sur l'ensemble des bases juridiques possibles prévues à l'article 6 du RGPD.

2) Lorsque le traitement de données à caractère personnel relève à la fois du champ d'application matériel du RGPD et de celui de la directive « vie privée et communications électroniques », les autorités de protection des données ne sont compétentes pour contrôler les sous-ensembles du traitement qui sont régis par des règles nationales transposant la directive « vie privée et communications électroniques » que si la législation nationale leur confère cette compétence. Toutefois, la compétence des autorités de protection des données au titre du RGPD reste en tout état de cause inchangée en ce qui concerne les traitements qui ne sont pas soumis à des règles particulières prévues par la directive « vie privée et communications électroniques ». Le simple fait qu'un sous-ensemble du traitement relève du champ d'application de la directive « vie privée et

communications électroniques » ne limite pas la compétence des autorités de protection des données au titre du RGPD.

L'article 5, paragraphe 3, de la directive « vie privée et communications électroniques » contient une règle spéciale applicable au stockage d'informations, ou à l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un utilisateur final. Il ne contient en revanche pas de règle spéciale pour toute activité de traitement antérieure ou ultérieure (par exemple, le stockage et l'analyse des données relatives à la navigation sur internet à des fins de publicité comportementale en ligne ou de sécurité). En conséquence, les autorités de protection des données restent pleinement compétentes pour évaluer la licéité de tous les autres traitements qui suivent le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans l'équipement terminal de l'utilisateur final.

3) Les mécanismes de coopération et de cohérence dont disposent les autorités de protection des données au titre du chapitre VII du RGPD concernent le contrôle de l'application des dispositions du RGPD. Les mécanismes du RGPD ne s'appliquent pas au contrôle de l'application de la transposition nationale de la directive « vie privée et communications électroniques ». Le mécanisme de coopération et de cohérence reste néanmoins pleinement applicable dans la mesure où le traitement est soumis aux dispositions générales du RGPD.

CEPD, 12 mars 2019, Avis Art. 64, Interactions entre la directive ePrivacy et le RGPD, 5/2019

6.5.3 Consentement et informations pour les opérations de lecture-écriture (cookies et autres traceurs)

Prospection commerciale – 1) Exigence d'obtenir un consentement préalable à la réception d'annonces publicitaires par courrier électronique – 2) Service gratuit de messagerie électronique – Information claire et précise des personnes concernées – Consentement de manière spécifique et en pleine connaissance de cause à recevoir des messages publicitaires

1) S'agissant de l'exigence d'obtenir un consentement préalable à la prospection commerciale par voie électronique, il résulte de l'article 2, second alinéa, sous f), de la directive 2002/58, lu en combinaison avec l'article 94, paragraphe 2, du règlement 2016/679, que ce consentement doit satisfaire aux exigences résultant de l'article 2, sous h), de la directive 95/46 ou de l'article 4, point 11, de ce règlement, selon que l'une ou l'autre de ces deux normes est applicable *ratione temporis* aux faits en cause au principal.

2) Lorsqu'un service de messagerie électronique est proposé aux utilisateurs sous la forme de deux catégories de services de messageries, à savoir, d'une part, un service de messagerie gratuit, financé par la publicité et, d'autre part, un service de messagerie payant, sans publicité, il appartient à la juridiction de renvoi de déterminer si l'utilisateur concerné, ayant opté pour la gratuité du service de messagerie électronique, a été dûment informé des modalités précises de diffusion d'une telle publicité et a effectivement consenti à recevoir des messages publicitaires tels que ceux en cause au principal. En particulier, il y a lieu de s'assurer, d'une part, que cet utilisateur a été informé de manière claire et précise notamment du fait que des messages publicitaires sont affichés au sein de la liste des courriels privés reçus et, d'autre part, qu'il a manifesté son consentement de manière spécifique et en pleine connaissance de cause à recevoir de tels messages publicitaires (voir, en ce sens, arrêt du 11 novembre 2020, Orange Romania, C-61/19, EU :C :2020:901, point 52).

CJUE, 20 novembre 2021, StWL, C-102/20, points 53, 58-59

Cookies – Recueil du consentement préalablement au dépôt et à l'utilisation de traceurs de connexion pour des opérations d'affiliation

Dans le cadre d'opérations d'affiliation impliquant l'utilisation de traceurs de connexion afin de déterminer si l'internaute qui a accompli un acte d'achat sur un site marchand s'est connecté sur ce site à partir d'un lien figurant sur celui de l'opérateur affilié, ces traceurs ont pour seule finalité de permettre la rémunération de l'affilié par l'éditeur du site marchand, le cas échéant par l'intermédiaire d'une plateforme d'affiliation. Ils n'ont pas pour finalité de permettre ou de faciliter la communication par voie électronique au sens de l'article 82 de la loi n°78-17 du 6 janvier 1978, dès lors qu'aucun traceur de connexion de la nature de ceux utilisés pour la facturation des opérations d'affiliation n'est nécessaire pour qu'un internaute se connecte à un site marchand à partir d'un site édité par un tiers et y effectue un achat. Ils ne peuvent davantage être regardés comme strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur, alors que la rémunération de l'affilié par l'éditeur du site marchand ne répond pas à une demande de l'utilisateur. Par ailleurs, la circonstance que certains traceurs seraient nécessaires à la viabilité économique d'un site ou d'un partenariat ne saurait conduire à les ranger dans l'une ou l'autre des exceptions prévues par l'article 82 de la loi de la loi du 6 janvier 1978. Enfin, ces traceurs n'ont, en tout état de cause, pas la même finalité que ceux permettant la mesure de l'audience des sites internet. Par suite, il doit être exigé que le consentement des utilisateurs soit recueilli préalablement au dépôt et à l'utilisation des traceurs en cause.

CE, 10ème–9ème chambres réunies, 8 avril 2022, Syndicat national du marketing à la performance (SNMP), n°452668, Rec., point 13

Traitements de données consistant en l'utilisation de traceurs de connexion (« cookies ») – 1) Caractère éclairé du consentement – Conditions – a) Information sur l'identité des responsables de traitement et de leurs destinataires – Portée – b) Consentement à chaque finalité poursuivie par le traitement (art. 82 de la loi du 6 janvier 1978) – Modalités d'application – 2) Conditions d'expression du refus de consentement – 3) Interdiction générale et absolue tirée de la seule exigence d'un consentement libre dans le cadre d'un instrument de droit souple – Illégalité dans cette mesure

1) a) Il résulte de l'article 82 de la loi n°78-17 du 6 janvier 1978, éclairée par les dispositions respectives de la directive 2002/58/CE telles qu'interprétées par la Cour de justice de l'Union européenne dans son arrêt C-673/17 du 1er octobre 2019 et du RGPD, que pour que le consentement préalable puisse être regardé comme éclairé, l'utilisateur doit pouvoir disposer de l'identité du ou des responsables de traitement ainsi que de la liste des destinataires ou des catégories de destinataires de ses données. En particulier, si l'éditeur d'un site qui dépose des « cookies » doit être considéré comme un responsable de traitement, y compris lorsqu'il sous-traite à des tiers la gestion de « cookies » mis en place pour son propre compte, doivent également être considérés comme responsables de traitement les tiers qui déposent des cookies à l'occasion de la visite du site d'un éditeur dès lors qu'ils agissent pour leur compte propre. Il résulte clairement de l'article 7, point 1, du RGPD que le responsable de traitement doit être en mesure, à tout moment, de fournir la preuve du recueil valable du consentement de l'utilisateur. Par suite, la CNIL a pu légalement rappeler qu'une liste exhaustive et régulièrement mise à jour des responsables ou co-responsables du traitement de données doit être mise à disposition de l'utilisateur directement lors du recueil de son consentement.

b) Il découle des dispositions de l'article 82 de la loi n° 78-17 du 6 janvier 1978 que le consentement de l'utilisateur doit porter sur chacune des finalités poursuivies par le traitement de données et que toute nouvelle finalité ultérieure, compatible avec la ou les finalités initiales, assignée au traitement de données est soumise au recueil d'un consentement propre. Le respect d'une telle exigence implique à tout le moins, dans l'hypothèse où le recueil du consentement serait effectué de manière globale, qu'il soit précédé d'une information spécifique à chacune des finalités.

2) Il résulte clairement de la combinaison de l'article 4, point 11 et de l'article 7, paragraphe 3 du RGPD avec l'article 82 de la loi n° 78-17 du 6 janvier 1978 que, d'une part, en l'absence de consentement exprimé par un acte positif clair, l'utilisateur doit être considéré comme ayant refusé l'accès à son terminal ou l'inscription d'informations dans ce dernier, et que, d'autre part, il peut retirer son consentement à tout moment. Il s'ensuit que la CNIL qui, en indiquant qu'il devait « être aussi facile de refuser ou de retirer son consentement que de le donner », s'est bornée à caractériser les conditions du refus de l'utilisateur sans définir de modalités techniques particulières d'expression d'un tel refus, n'a entaché sa délibération d'aucune méconnaissance des règles applicables en la matière.

3) La CNIL affirmait, à l'article 2 de sa recommandation, que la validité du consentement est soumise à la condition que la personne concernée ne subisse pas d'inconvénient majeur en cas d'absence ou de retrait de son consentement, un tel inconvénient majeur pouvant consister, selon elle, dans l'impossibilité d'accéder à un site Internet, en raison de la pratique des « cookies walls ». En déduisant pareille interdiction générale et absolue de la seule exigence d'un consentement libre, posé par le RGPD, la CNIL a excédé ce qu'elle peut légalement faire, dans le cadre d'un instrument de droit souple, édicté sur le fondement du 2° du I de l'article 8 de la loi du 6 janvier 1978 cité au point 3. Il s'ensuit que la délibération attaquée est, dans cette mesure, entachée d'illégalité.

CE, 10ème–9ème chambres réunies, 19 juin 2020, Association des agences-conseil en communication et autres, n° 434684, T. points 10, 12-13, 15

Obligations pesant sur les responsables de traitement consistant en l'utilisation de témoins de connexion (« cookies ») – 1) Portée – Obligations d'information des utilisateurs de services de communications électroniques sur la finalité de ces témoins de connexion et sur les moyens dont ils disposent pour s'y opposer ainsi que de recueil préalable de leur consentement – Exception – « Cookies » essentiels au fonctionnement technique du site au rang desquels ne figurent pas les cookies ayant une finalité publicitaire qui seraient nécessaires à la viabilité économique d'un site – Notion – 2) Espèce – Éléments portés à la connaissance des utilisateurs d'un site ne leur permettant pas de différencier les catégories de « cookies », ni de s'opposer à ceux dont le dépôt est soumis à leur consentement préalable, ni de connaître les conséquences attachées à leur éventuelle opposition

1) Les dispositions de l'article 32 de la loi n°78-17 du 6 janvier 1978 éclairées par les objectifs de la directive n° 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques qu'elles transposent, instituent une obligation d'information claire et complète des utilisateurs d'internet sur les témoins de connexion (« cookies ») qui sont susceptibles d'être déposés, notamment sous la forme de fichiers, sur leurs terminaux lorsqu'ils visitent un site, ces témoins de connexion et les informations qu'ils contiennent étant par la suite accessibles lors de connexions ultérieures à internet à l'aide du même terminal. Elles imposent, d'une part, une information des utilisateurs de services de communications électroniques, en particulier des utilisateurs d'internet, sur la finalité de ces « cookies » et les moyens dont ils disposent pour s'y opposer. Elles imposent, d'autre part, le recueil de leur consentement avant tout dépôt de « cookies » sur le terminal grâce auquel ils accèdent à ces services. Ne sont pas concernés par ces obligations les « cookies » qui sont essentiels au fonctionnement technique du site ni ceux qui correspondent à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur. En revanche, le fait que certains « cookies » ayant une finalité publicitaire soient nécessaires à la viabilité économique d'un site ne saurait conduire à les regarder comme « strictement nécessaires à la fourniture » du service de communication en ligne.

2) Alors que la société requérante soutient qu'elle s'est mise en conformité avec ces exigences, en proposant aux personnes concernées le paramétrage de leur navigateur pour s'opposer au dépôt de cookies, les éléments portés à la connaissance des utilisateurs du site « www.challenges.fr » ne leur permettaient ni de différencier clairement les catégories de « cookies » susceptibles d'être déposés sur

leur terminal, ni de s'opposer seulement à ceux dont le dépôt est soumis à leur consentement préalable, ni de connaître les conséquences, en termes de navigation sur le site, attachées à leur éventuelle opposition. Dans ces conditions, c'est à bon droit que la formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL) a considéré que le paramétrage du navigateur proposé aux utilisateurs ne constituait pas un mode valable d'opposition au dépôt de « cookies » et en a déduit qu'il n'avait pas été remédié au manquement à l'obligation d'information et de mise en œuvre d'un mécanisme d'opposition en cas de dépôt de témoins de connexion qu'elle avait constaté dans sa mise en demeure.

CE, 10ème-9ème chambres réunies, 6 juin 2018, Société Éditions Croque Futur, n° 412589, Rec., points 7-8

Dispositif dit de « re-captcha » – Cas où les données sont utilisées pour des finalités complémentaires à la seule sécurité du site internet par une société tierce – Nécessité du consentement

Si un responsable de traitement peut se prévaloir d'une exemption à l'information et au recueil du consentement lorsque les opérations de lecture/écriture effectuées dans le terminal d'un utilisateur ont pour seule finalité la sécurisation d'un mécanisme d'authentification au bénéfice des utilisateurs, il en va autrement lorsque ces opérations poursuivent également d'autres finalités qui ne sont pas strictement nécessaires à la fourniture d'un service. Ainsi, un mécanisme de reCAPTCHA n'ayant pas pour seule finalité la sécurisation du mécanisme d'authentification au bénéfice des utilisateurs mais permettant par ailleurs des opérations d'analyse de la part d'une société tierce doit faire l'objet d'une information des utilisateurs et du recueil de leur consentement.

CNIL, FR, 16 mars 2023, Sanction, Société X, n°SAN-2023-003, publié, point 86

Modalités de refus des cookies – Possibilité de refuser les opérations de lecture et/ou d'écriture avec le même degré de simplicité – Absence – Altération de la liberté de choix – Manquement – Article 82 loi Informatique et libertés

Le fait de rendre le mécanisme de refus des cookies plus complexe que celui consistant à les accepter revient en réalité à décourager les utilisateurs de refuser les cookies et à les inciter à privilégier la facilité d'un bouton « Tout accepter ». En effet, un utilisateur d'internet est généralement conduit à consulter de nombreux sites. La navigation sur internet se caractérise par sa rapidité et sa fluidité. Le fait de devoir cliquer sur un bouton de gestion des paramètres et de devoir comprendre la façon dont est construite la page permettant de refuser les cookies est susceptible de décourager l'utilisateur, qui souhaiterait pourtant refuser le dépôt des cookies. Les modalités par lesquelles le refus des cookies peut être exprimé, dans le contexte de la navigation sur Internet, peuvent biaiser l'expression du choix en faveur du consentement de façon à altérer la liberté de choix. Le fait de ne pas offrir à l'utilisateur la possibilité de refuser les opérations de lecture et/ou d'écriture avec le même degré de simplicité qu'il avait de les accepter est de nature à caractériser un manquement aux dispositions de l'article 82 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, interprétées à la lumière du RGPD.

CNIL, FR, 29 décembre 2022, Sanction, Société X, n° SAN-2022-027, publié, points 75, 77

Lecture d'informations collectées via des traceurs strictement nécessaires à la fourniture d'un service – Association des requêtes émises à un compte

utilisateur – Univers « authentifié » ou « logué » – Nécessité d'un consentement avant lecture si certaines des finalités sont soumises à consentement

Lorsqu'un identifiant mobile est créé pour chaque compte utilisateur sur les serveurs d'une société, des « informations » sont lues sur l'équipement terminal de ce dernier pour permettre d'associer les requêtes émises à un compte utilisateur (c'est-à-dire le fait que l'utilisateur effectue une recherche, télécharge ou achète des applications) et, plus tard, d'affecter cet utilisateur unique à des segments au sein d'un univers nécessitant une authentification (univers dit « authentifié » ou « logué »). Quand bien même la principale fonction de ces « informations » serait de permettre l'authentification d'un utilisateur au sein d'un univers logué – ce qui constituerait en soi une finalité dispensée de recueil du consentement car strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur - , la circonstance que les informations collectées grâce à ces témoins de connexion soient également utilisées pour permettre la segmentation à des fins publicitaires empêche nécessairement lesdits témoins de connexion de rentrer dans les catégories de traceurs dont la lecture est exemptée de recueil du consentement au sens de l'article 82 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée.

CNIL, FR, 29 décembre 2022, Sanction, Société X, n° SAN-2022-025, publié, point 98

Voir aussi : CNIL, FR, 29 décembre 2022, Sanction, Société X, n° SAN-2022-026, publié

---

1) Cookie multi-finalités – Nécessité d'un consentement avant inscription si certaines des finalités sont soumises à consentement – 2) Lutte contre la fraude publicitaire – Finalité non essentielle, nécessitant un consentement

1) Si un cookie multi-finalités peut être déposé sans consentement pour une finalité essentielle qui relève de l'une des deux exemptions prévues à l'article 82 de la loi Informatique et Libertés, la société ne pourra utiliser ce cookie pour des finalités non essentielles que si l'utilisateur a effectivement consenti à ces finalités spécifiques préalablement à son inscription dans son terminal. En effet, déposer un cookie multi-finalités sur le terminal de l'utilisateur pour des finalités essentielles exemptes du recueil du consentement au titre des exemptions prévues à l'article 82 de la loi Informatique et Libertés, puis faire relever du RGPD les traitements ultérieurs réalisés pour des finalités non essentielles dudit cookie, reviendrait à détourner les dispositions de l'article 82 de la loi Informatique et Libertés puisque le consentement de l'utilisateur ne serait plus jamais sollicité préalablement au dépôt de cookies.

2) À ce titre, la finalité de lutte contre la fraude publicitaire, comprise comme l'ensemble des pratiques de tiers visant à manipuler la distribution et la mesure publicitaire opérée par une régie, que cette fraude soit opérée au détriment de ladite régie ou de ses partenaires publicitaires, concerne la diffusion publicitaire et n'impacte pas la fourniture d'un service de moteur de recherche aux utilisateurs. Les cookies ayant cette finalité ne remplissent aucune des conditions prévues pour les deux exceptions de l'article 82 de la loi Informatique et libertés, dès lors notamment que la publicité n'est pas le service demandé par l'utilisateur, et nécessitent le consentement de l'utilisateur.

CNIL, FR, 19 décembre 2022, Sanction, Société X, n° SAN-2022-023, publié, points 50, 52-53

Plateforme en ligne – Caractère libre, spécifique, éclairé et univoque du consentement – Dispositif ne permettant pas de refuser les cookies soumis à consentement aussi facilement qu'il est possible de les accepter – Visibilité très faible du bouton permettant de refuser le dépôt de cookies – Manquement – Article 82 loi Informatique et libertés

Pour être valable, le consentement de l'utilisateur doit être donné de manière libre, spécifique, éclairée et univoque, et ce, conformément à l'article 4.11 du RGPD. À ce titre, les solutions mises à la

disposition de l'utilisateur pour refuser les opérations de lecture et/ou d'écriture d'informations dans le terminal des utilisateurs doivent présenter le même degré de simplicité que celles prévues pour en accepter l'usage.

Lorsque le lien permettant de refuser le dépôt de cookies soumis à consentement bénéficie d'une visibilité très faible au regard de la visibilité du bouton permettant de l'accepter, un tel dispositif ne permet pas de refuser les cookies soumis à consentement aussi facilement qu'il est possible de les accepter, et constitue un manquement à l'article 82 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée.

Tel est le cas d'un lien permettant de refuser le dépôt de cookies qui n'est en actif que sur un seul mot d'une phrase, sans mise en valeur particulière, autre que le soulignement du lien, de sorte qu'un effort de recherche supplémentaire de la part de l'utilisateur est nécessaire pour voir ce lien hypertexte dissimulé et comprendre qu'il permet de refuser en un clic le dépôt de cookies sur son terminal ; et qu'à l'inverse, le bouton permettant d'accepter les cookies est isolé dans un cadre propre, parfaitement visible et identifiable et utilisant un contraste élevé entre la police du texte et la couleur du fond du bouton.

CNIL, P, 7 avril 2022, Mise en demeure, Société X, n° MED-2022-027, non publié

Voir aussi : CNIL, FR, 31 décembre 2021, Sanction, Société X, n°SAN-2021-024, publié

Plateforme en ligne – Mécanisme de refus des cookies – Complexité d'exprimer le refus – Altération de la liberté de choix – Manquement – Article 82 loi Informatique et libertés

Le fait, pour une plateforme en ligne, de rendre le mécanisme de refus des cookies plus complexe que celui consistant à les accepter revient en réalité à décourager les utilisateurs de refuser les cookies et à les inciter à privilégier la facilité du bouton « Tout accepter ». En effet, un utilisateur d'internet est généralement conduit à consulter de nombreux sites. La navigation sur internet se caractérise par sa rapidité et sa fluidité. Le fait de devoir cliquer sur « Personnaliser » et de devoir comprendre la façon dont est construite la page permettant de refuser les cookies est susceptible de décourager l'utilisateur, qui souhaiterait pourtant refuser le dépôt des cookies.

En l'espèce, les plateformes offrent un choix entre l'acceptation ou le refus des cookies, mais les modalités par lesquelles ce refus peut être exprimé, dans le contexte de la navigation sur internet, biaise l'expression du choix en faveur du consentement de façon à altérer la liberté de choix. En effet, les utilisateurs résidant en France se rendant sur les sites concernés doivent effectuer une seule action pour accepter les cookies, alors qu'ils doivent en effectuer cinq pour les refuser.

Au regard de ce qui précède, un manquement aux dispositions de l'article 82 de la loi Informatique et Libertés , interprétées à la lumière du RGPD, est constitué, dans la mesure où les plateformes ne mettent pas à disposition des utilisateurs situés en France, sur les sites internet concernés, un moyen de refuser les opérations de lecture et/ou d'écriture d'informations dans leur terminal présentant le même degré de simplicité que celui prévu pour en accepter l'usage.

CNIL, FR, 31 décembre 2021, Sanction, Sociétés X et Y, n°SAN-2021-023, publié, points 133, 135-136

Voir aussi : CNIL, FR, 31 décembre 2021, Sanction, Société X, n°SAN-2021-024, publié

Cookies – Obligations d'un éditeur de site web suite au retrait du consentement de l'utilisateur

Les utilisateurs ayant donné leur consentement à l'utilisation de traceurs doivent être mis en mesure de le retirer aussi simplement et à tout moment. Dès lors que les personnes retirent leur consentement, une société éditrice de site web, lorsqu'elle réalise techniquement le dépôt de cookies

et dispose de la maîtrise des requêtes réalisant les opérations de lecture et écriture sur ces cookies, doit s'assurer qu'il n'y a plus d'action de lecture ou d'écriture des cookies réalisée en violation du retrait du consentement de l'utilisateur, par exemple en effaçant le contenu desdits cookies ou en les rendant invalides à travers leur durée de validité.

CNIL, P, 14 octobre 2021, Mise en demeure, Société X, n° MED-2021-095, non publié

Cookies tiers – Responsabilité de l'éditeur du site internet qui les accueille – Cas où les cookies sont déposés sous le nom de domaine de l'éditeur – Mise en place de moyens adaptés

Au titre des obligations qui pèsent sur l'éditeur d'un site qui dépose des « cookies tiers », figurent celle de s'assurer auprès de ses partenaires, d'une part, qu'ils n'émettent pas, par l'intermédiaire de son site, des traceurs qui ne respectent pas la règlementation applicable en France et, d'autre part, celle d'effectuer toute démarche utile auprès d'eux pour mettre fin à des manquements. Cette obligation est une obligation de moyen, et non de résultat.

S'agissant de la responsabilité associée aux cookies déposés par des tiers sous le nom de domaine d'un éditeur de site web, pour que des opérations de lecture ou d'écriture d'informations puissent être effectuées par des tiers sous les noms de domaine de la société éditrice, ceci n'est en principe rendu possible que par l'inclusion par la société d'un fragment de code sur son site permettant aux tiers de déposer ou non un cookie.

Lorsqu'un éditeur de site web choisit ses partenaires et les autorise, à la fois juridiquement et par le codage informatique du site, à déposer des cookies sur les terminaux des utilisateurs et que, du fait de ce choix, le fonctionnement de son site ne lui permet pas de bloquer les cookies déposés par des tiers, cela n'exonère pas l'éditeur de sa responsabilité et il lui appartient de mettre en place des moyens adaptés au choix qu'il a opéré, tant dès l'arrivée de l'utilisateur sur le site qu'après avoir exprimé son refus.

En permettant que des opérations de lecture ou d'écriture d'informations puissent être effectuées par des tiers sous ses noms de domaine, l'éditeur d'un site web peut décider, si l'un de ses partenaires ne respecte pas la réglementation, de mettre en œuvre tous les moyens nécessaires pour faire cesser le manquement, puis, en dernier recours, de mettre fin à la relation du contrat ou d'engager des actions à son encontre. Lorsqu'une société constate qu'un de ses partenaires continue d'effectuer des opérations en violation des règles applicables malgré les outils qu'elle a mis en œuvre pour éviter cette situation et ses demandes ultérieures pour que de telles violations ne se reproduisent plus, il lui appartient d'envisager les différents moyens juridiques à sa disposition qui sont nécessaires pour faire cesser ces manquements, en prévoyant par exemple contractuellement la possibilité d'engager des actions contre ses partenaires (par exemple une action en responsabilité ou la suspension temporaire du contrat jusqu'au respect de ses engagements par le partenaire), et, en dernier recours, en appréciant l'opportunité de mettre un terme aux relations commerciales.

CNIL, FR, 27 juillet 2021, Sanction, Société X, n°SAN-2021-013, publié, points 52, 100-102

Voir aussi : CE, 10ème-9ème chambres réunies, 6 juin 2018, Société Éditions Croque Futur, n°412589, Rec.

6.5.4 Annuaire (article 12, ePrivacy)

1) Demande de suppression des données à caractère personnel d'un abonné – Droit à l'effacement – Application – 2) Mesures techniques et organisationnelles appropriées pour informer les responsables de traitement tiers concernés du retrait de

consentement de l'abonné – Application – 3) Mesures raisonnables afin d'informer les fournisseurs de moteurs de recherche de cette demande d'effacement des données – Application – 4) Consentement de la personne concernée à figurer dans des annuaires d'autres opérateurs que le sien – Consentement au sens de l'article 4, point 11, du RGPD – Application

1) L'article 17 du RGPD doit être interprété en ce sens que la demande d'un abonné tendant à la suppression de ses données à caractère personnel des annuaires constitue un recours au « droit à l'effacement » au sens de cet article.

2) L'article 5, paragraphe 2, et l'article 24 du RGPD doivent être interprétés en ce sens qu'une autorité de contrôle nationale peut exiger que le fournisseur d'annuaires, en tant que responsable du traitement, prenne les mesures techniques et organisationnelles appropriées pour informer les responsables du traitement tiers, à savoir l'opérateur de services téléphoniques qui lui a communiqué les données à caractère personnel de son abonné ainsi que les autres fournisseurs d'annuaires auxquels il a fourni de telles données, du retrait de consentement de cet abonné.

3) L'article 17, paragraphe 2, du RGPD, doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'une autorité de contrôle nationale ordonne à un fournisseur d'annuaires et de services de renseignements téléphoniques accessibles au public, auquel l'abonné d'un opérateur de services téléphoniques a demandé de ne plus publier les données à caractère personnel le concernant, de prendre des « mesures raisonnables », au sens de cette disposition, afin d'informer les fournisseurs de moteurs de recherche de cette demande d'effacement des données.

4) L'article 12, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 2, second alinéa, sous f), de cette directive et avec l'article 95 du RGPD, doit être interprété en ce sens que le « consentement », au sens de l'article 4, point 11, du RGPD, de l'abonné d'un opérateur de services téléphoniques est exigé afin que les données à caractère personnel de cet abonné figurent dans les annuaires et les services de renseignements téléphoniques accessibles au public publiés par des fournisseurs autres que cet opérateur, ce consentement pouvant être fourni soit audit opérateur soit à l'un de ces fournisseurs.

CJUE, 27 octobre 2022, Proximus, C-129/21

Fourniture de services de renseignements téléphoniques et d'annuaire – Réglementation nationale obligeant une entreprise attribuant des numéros de téléphone de transmettre à d'autres entreprises les données qu'elle détient concernant les abonnés d'entreprises tierces – Conditions de licéité

L'article 12 de la directive 2002/58/CE du 12 juillet 2002 (directive «vie privée et communications électroniques») doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale qui fait obligation à une entreprise publiant des annuaires publics de transmettre des données à caractère personnel qu'elle détient concernant les abonnés d'autres fournisseurs de services téléphoniques à une entreprise tierce dont l'activité consiste à publier un annuaire public imprimé ou électronique ou à rendre de tels annuaires consultables par l'intermédiaire de services de renseignements, sans qu'une telle transmission soit subordonnée à un nouveau consentement des abonnés, pour autant toutefois que, d'une part, ces derniers ont été informés avant la première inscription de leurs données dans un annuaire public de la finalité de celui-ci ainsi que du fait que ces données seraient susceptibles d'être communiquées à un autre fournisseur de services téléphoniques ; et que, d'autre part, il est garanti que lesdites données ne seront pas, après leur transmission, utilisées à des fins autres que celles pour lesquelles elles ont été collectées en vue de leur première publication.

CJUE, 5 mai 2011, Deutsche Telekom, C-543/09

Service d'annuaire recensant les données de médecins – 1) Données à caractère personnel – Existence – 2) Obligation de recueil du consentement préalable du professionnel concerné – Absence – 3) Obligation d'informer les personnes concernées des finalités et des conditions de mise en œuvre du traitement - Existence

1) Les données des médecins référencés sur un service d'annuaire, bien que déjà publiquement accessibles et d'ordre professionnel, sont des données personnelles. Dès lors, elles ne peuvent être réutilisées par les éditeurs de tels annuaires que dans le respect du règlement général sur la protection des données (RGPD).

2) À cet égard, la CNIL estime que lorsque ces annuaires consistent uniquement à référencer des professionnels et se limitent, par défaut (c'est-à-dire sauf intervention directe de ces derniers), à rediffuser les données « élémentaires » sur leur activité (données d'identité, spécialités / domaines d'expertise, coordonnées du lieu d'exercice de la profession, etc.) qui se trouvent publiées dans un format ouvert en vertu d'un cadre légal spécifique (en l'espèce, dans le cadre du « Répertoire partagé des professionnels intervenant dans le système de santé»), leur licéité n'est pas subordonnée au recueil d'un consentement préalable du professionnel concerné.

3) Pour autant, si un consentement n'est pas requis, les éditeurs d'annuaires doivent informer les personnes dont ils traitent les données des finalités qu'ils poursuivent et des conditions de mise en œuvre de leurs traitements. Une telle information permet aux personnes de conserver la maîtrise des usages qui sont faits de leurs données, en les mettant notamment en mesure d'exercer leurs droits, dont celui de pouvoir s'opposer à un tel traitement.

CNIL, P, 24 juillet 2024, mise en demeure, Société X, décision n° MED-2024-107, non publié

6.5.5 Communications non sollicitées (article 13, ePrivacy)

Prospection commerciale – Messages publicitaires sous la forme de courriers électroniques sans destinataire prédéterminé – Inclusion

Des messages publicitaires qui visent la promotion de services, diffusés sous la forme d'un courrier électronique, de telle sorte qu'ils apparaissent directement dans la boîte de réception de la messagerie électronique privée de l'utilisateur concerné permettent de qualifier ces messages de communications visant la prospection directe, au sens de l'article 13, paragraphe 1, de la directive 2002/58.

Le choix aléatoire ou prédéfini du destinataire ne constitue pas une condition de l'application de l'article 13, paragraphe 1, de la directive 2002/58. En d'autres termes, il importe peu que la publicité en cause soit adressée à un destinataire prédéterminé et individuellement identifié ou bien qu'il s'agisse d'une diffusion massive et aléatoire auprès de multiples destinataires. Ce qui importe est qu'il existe une communication à finalité commerciale qui atteint directement et individuellement un ou plusieurs utilisateurs de services de messagerie électronique en étant insérée dans la boîte de réception du compte de messagerie électronique de ces utilisateurs.

CJUE, 20 novembre 2021, StWL Städtische Werke Lauf a.d Pegnitz, C-102/20, points 53, 58-59

6.5.6 Notification des violations (régime ePrivacy)

Obligation des fournisseurs de services de communications électroniques accessibles au public d'informer la CNIL en cas de violation de données à caractère personnel (art. 34 bis de la loi du 6 janvier 1978) – 1) Moyen tiré de ce que cette obligation méconnaît l'art. 6-1 de la CEDH et les art. 47 et 48 de la Charte des droits

fondamentaux – Inopérance – 2) Moyen tiré de ce qu'une sanction prononcée à raison d'un manquement révélé du fait de cette obligation méconnaît ces mêmes stipulations – Opérance

1) Les dispositions de l'article 34 bis de la loi n°78-17 du 6 janvier 1978 imposent seulement aux fournisseurs de services de communications électroniques accessibles au public d'informer la CNIL et, le cas échéant, les personnes intéressées lorsqu'ils constatent une violation de données à caractère personnel. Elles n'ont ni pour objet ni pour effet de leur imposer de révéler des manquements qui leur seraient imputables. Un requérant ne saurait dès lors utilement soutenir qu'elles méconnaîtraient les stipulations du 1 de l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), qui garantissent le droit de ne pas contribuer à sa propre incrimination, et les articles 47 et 48 de la Charte des droits fondamentaux de l'Union européenne, qui garantissent le droit d'accéder à un tribunal impartial et les droits de la défense.

2) En revanche, un requérant peut utilement soutenir qu'une sanction prononcée par la CNIL contre un fournisseur de services de communications électroniques accessibles au public à raison d'un manquement révélé du fait de l'obligation prévue par les dispositions de l'article 34 bis méconnaît ces stipulations.

CE, 10ème/9ème SSR, 30 décembre 2015, Société Orange, n° 385019, T., point 7

6.5.7 Protection de la propriété intellectuelle

Accès à l'identité civile correspondant à des adresses IP par une autorité publique chargée de la protection des droits d'auteur – Conformité – Conditions

L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale qui autorise l'autorité publique chargée de la protection des droits d'auteur et des droits voisins contre les atteintes à ces droits commises sur Internet à accéder aux données, conservées par les fournisseurs de services de communications électroniques accessibles au public, relatives à l'identité civile correspondant à des adresses IP collectées préalablement par des organismes d'ayants droit, afin que cette autorité puisse identifier les titulaires de ces adresses, utilisées pour des activités susceptibles de constituer de telles atteintes, et puisse prendre, le cas échéant, des mesures à leur égard, à condition que, en vertu de cette réglementation,

– ces données soient conservées dans des conditions et selon des modalités techniques garantissant qu'il soit exclu que cette conservation puisse permettre de tirer des conclusions précises sur la vie privée de ces titulaires, par exemple en établissant leur profil détaillé, ce qui peut être accompli, en particulier, en imposant aux fournisseurs de services de communications électroniques une obligation de conservation des différentes catégories de données à caractère personnel, telles les données relatives à l'identité civile, les adresses IP ainsi que les données relatives au trafic et les données de localisation, garantissant une séparation effectivement étanche de ces différentes catégories de données empêchant, au stade de la conservation, toute exploitation combinée de ces différentes catégories de données, et pour une durée ne dépassant pas le strict nécessaire,

– l'accès de cette autorité publique à de telles données conservées de manière séparée et effectivement étanche serve exclusivement à identifier la personne soupçonnée d'avoir commis une infraction pénale et soit entouré des garanties nécessaires pour exclure que, hormis dans des situations atypiques, cet accès puisse permettre de tirer des conclusions précises sur la vie privée des

titulaires des adresses IP, par exemple en établissant leur profil détaillé, ce qui implique, en particulier, qu'il soit interdit aux agents de cette autorité autorisés à avoir un tel accès de divulguer, sous quelque forme que ce soit, des informations sur le contenu des fichiers consultés par ces titulaires, sauf à seules fins de saisir le ministère public, de procéder à un traçage du parcours de navigation de ces titulaires et, de manière plus générale, d'utiliser ces adresses IP à une fin autre que celle d'identifier leurs titulaires en vue de l'adoption d'éventuelles mesures contre ces derniers,

– la possibilité, pour les personnes chargées de l'examen des faits au sein de ladite autorité publique, de mettre en relation de telles données avec les fichiers comportant des éléments permettant de connaître le titre d'œuvres protégées dont la mise à disposition sur Internet a justifié la collecte des adresses IP par des organismes d'ayants droit, soit subordonnée, dans des hypothèses de nouvelle réitération d'une activité portant atteinte aux droits d'auteur ou aux droits voisins par une même personne, à un contrôle par une juridiction ou une entité administrative indépendante, lequel ne peut être entièrement automatisé et doit intervenir préalablement à une telle mise en relation, cette dernière étant susceptible, dans de telles hypothèses, de permettre que soient tirées des conclusions précises sur la vie privée de ladite personne dont l'adresse IP a été utilisée pour des activités pouvant porter atteinte aux droits d'auteur ou aux droits voisins,

– le système de traitement de données utilisé par l'autorité publique fasse l'objet, à intervalles réguliers, d'un contrôle par un organisme indépendant et ayant la qualité de tiers par rapport à cette autorité publique visant à vérifier l'intégrité du système, y compris les garanties effectives contre les risques d'accès et d'utilisation abusifs ou illicites de ces données, ainsi que son efficacité et sa fiabilité pour détecter les éventuels manquements.

CJUE, assemblée plénière, 30 avril 2024, La Quadrature du Net, C-470/21

Notion de traitement de données à caractère personnel – Enregistrement, par un titulaire de droits de propriété intellectuelle ou par un tiers, d'adresses IP d'utilisateurs d'un réseau de pair à pair aux fins d'une action en indemnisation – Inclusion – Condition de licéité – Demande justifiée, proportionnée et non abusive formulée sur le fondement d'une mesure législative nationale qui limite la portée de certains droits et obligations au sens de l'article 15§1 de la directive ePrivacy

L'article 6, paragraphe 1, premier alinéa, sous f), du RGPD, lu en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002 (directive vie privée et communications électroniques), doit être interprété en ce sens qu'il ne s'oppose, en principe, ni à l'enregistrement systématique, par le titulaire de droits de propriété intellectuelle ainsi que par un tiers pour son compte, d'adresses IP d'utilisateurs de réseaux de pair à pair (peer-to-peer) dont les connexions internet ont été prétendument utilisées dans des activités contrefaisantes ni à la communication des noms et des adresses postales de ces utilisateurs à ce titulaire ou à un tiers afin de lui permettre d'introduire un recours en indemnisation devant une juridiction civile pour un dommage prétendument causé par lesdits utilisateurs, à condition toutefois que les initiatives et les demandes en ce sens dudit titulaire ou d'un tel tiers soient justifiées, proportionnées et non abusives et trouvent leur fondement juridique dans une mesure législative nationale, au sens de l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, qui limite la portée des règles énoncées aux articles 5 et 6 de cette directive, telle que modifiée.

CJUE, 17 juin 2021, M.I.C.M., C-597/19

Communication au titulaire d'un droit d'auteur ou à son ayant droit de l'identité de l'abonné dont l'adresse IP a servi à l'atteinte audit droit – Législation permettant à une juridiction de communiquer des données à caractère personnel – Licéité – Conditions

Les directives 2002/58/CE du 12 juillet 2002 (directive vie privée et communications électroniques), et 2004/48 (droits de propriété intellectuelle) ne s'opposent pas à une législation nationale qui, aux fins d'identification d'un abonné Internet ou d'un utilisateur d'Internet, permet d'enjoindre à un fournisseur d'accès Internet de communiquer au titulaire d'un droit d'auteur ou à son ayant droit l'identité de l'abonné à qui une adresse IP (protocole internet) qui aurait servi à l'atteinte audit droit a été attribuée, dans la mesure où cette législation permet, à la juridiction nationale saisie d'une demande d'injonction de communiquer des données à caractère personnel, introduite par une personne ayant qualité pour agir, de pondérer, en fonction des circonstances de chaque espèce et en tenant dûment compte des exigences résultant du principe de proportionnalité, les intérêts opposés en présence.

CJUE, 19 avril 2012, Bonnier Audio e.a., C-461/10

6.5.8 Limitations, conservation et accès aux données de connexion

Directive 2002/58/CE – Article 15, paragraphe 1 - Faculté pour les États membres de limiter la portée de certains droits et obligations – Décision judiciaire autorisant l'interception, l'enregistrement et le stockage des conversations téléphoniques de personnes suspectées d'avoir commis une infraction pénale – Exigence de motivation – Portée

L'article 15, paragraphe 1, de la directive 2002/58/CE lu à la lumière de l'article 47, deuxième alinéa, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il ne s'oppose pas à une pratique nationale en vertu de laquelle les décisions judiciaires autorisant le recours à des techniques spéciales de renseignement à la suite d'une demande motivée et circonstanciée des autorités pénales sont rédigées au moyen d'un texte préétabli et dépourvu de motifs individualisés, mais se limitant à indiquer, outre la durée de validité de l'autorisation, que les exigences prévues par la législation dont ces décisions font mention, sont respectées, à condition que les raisons précises pour lesquelles le juge compétent a considéré que les exigences légales étaient respectées au regard des éléments factuels et juridiques caractérisant le cas d'espèce puissent être inférées aisément et sans ambiguïté d'une lecture croisée de la décision et de la demande d'autorisation, cette dernière devant être rendue accessible, postérieurement à l'autorisation donnée, à la personne contre laquelle le recours à des techniques spéciales de renseignement a été autorisé.

CJUE, 16 février 2023, HYA e.a., C-349/21

Accès à des données de connexion demandé par une autorité nationale compétente à des fins de poursuites d'infractions de vols avec circonstances aggravantes – Notion d'"infraction grave" - Définition – Compétence des États membres – Principe de proportionnalité – Étendue du contrôle préalable du juge sur les demandes d'accès aux données conservées par les fournisseurs de services de communications électroniques

L'article 15, paragraphe 1, de la directive vie privée et communications électroniques (2002/58/CE) modifiée, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il ne s'oppose pas à une disposition nationale qui impose au juge national, intervenant dans le cadre d'un contrôle préalable effectué à la suite d'une demande motivée d'accès à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de permettre de tirer des conclusions précises sur la vie privée d'un utilisateur d'un moyen de communication électronique, conservées par les fournisseurs de services de communications électroniques, présentée par une autorité nationale compétente dans le cadre d'une enquête pénale, d'autoriser cet accès si celui-ci est demandé aux fins

de la recherche d'infractions pénales punies, par le droit national, d'une peine de réclusion maximale d'au moins trois ans, sous réserve qu'il existe des indices suffisants de telles infractions et que ces données soient pertinentes pour constater les faits, à condition, toutefois, que ce juge soit habilité à refuser ledit accès si ce dernier est sollicité dans le cadre d'une enquête portant sur une infraction qui n'est manifestement pas grave, au regard des conditions sociétales prévalant dans l'État membre concerné.

CJUE, grande chambre, 30 avril 2021, Procura della Repubblica presso il Tribunale di Bolzano, C-178/22

Article 15, paragraphe 1, directive 2002/58/CE – 1) Législation permettant l'accès d'autorités publiques aux données de trafic et de localisation – Prévention, recherche, détection, poursuite d'infractions pénales – Illicéité en l'absence de limitation à certaines procédures – 2) Réglementation donnant compétence au ministère public pour autoriser l'accès d'une autorité publique aux données de trafic et de localisation – Illicéité

L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002 (directive vie privée et communications électroniques), lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens :

> 1) qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période ;
> 2) qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale.

CJUE, grande chambre, 2 mars 2021, Prokuratuur, C-746/18

---

1) Directive 2002/58 – Champ d'application – Réglementation nationale imposant aux fournisseurs de services de communications électroniques de transmettre des données relatives au trafic et à la localisation aux services de sécurité et de renseignement – Objectif de protection de la sécurité nationale – Inclusion – 2) Faculté pour les États membres de limiter la portée de certains droits et obligations – Réglementation nationale imposant aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et à la localisation aux services de sécurité et de renseignement – Objectif de protection de la sécurité nationale – Exclusion

1) L'article 1er, paragraphe 3, l'article 3 et l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

(directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lus à la lumière de l'article 4, paragraphe 2, TUE, doivent être interprétés en ce sens que relève du champ d'application de cette directive une réglementation nationale permettant à une autorité étatique d'imposer aux fournisseurs de services de communications électroniques de transmettre aux services de sécurité et de renseignement des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale.

2) L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement.

CJUE, grande chambre, 6 octobre 2020, Privacy International, C-623/17

Accès des autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé – Ingérence dans les droits fondamentaux desdits titulaires – Limitation à la lutte contre la criminalité grave – Absence

L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002 (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

CJUE, grande chambre, 2 octobre 2018, Ministerio Fiscal, C-207/16

Conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation – 1) Incompatibilité avec le droit de l'Union – 2) Accès des autorités nationales – Absence de contrôle préalable par une juridiction ou une autorité administrative indépendante – Absence d'exigence de conservation au sein de l'Union – Incompatibilité avec le droit de l'Union

1) L'article 15, paragraphe 1, de la directive 2002/58/CE du 12 juillet 2002 s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.

2) L'article 15, paragraphe 1, de la directive 2002/58/CE du 12 juillet 2002 s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.

CJUE, grande chambre, 21 décembre 2016, Tele2 Sverige, C-203/15, C-698/15

Conservation des données à caractère personnel pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales – Conservation générale et indifférenciée – Non-conformité

Compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les utilisateurs de services de communications électroniques ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée.

Des dispositions législatives autorisant, dans le but de permettre la mise à disposition de l'autorité judiciaire, la conservation générale et indifférenciée des données de connexion, applicable de façon générale à tous les utilisateurs des services de communications électroniques et indifféremment sur toutes les données de connexion relatives à ces personnes, quelle qu'en soit la sensibilité et sans considération de la nature et de la gravité des infractions susceptibles d'être recherchées, portent une atteinte disproportionnée au droit au respect de la vie privée et doivent être déclarées contraires à la Constitution.

CC, 2021-976/977 QPC, 25 février 2022, M. Habib A. et autre, points 11-13

Dérogation à l'obligation de confidentialité des données à caractère personnel et des données relatives au trafic – Conservation généralisée et indifférenciée – 1) Données relatives à l'identité civile, aux paiements effectués en ligne – Conditions – 2) Adresses IP – Conditions – 3) Données de trafic et de localisation autres que les adresses IP – Exclusion en principe – Conditions le cas échéant – 4) Conservation rapide des données de trafic et de localisation imposée par les autorités – Conditions

Les États-membres de l'UE sont autorisés, pour des motifs tenant à la sauvegarde de la sécurité nationale, à la sûreté de l'État ou à la lutte contre les infractions pénales, à prévoir une dérogation à l'obligation de confidentialité des données à caractère personnel et à celle de confidentialité des données relatives au trafic y afférentes, qui découlent de l'article 5, paragraphe 1, de la directive 2002/58/CE du 12 juillet 2002 et des articles 12 à 22 du RGPD.

1) Les données relatives à l'identité civile des utilisateurs de moyens de communications électroniques ainsi que les informations fournies lors de la souscription d'un contrat ou lors de la création d'un compte par un utilisateur et celles relatives aux paiements effectués en ligne listées aux 3° et 4° de l'article 1er du décret n° 2011-219 du 25 février 2011 peuvent faire l'objet, sans limitation de durée, d'une conservation généralisée et indifférenciée pour les besoins de toute procédure pénale, de la prévention de toute menace contre la sécurité publique et de la sauvegarde de la sécurité nationale.

2) Les adresses IP attribuées à la source d'une connexion peuvent faire l'objet d'une obligation de conservation généralisée et indifférenciée à des fins de lutte contre la criminalité grave ou de prévention des menaces graves contre la sécurité publique, pour une période temporellement limitée au strict nécessaire. Cette durée a pu être légalement être fixée à un an.

3) Les données de trafic et de localisation autres que les adresses IP ne peuvent pas faire l'objet d'une obligation de conservation généralisée et indifférenciée aux fins de lutte contre la criminalité, même grave. En revanche, une telle obligation peut être définie, sous réserve qu'une décision soumise à un contrôle effectif constate l'existence d'une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. La durée de cette conservation doit être limitée au strict nécessaire mais est renouvelable en cas de persistance de la menace. Dès lors que la France fait face, à la date de la décision, à une telle menace au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure, une telle obligation de conservation pouvait

légalement être édictée. En revanche, l'évaluation de la menace doit faire l'objet d'un réexamen périodique, qui ne saurait excéder un an.

4) Les autorités peuvent en revanche imposer aux opérateurs de communications électroniques et aux fournisseurs d'accès à internet de procéder, aux fins de lutte contre la criminalité grave, à la conservation rapide des données de trafic et de localisation qu'ils détiennent, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale. Les données ayant fait l'objet d'une conservation rapide peuvent non seulement appartenir aux personnes soupçonnées d'avoir commis ou projeté une infraction pénale ou une atteinte à la sécurité nationale, mais également à d'autres personnes, pour autant qu'elles peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation de cette infraction ou de cette atteinte à la sécurité nationale. La durée de conservation de ces données doit être limitée au strict nécessaire, dans une limite maximale de quatre-vingt-dix jours, renouvelable le cas échéant.

La gravité des infractions susceptibles de justifier la conservation généralisée et indifférenciée des adresses IP et la conservation rapide des données de trafic et de localisation a vocation à s'apprécier de façon concrète, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce, dans le respect du principe de proportionnalité rappelé à l'article préliminaire du code de procédure pénale. Elle ne saurait se rattacher à une liste exhaustive d'infractions prédéfinies en droit pénal.

CE, Assemblée, 21 avril 2021, French Data Network et autres, n°393099, Rec., points 35, 37-41, 55, 38

6.6 Règles en matière de prospection

Prospection téléphonique non soumise au consentement préalable de la personne – 1) Obligation d'informer au plus tard lors de l'appel téléphonique – 2) Forme de l'information prévue par le RGPD

1) Il résulte de l'article 14 du RGPD que, lorsqu'un prospecteur récupère un numéro de téléphone d'un tiers, par exemple un fournisseur d'accès à internet (FAI), à des fins de prospection par voie téléphonique, il doit informer la personne prospectée du traitement de ces données pour cette finalité, au plus tard lors de l'appel téléphonique.

2) Lorsqu'une information prévue par le RGPD est fournie dans le cadre d'échanges téléphoniques, il est admis que cette information puisse se limiter aux éléments les plus importants pour l'interlocuteur, afin de rester brève, à condition d'indiquer un moyen d'obtenir les informations complètes (exemples : touche à activer sur le téléphone, courriel reçu par l'interlocuteur, renvoi vers une page web). L'information sur le traitement des données transmises par les FAI, notamment les coordonnées téléphoniques des personnes, à des fins de prospection téléphonique, en application de l'article 14 du RGPD, et celle relative à l'enregistrement de la conversation, en application de l'article 13 du RGPD, peuvent par ailleurs être fusionnées.

CNIL, FR, 12 octobre 2023, Sanction, Société X, n° SAN-2023-015, publié, point 59

Voir aussi : CNIL, FR, 23 juin 2022, Sanction, n° SAN-2022-011, publié ; CNIL, FR, 24 novembre 2022, Sanction, n° SAN-2022-021, publié

Opposition à la prospection – 1) Liste repoussoir – Données nécessaires pour la prise en compte de l'opposition – 2) Conservation de la civilité, du nom/prénom, date de naissance, numéro de téléphone, adresse électronique, ville ou code postal, niveau

d'imposition et situation familiale des prospects ayant exercé leur droit d'opposition – Illicéité

Conservation des données d'opposition d'une personne à recevoir de la prospection commerciale.

1) Afin d'assurer l'effectivité du droit d'opposition, le responsable de traitement peut créer une « liste repoussoir » lui permettant de ne pas utiliser à nouveau les données de contact si elles venaient à lui être transmises à nouveau par une autre personne que la personne concernée. La CNIL recommande de conserver l'inscription à la « liste repoussoir » de la personne ayant fait opposition pendant une durée minimale de trois ans et de ne conserver que les empreintes de l'adresse ou du numéro utilisé pour la prospection. Cela permet de prendre en compte l'opposition dans le temps sans conserver de données directement identifiantes.

2) En l'espèce, la liste repoussoir comprenait la civilité, le nom, le prénom, la date de naissance, le numéro de téléphone, l'adresse électronique, la ville ou le code postal, le niveau d'imposition et la situation familiale alors que l'ensemble de ces données n'apparaissaient pas nécessaires au regard de la finalité liée à la prise en compte de l'opposition des prospects à recevoir de la prospection. Seules les données nécessaires à la prise en compte de l'opposition dans le temps et qui correspondent l'espèce au numéro de téléphone et à l'adresse électronique de la personne concernée auraient dû être conservées sous une forme hachée. Il en résulte une méconnaissance de l'article 5-1-c) du RGPD.

CNIL, P, 26 juin 2023, Mise en demeure, Société X, n°MED-2023-040, non publié

Enregistrement systématique des appels téléphoniques entre téléopérateurs et prospects – Finalité d'établissement d'une preuve du contrat éventuellement conclu – Caractère non nécessaire si obligation d'une confirmation écrite de l'offre

Un responsable du traitement, qui souhaite enregistrer des conversations téléphoniques à des fins probatoires, doit démontrer qu'il ne dispose pas d'autres moyens moins intrusifs pour prouver que le contrat conclu à distance a bien a été conclu avec la personne concernée.

En application de l'article L.221-16 du code de la consommation, dès lors que la preuve de la souscription d'un contrat conclu à distance, à la suite d'un démarchage téléphonique, peut être apportée par la confirmation écrite de l'offre, l'enregistrement des conversations téléphoniques, passées entre les téléopérateurs et les prospects, à des fins de preuve de la formation du contrat, n'apparait pas nécessaire.

CNIL, FR, 8 juin 2023, Sanction, Société X, n° SAN-2023-008, publié, points 31-34

---

1) Revente de données à des partenaires commerciaux à des fins de prospection commerciale par voie électronique – Exigence d'un consentement – 2) Utilisation ultérieure des données à des fins de prospection commerciale par voie électronique – Exigence d'un consentement – Article L. 34-5 du code des postes et des communications électroniques

1) Pour vendre les données à des partenaires afin qu'ils les utilisent pour de la prospection commerciale par voie électronique, un responsable du traitement doit recueillir, sur le support de collecte des données, le consentement libre, spécifique, informé et univoque par lequel les personnes concernées acceptent, par une déclaration ou un acte positif clair, une telle transmission de leurs données.

2) Le consentement à la revente des données ne dispense pas que le consentement des personnes soit également recueilli, en application de l'article L. 34-5 du code des postes et des communications électroniques (CPCE), pour l'utilisation de leurs données à des fins de prospection commerciale par

voie électronique. Ce consentement à la réception de prospection peut soit être recueilli par les opérateurs ayant acheté ou reçu les données et qui les utiliseront concrètement pour envoyer des messages de prospection, soit par le primo-collectant qui souhaite les transmettre à des partenaires. Dans ce dernier cas, ce consentement peut alors être recueilli globalement pour la transmission et la prospection commerciale, mais cela implique que le primo-collectant puisse fournir la liste exhaustive des partenaires ainsi autorisés, comme responsables de traitement, à utiliser les données pour de la prospection électronique.

CNIL, P, 1er décembre 2021, Mise en demeure, Société X, n° MED-2021-131, non publié

Voir aussi : CNIL, SP, 23 septembre 2021, Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales, n°2021-131, publié

Exception permettant la prospection sans consentement préalable – Article L. 34-5 du CPCE – Création d'un compte sur une plateforme de vente en ligne en l'absence d'achat – Exclusion

La création d'un compte sur une plateforme de vente en ligne ne préjuge pas de la commande éventuelle de produits auprès de cette plateforme. En l'absence d'achat, la plateforme de vente en ligne ne peut utilement invoquer le bénéfice de l'exception, créée par l'article L. 34-5 du code des postes et des communications électroniques (CPCE), permettant la prospection sans consentement préalable lorsque les coordonnées du destinataire ont été recueillies auprès de lui à l'occasion d'une vente ou d'une prestation de services si la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale.

Dès lors, il appartient à la plateforme de vente en ligne de recueillir le consentement préalable, libre, spécifique et informé des personnes créant un compte sur le site web de la société sans avoir procédé à un achat, à recevoir des messages de prospection directe par courriers électroniques, conformément à l'alinéa 1 de l'article L. 34-5 du CPCE.

CNIL, FR, 14 juin 2021, Sanction, Société X, n° SAN-2021-008, publié, points 94-95

6.6.1 Transmission et vente de bases de données à des fins de prospection commerciale

1) Vente de base de données personnelles – Conditions de licéité – Compatibilité des finalités d'usage de l'acheteur – Base légale – 2) Revente d'une base de données à des fins de prospection commerciale en cas de liquidation – a) Licéité – Existence – b) Bases légales mobilisables – i) Par voie électronique – Information des personnes et recueil de leur consentement préalable – ii) Par voie postale/téléphonique – Intérêt légitime – Information des personnes et possibilité de s'opposer – c) Synthèse

1) La transmission de données personnelles à des tiers (qui en sont alors destinataires au sens du RGPD), lorsqu'elle ne constitue pas un moyen d'atteindre la finalité initialement prévue pour le traitement de ces données, n'est en principe possible que si elle est compatible avec cette finalité première. En particulier, dans le cas d'une vente d'une base de données, l'appréciation de cette compatibilité nécessite, sauf exception, que le vendeur connaisse la finalité pour laquelle la base de données sera utilisée par l'acheteur et ne vende la base que pour cet usage. L'appréciation de la nécessité d'un consentement se fait au cas par cas.

2) a) S'agissant de la revente d'une base de données de clients ou prospects d'une société en situation de liquidation, en vue de sa réutilisation à des fins de prospection commerciale, la CNIL considère que, eu égard à la finalité initiale de la base de données et du contexte de liquidation de l'entreprise, cette vente peut en principe être regardée comme compatible avec le traitement initial des données. Un consentement peut cependant être requis en raison des règles spécifiques à la prospection par voie électronique.

b) Les bases légales mobilisables pour la transmission, à titre onéreux ou non, de données à caractère personnel à des partenaires commerciaux souhaitant les réutiliser à des fins commerciales dépendent du canal utilisé pour la prospection faite par ces partenaires : prospection par voie électronique ou prospection par voie postale/téléphonique.

i) Si la transmission a pour finalité de permettre aux partenaires commerciaux de réaliser de la prospection électronique qui nécessite le recueil du consentement préalable des personnes en application des dispositions de l'article L.34-5 du code des postes et des communications électroniques, l'organisme transmettant les données doit informer les personnes concernées et recueillir leur consentement à cette transmission en application de l'article 6-1-a du RGPD.

ii) Si la transmission a pour finalité de permettre aux partenaires commerciaux de réaliser de la prospection sur la base de leur intérêt légitime (prospection non électronique, c'est-à-dire réalisée par voie téléphonique ou postale), elle peut elle-même être réalisée sur le fondement de l'intérêt légitime en application de l'article 6-1-f du RGPD. Dans ce cadre, l'organisme transmettant les données doit informer les personnes concernées de la finalité de cette transmission et des catégories de partenaires rendus destinataires des données et offrir aux personnes concernées, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais et de manière simple, à la transmission de leurs données à caractère personnel.

c) Il résulte de l'ensemble de ces exigences que la vente d'une base de données clients à des fins de prospection commerciale par l'acquéreur n'est possible que si :

- la base est vendue spécifiquement pour cette finalité, et non pour tout usage des données ;
- il est prévu d'informer les personnes dont les données figurant dans la base de données de la vente ;
- ces personnes vont, selon le cas, soit donner leur consentement, soit pouvoir s'opposer à figurer dans la base vendue.

CNIL, P, 27 avril 2023, Rappel aux obligations, Société X, n°RAL231017, non publié

6.7 Travail

Article 88 du RGPD – 1) Diffusion en direct par vidéoconférence de cours d'enseignement public – Traitement de données à caractère personnel des enseignants – Champ d'application – Inclusion – 2) Règlementation nationale « plus spécifique» – Conditions – 3) Dispositions nationales prises pour assurer la protection des droits et des libertés des employés dans le cadre de relations de travail – Absence sauf lorsque lesdites dispositions constituent une base juridique valide au sens de l'article 6, paragraphe 3, du RGPD

1) Le traitement des données à caractère personnel d'enseignants, à l'occasion de la diffusion en direct par vidéoconférence des cours d'enseignement public qu'ils délivrent, relève du champ d'application matériel du RGPD et entre dans le champ d'application de l'article 88 de ce règlement qui vise le traitement des données à caractère personnel des employés dans le cadre des relations de travail.

2) L'article 88 du RGPD doit être interprété en ce sens qu'une réglementation nationale ne peut constituer une « règle plus spécifique », au sens du paragraphe 1 de cet article, dans le cas où elle ne remplit pas les conditions posées au paragraphe 2 dudit article.

3) L'article 88, paragraphes 1 et 2, du RGPD doit être interprété en ce sens que l'application de dispositions nationales prises pour assurer la protection des droits et des libertés des employés en ce qui concerne le traitement de leurs données à caractère personnel dans le cadre de relations de travail doit être écartée lorsque ces dispositions ne respectent pas les conditions et les limites prescrites par cet article 88, paragraphes 1 et 2, à moins que lesdites dispositions constituent une base juridique visée à l'article 6, paragraphe 3, de ce règlement qui respecte les exigences prévues par celui-ci.

CJUE, 30 mars 2023, Hauptpersonalrat der Lehrerinnen und Lehrer, C-34/21, point 56

Articles 6 et 7 directive 95/46/CE – Réglementation nationale obligeant l'employeur à mettre à disposition de l'autorité nationale le registre du temps de travail – Licéité sous conditions

Les articles 6, paragraphe 1, sous b) et c), ainsi que 7, sous c), de la directive 95/46 ne s'opposent pas à une réglementation nationale qui impose à l'employeur l'obligation de mettre à la disposition de l'autorité nationale compétente en matière de surveillance des conditions de travail le registre du temps de travail afin d'en permettre la consultation immédiate, pour autant que cette obligation est nécessaire aux fins de l'exercice par cette autorité de ses missions de surveillance de l'application de la réglementation en matière de conditions de travail, notamment, en ce qui concerne le temps de travail.

CJUE, 30 mai 2013, Worten, C-342/12

Système de contrôle des antécédents personnels et politiques pour les titulaires ou les candidats à des postes importants pour la sécurité nationale – Garanties spéciales prévues par la législation nationale – Absence de violation de l'article 8 CEDH

La Suède a instauré un système de contrôle du personnel pour les titulaires de postes importants pour la sécurité nationale ou les candidats à de tels postes. Ce système consiste en la collecte d'informations tirées de registres de police. Une ordonnance détaille les conditions de collecte et contient des dispositions explicites et détaillées sur la nature des renseignements pouvant être communiqués (antécédents personnels ou politiques), les autorités destinataires, les circonstances de pareille communication et la procédure que le Conseil national de la police, organe compétent pour décider de la communication desdites informations, doit suivre avant de se décider.

La Cour EDH affirme que la mémorisation et la communication des données relative à la vie privée, assorties du refus d'accorder au requérant la faculté de les réfuter, portent atteinte à son droit au respect de sa vie privée, garanti par l'article 8 paragraphe 1 de la conv. EDH.

Si la Cour EDH reconnaît que le système mis en place poursuit un but légitime, la protection de la sécurité nationale, elle recherche si cette ingérence est « prévue par la loi » et « nécessaire dans une société démocratique ».

L'expression « prévue par la loi », au sens du paragraphe 2 de l'article 8 (art. 8-2), veut d'abord que l'ingérence ait une base en droit interne, mais l'observation de celui-ci ne suffit pas : la loi en cause doit être accessible à l'intéressé, qui en outre doit pouvoir en prévoir les conséquences pour lui (voir, mutatis mutandis, l'arrêt Malone du 2 août 1984, série A no 82, pp. 31-32, par. 66). En l'espèce, il existe des dispositions explicites et détaillées sur la nature des renseignements pouvant être communiqués, les autorités destinataires, les circonstances de pareille communication et la procédure que le Conseil national de la police doit suivre avant de s'y décider. Aussi, l'ingérence litigieuse était donc "prévue par la loi" au sens de l'article 8.

S'agissant du caractère « nécessaire dans une société démocratique », la notion de nécessité implique une ingérence fondée sur un besoin social impérieux, et notamment proportionnée au but légitime recherché. Les autorités nationales jouissent d'une marge d'appréciation dont l'ampleur dépend non seulement de la finalité, mais encore du caractère propre de l'ingérence. En l'occurrence, il échet de mettre en balance l'intérêt de l'État défendeur à protéger sa sécurité nationale avec la gravité de l'atteinte au droit du requérant au respect de sa vie privée.

La Cour admet, la marge dont l'État défendeur disposait pour apprécier en l'espèce le besoin social impérieux, et notamment pour choisir les moyens de sauvegarder la sécurité nationale, revêtait une grande ampleur. Néanmoins, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre (arrêt Klass et autres du 6 septembre 1978, série A no 28, pp. 23-24, paras. 49-50).

La Cour conclut ainsi, que les garanties dont s'entoure le système suédois de contrôle du personnel, par exemple la présence de parlementaires dans le Conseil national et le contrôle du ministre de la Justice, remplissent les exigences du paragraphe 2 de l'article 8. Vu sa grande marge d'appréciation, le gouvernement défendeur était en droit de considérer que les intérêts de la sécurité nationale prévalaient en l'occurrence sur les intérêts individuels du requérant. L'ingérence que M. Leander a subie ne saurait donc passer pour disproportionnée au but légitime poursuivi. La Cour EDH exclut la violation de l'article 8 de la CEDH

CEDH, 26 mars 1987, Affaire Leander c/ Suède, n°9248/81

Caractérisation du délit de collecte de données à caractère personnel par un moyen déloyal dans le cadre de rapports employeur/employés - Données disponibles en accès libre sur internet – Utilisation sans rapport avec l'objet de leur mise en ligne – Collecte à l'insu des personnes concernées – Méconnaissance de l'obligation d'information des personnes et de leur droit d'opposition

Dans le cadre de rapports employeur/employés, le fait d'effectuer des recherches sur des personnes portant sur des données à caractère personnel telles qu'antécédents judiciaires, renseignements bancaires et téléphoniques, véhicules, propriétés, qualité de locataire ou de propriétaire, situation matrimoniale, santé, déplacement à l'étranger est susceptible de constituer un moyen de collecte déloyal dès lors que, issues de la capture et du recoupement d'informations diffusées sur des sites publics tels que sites web, annuaires, forums de discussion, réseaux sociaux, sites de presse régionale, de telles données ont fait l'objet d'une utilisation sans rapport avec l'objet de leur mise en ligne et ont été recueillies à l'insu des personnes concernées, ainsi privées du droit d'opposition institué par la loi informatique et libertés.

En effet, le fait que les données à caractère personnel collectées en l'espèce par le prévenu aient été pour partie en accès libre sur internet ne retire rien au caractère déloyal de cette collecte, dès lors qu'une telle collecte, de surcroît réalisée à des fins dévoyées de profilage des personnes concernées et d'investigation dans leur vie privée, à l'insu de celles-ci, ne pouvait s'effectuer sans qu'elles en soient informées.

Cass, crim., 30 avril 2024, n°23-80.962, B., points 8,10

Utilisation par un employeur de messages envoyés au moyen de la messagerie professionnelle s'inscrivant dans le cadre d'échanges privés sans vocation à devenir publics et aux opinions exprimées sans incidence sur l'emploi ou les relations de travail – Disproportion – Inopposabilité au salarié des messages dans le cadre d'une procédure de licenciement

Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée de sorte qu'un motif tiré de la vie personnelle du salarié ne peut justifier, en principe, un licenciement disciplinaire, sauf s'il constitue un manquement de l'intéressé à une obligation découlant de son contrat de travail. Doit être approuvé l'arrêt de la cour d'appel qui retient que l'employeur ne peut, pour procéder au licenciement d'un salarié, se fonder sur le contenu de messages, qui, même s'ils avaient été envoyés au moyen de la messagerie professionnelle, relèvent de la vie personnelle du salarié dès lors, d'une part, que ces messages s'inscrivaient dans le cadre d'échanges privés, à l'intérieur d'un groupe de personnes, et n'avaient pas vocation à devenir publics, d'autre part, que les opinions exprimées par la salariée n'avaient eu aucune incidence sur son emploi ou ses relations avec les usagers ou ses collègues et qu'il n'est pas établi qu'ils auraient été connus en dehors du cadre privé.

Cass, soc., 6 mars 2024, n° 22-11.016

Mesure de communication de bulletins de salaire par le juge sur le fondement des articles 6 et 8 de la CESDH, de l'article 9 du code civil et de l'article 9 du code de procédure civile – Communication nécessaire à l'exercice ou à la défense d'un droit en justice – Licéité – Conditions

Il résulte du point (4) de l'introduction du RGPD, que le droit à la protection des données à caractère personnel n'est pas un droit absolu et doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité, en particulier le droit à un recours effectif et à accéder à un tribunal impartial. Selon l'article 145 du code de procédure civile, s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé. Il résulte par ailleurs des articles 6 et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 9 du code civil et 9 du code de procédure civile, que le droit à la preuve peut justifier la production d'éléments portant atteinte à la vie personnelle à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi. Doit en conséquence être approuvé l'arrêt qui ordonne à l'employeur de communiquer à une salariée les bulletins de salaires d'autres salariés occupant des postes de niveau comparable au sien avec occultation des données personnelles à l'exception des noms et prénoms, de la classification conventionnelle et de la rémunération, après avoir relevé que cette communication d'éléments portant atteinte à la vie personnelle d'autres salariés était indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, soit la défense de l'intérêt légitime de la salariée à l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail.

Cass, soc., 8 mars 2023, n° 21-12.492, points 5-10

Utilisation par un employeur d'un dispositif de vidéosurveillance filmant en permanence l'unique salarié de la société pour le contrôle des règles d'hygiène et de sécurité– Disproportion – Inopposabilité au salarié des enregistrements issus de cette vidéosurveillance dans le cadre d'une procédure de licenciement

Aux termes de l'article L. 1121-1 du code du travail, nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

La cour d'appel a constaté que le salarié, qui exerçait seul son activité en cuisine, était soumis à la surveillance constante de la caméra qui y était installée. Elle en a déduit à bon droit que les enregistrements issus de ce dispositif de surveillance, attentatoire à la vie personnelle du salarié et

disproportionné au but allégué par l'employeur de sécurité des personnes et des biens, n'étaient pas opposables au salarié et a, par ces seuls motifs, légalement justifié sa décision.

Cass, soc., 23 juin 2021, n°19-13.856, B., points 5-6

Utilisation par un employeur d'un système de géolocalisation pour le contrôle de la durée du travail de ses salariés – Caractère excessif – Existence, sauf lorsque ce contrôle ne peut pas être fait par un autre moyen, même moins efficace

Il résulte des articles 6 de la loi n° 78-17 du 6 janvier 1978 et L. 1121-1 du code du travail que l'utilisation par un employeur d'un système de géolocalisation pour assurer le contrôle de la durée du travail de ses salariés n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, fût-il moins efficace que la géolocalisation. En dehors de cette hypothèse, la collecte et le traitement de telles données à des fins de contrôle du temps de travail doivent être regardés comme excessifs au sens du 3° de l'article 6 de la loi du 6 janvier 1978.

CE, 10ème-9ème chambres réunies, 15 décembre 2017, Société Odeolis, n° 403776, Rec., point 7

Dispositif de vidéosurveillance plaçant sous surveillance permanente au moins un salarié – Disproportion

Est disproportionné et peut légalement faire l'objet d'une sanction un dispositif de vidéosurveillance plaçant sous surveillance en permanence au moins un salarié. En l'espèce, la circonstance que la société ait voulu lutter contre des vols susceptibles d'être perpétrés par ses propres salariés ne permet pas de considérer que le dispositif était proportionné alors qu'en outre il était installé dans des locaux sécurisés, dont l'entrée ne peut s'effectuer qu'après autorisation et vérification d'identité.

CE, 10ème/9ème SSR, 18 novembre 2015, Société PS Consulting, n° 371196, Inédit., points 9-12

Utilisation par un employeur d'un système de géolocalisation pour la protection des biens ainsi que le suivi et l'optimisation des tournées de livraison - Caractère excessif - Existence, sauf lorsque les employés ont la possibilité de désactiver la fonction de géolocalisation des véhicules pendant leurs temps de pause ou à l'issue de leur temps de travail

Dispositif géolocalisant les véhicules professionnels en permanence, afin de lutter contre le vol du véhicule et de sa cargaison, ainsi que pour permettre d'optimiser les tournées de livraison. La CNIL considère de façon constante que l'enregistrement en continu des données de géolocalisation d'un véhicule professionnel, sans possibilité pour les salariés de ne pas être géolocalisé en dehors de leurs horaires de travail, porte en principe une atteinte excessive à la liberté d'aller et venir et au droit à la vie privée des salariés. La commission recommande ainsi que les employés puissent avoir la possibilité de désactiver la fonction de géolocalisation des véhicules pendant leurs temps de pause ou à l'issue de leur temps de travail lorsque ces véhicules peuvent être utilisés à des fins privées durant ces périodes. Cette possibilité de désactivation n'empêche pas la société de réactiver le dispositif à distance, comme cela est parfois, possible, s'il a pour finalité de lutter contre le vol du véhicule.

CNIL, P, 29 mai 2024, Rappel aux obligations légales, Société X, n° ROL 2024-231459, non publié

Système automatisé de gestion d'un entrepôt de marchandises enregistrant chaque manipulation des objets par les salariés 1) a) Légalité en principe de la collecte des données et de leur utilisation en temps réel – b) Illégalité de certaines données excessives - i) Indicateur mesurant la vitesse d'exécution des actions d'un salarié assorti d'un indicateur d'erreur chaque fois qu'une tâche dépasse une durée de l'ordre d'une seconde – ii) Indicateur calculant les temps d'inactivité supérieurs à dix minutes pour chaque salarié – iii) Indicateur enregistrant les temps d'inactivité inférieurs à dix minutes pour chaque salarié – 2) Conservation de l'ensemble des données brutes remontées par les scanners et de tous les indicateurs associés pendant 31 jours – Méconnaissance du principe de minimisation.

Cas d'un système automatisé de gestion d'un très grand nombre de marchandises dans un entrepôt au moyen de scanners permettant de suivre toutes les manipulations des objets et les principales actions des salariés. Les données brutes des scanners sont conservées et permettent l'établissement d'un très grand nombre d'indicateurs individuels de qualité, de productivité et de temps de travail.

1) a) Lorsqu'un service rendu à des clients entraîne des contraintes exceptionnelles, en raison de volumes importants et de courts délais de livraison, un suivi très précis en temps réel de toutes les manipulations des objets dans un entrepôt et de la situation de chaque poste de travail, donc de chaque salarié, peut s'avérer nécessaire. Néanmoins, ce type de suivi entraîne le traitement d'un très grand nombre de données, dont beaucoup de données personnelles en temps réel, chaque fois qu'un colis est manipulé par un salarié dans le cadre de tâches directes. Aussi, si le traitement en temps réel par une société de données brutes et indicateurs pour la bonne gestion de stocks et de commandes ne saurait être remis en cause de façon générale, les indicateurs mobilisés dans ce cadre, sur le fondement de l'intérêt légitime de l'employeur, doivent répondre aux exigences de nécessité et de proportionnalité de l'article 6 du RGPD.

b) i) La collecte de données pour mesurer la rapidité d'exécution des actions d'un salarié lors de la réalisation de certaines tâches, en associant un indicateur d'erreur chaque fois que cette rapidité est inférieure à une certaine durée de l'ordre de la seconde, au motif que cette rapidité est en principe incompatible avec la bonne exécution desdites tâches, est de nature à exercer sur lui une surveillance continue. Ce type d'indicateur est intrusif et peut avoir des répercussions morales négatives sur les salariés. Une telle précision dans la surveillance dépasse les attentes raisonnables des salariés, qui peuvent s'attendre à une certaine surveillance de leur travail, mais pas à ce que leurs actions fassent l'objet d'une évaluation informatique à un rythme de l'ordre de la seconde. Par conséquent, le traitement de cet indicateur excède ce qui est admissible pour servir les intérêts légitimes de l'entreprise en matière de qualité et de sécurité dans ses entrepôts, car il porte atteinte de manière excessive aux droits et intérêts des salariés, notamment à leur vie privée et personnelle, ainsi qu'à leur droit à des conditions de travail respectueuses de leur santé et de leur sécurité. Absence de base légale du traitement.

ii) De façon similaire, la collecte d'un indicateur signalant les temps d'inactivité et de latence de chaque salarié supérieurs à dix minutes à tout moment de la journée présente un caractère intrusif important, car elle contraint en pratique le salarié à pouvoir justifier de tout temps considéré comme non productif. Le traitement de cet indicateur peut avoir des répercussions négatives sur le salarié en raison du suivi continu qu'il permet des temps très courts considérés comme non productifs. Un tel traitement, pour des finalités de gestion d'un entrepôt, d'exécution des commandes et de fourniture de conseils aux salariés, est disproportionné par rapport aux intérêts et droits fondamentaux des salariés, notamment leur droit à la protection de leur vie privée et personnelle ainsi qu'à des conditions de travail respectueuses de leur santé et de leur sécurité. La base légale de l'intérêt légitime ne peut donc être retenue.

iii) Il en va de même de la collecte d'un indicateur signalant les temps d'inactivité et de latence inférieurs à dix minutes de chaque salarié à certains moments de la journée (en particulier avant et après les pauses), laquelle est disproportionnée au regard des finalités de gestion d'un entrepôt,

d'exécution des commandes et de fourniture de conseils aux salariés. La base légale de l'intérêt légitime ne peut donc être retenue.

2) La conservation et l'utilisation, pour chaque salarié, de données aussi fines et riches que l'intégralité des données brutes remontées par les scanners, ainsi que l'ensemble des nombreux indicateurs associés mesurant diverses variables, y compris sur de courtes périodes (une heure), sur une profondeur de 31 jours, pour des finalités d'évaluations individuelles régulières des salariés et, s'agissant de la plupart de ces données, pour des finalités d'organisation du travail dans les entrepôts , ne sont ni nécessaires ni proportionnées, notamment dès lors que la société peut atteindre ces finalités sans conserver l'intégralité des données brutes sur 31 jours et en ayant recours à des statistiques individuelles de qualité et de productivité, par exemple hebdomadaires. La conservation et l'utilisation de l'ensemble de ces données méconnaît le principe de minimisation de l'article 5. 1. c) du RGPD et, en tout état de cause, porte une atteinte disproportionnée aux droits du salarié contraire à l'article 6 du RGPD.

CNIL, FR, 27 décembre 2023, Sanction, Société X, n° SAN 2023-021, publié

Surveillance des salariés – Télétravail – Recours à des dispositifs de surveillance automatisée constante ou quasi-constante – Surveillance permanente et disproportionnée des activités des salariés – Illicéité

Si le télétravail ne constitue qu'une modalité d'organisation de travail et que l'employeur conserve, au même titre que lorsque le travail est effectué dans les locaux de la société, le pouvoir d'encadrer et de contrôler l'exécution des tâches confiées à son salarié, la jurisprudence a en revanche rappelé de manière constante que ce pouvoir ne saurait être exercé de manière excessive. L'employeur doit donc toujours justifier que les dispositifs mis en œuvre sont proportionnés à l'objectif poursuivi et ne portent pas une atteinte excessive au respect des droits et libertés des salariés, particulièrement le droit au respect de leur vie privée.

À cet égard, la CNIL considère de manière constante qu'une surveillance automatisée permanente des salariés est excessive, sauf dans des cas exceptionnels dûment justifiés au regard de la nature de la tâche. Il en est de même dans le cadre du télétravail. La Commission considère ainsi que la surveillance constante ou quasi-constante au moyen de dispositifs vidéo, le partage permanent de l'écran ou l'utilisation d'enregistreurs de frappe (ou keyloggers), la surveillance de la fréquence des frappes de clavier et des clics de souris ou la prise de captures d'écran à intervalles réguliers, constituent des procédés particulièrement intrusifs et s'analysent en une surveillance permanente et disproportionnée des activités des salariés, y compris, en ce qu'ils peuvent conduire à la captation d'éléments d'ordre privé (courriels personnels, conversations de messageries instantanées ou de mots de passe confidentiels). Le recours à de tels dispositifs est susceptible de constituer un manquement à l'article 5-1-c du RGPD.

CNIL, P, 17 novembre 2023, Mise en demeure, Société X, décision n° MED 2023-102, non publié

Contrôle des horaires de travail – Principe de minimisation des données – Vie personnelle des salariés – 1) Recours à des « badgeuses », y compris avec un mécanisme d'authentification des salariés – Admissibilité – 2) Recours à des photographies systématiques au moment de la prise de poste – Inadmissibilité

Le traitement de données à caractère personnel sur lequel repose un dispositif de contrôle des horaires de travail, fondé sur l'intérêt légitime, doit respecter le principe de minimisation des données fixé à l'article 5-1-c du RGPD. Il ne doit, en outre, pas porter une atteinte disproportionnée à la vie personnelle des salariés, en application de l'article 6-1-f du RGPD et de l'article L. 1121-1 du code du travail.

1) La CNIL estime en principe adéquat le recours à des « pointeuses » à badge ou « badgeuses », qui enregistrent l'identifiant ou le nom rattaché au badge associés au jour et à l'heure de pointage de la personne utilisant le badge. Ces dispositifs prévoient parfois un mécanisme d'authentification des salariés par un numéro d'identification personnel - NIP (ou *Personal Identification Number - PIN*). De tels systèmes permettent en principe d'assurer un contrôle satisfaisant des horaires de travail des salariés.

2) En revanche, la CNIL estime en principe que le recours à des photographies systématiques au moment de la prise de poste soit méconnaît le principe de minimisation, dès lors que les badgeuses sans photographie suffisent généralement à atteindre les objectifs fixés, soit est disproportionné, dès lors que la lutte contre la fraude peut en principe être détectée par d'autres moyens, notamment par l'action du personnel encadrant auquel il appartient de s'assurer du respect des consignes par les salariés. Il n'en va autrement que lorsque la société fait valoir des circonstances particulières justifiant le recours à un contrôle par photographie, telles que des difficultés spécifiques de contrôles des salariés ayant badgé ou des cas de fraude massive.

CNIL, P, 13 avril 2023, Rappel aux obligations, Société X, n°RAL231017, non publié

Dispositif de vidéosurveillance de salariés – 1) a) Exigences de minimisation des données et de proportionnalité – b) Illicéité de la surveillance permanente d'un salarié, sauf exception – 2) Cas d'un dispositif filmant en permanence des traducteurs destiné à protéger des documents traduits

1) a) La mise en œuvre d'un système de vidéosurveillance de salariés n'est licite qu'à condition de ne collecter que les données nécessaires à l'objectif poursuivi et de ne pas porter une atteinte disproportionnée aux droits et libertés de ceux-ci, ainsi qu'en dispose l'article L. 1121-1 du code du travail. Le nombre, l'emplacement, l'orientation, les périodes de fonctionnement des caméras ou la nature des tâches accomplies par les personnes concernées, sont autant d'éléments à prendre en compte lors de l'installation du système.

b) Si la surveillance de zones sensibles peut être justifiée par des impératifs de sécurité, le placement sous surveillance permanente de salariés, attentatoire à leur vie privée, ne peut toutefois intervenir que dans des circonstances exceptionnelles tenant, par exemple, à la nature de la tâche à accomplir. Il en est ainsi lorsqu'un employé manipule des objets de grande valeur ou lorsque le responsable de traitement est à même de justifier de vols ou de dégradations commises sur ces zones.

2) En l'espèce, est manifestement disproportionnée l'utilisation d'un dispositif de vidéosurveillance conduisant à placer des traducteurs assermentés sous une surveillance permanente en vue de protéger des documents traduits. En effet, si la nature des documents peut justifier la mise en place de mesures particulières de protection, il convient d'envisager des procédés alternatifs tels que la sécurisation des accès sur le lieu de travail.

CNIL, FR, 13 juin 2019, Sanction, Société X, n°SAN-2019-006, publié, points 31-36

Dispositif de vidéosurveillance filmant en permanence des salariés – Locaux exigus – Justification – Absence en l'espèce

Le placement sous surveillance continue des postes de travail des salariés n'est possible que s'il est justifié par une situation particulière ou un risque particulier auxquels sont exposées les personnes objets de la surveillance. Il appartient au responsable du traitement de justifier de ces circonstances et de la proportionnalité du traitement. En l'espèce, l'utilisation de dispositifs de vidéoprotection et vidéosurveillance constitue une réponse adaptée au risque de sécurité qui pèse sur les salariés du groupe dont les établissements ont subi un nombre important de cambriolages. Néanmoins, quand bien même l'objectif de sécurité assigné au dispositif est parfaitement légitime, les seules difficultés

liées à l'exigüité des locaux ne peuvent justifier une atteinte disproportionnée à la vie privée des salariés ou leur mise sous surveillance constante.

CNIL, FR, 17 juillet 2014, Sanction, Société X, n°2014-307, publié, points 14-22

Voir aussi : CNIL, FR, 14 octobre 2014, Mise en demeure, Société X exploitant les magasins Y, n°2014-051, publié

6.8 Social

6.9 Traitements mis en œuvre à des fins journalistiques

Enregistrement et publication d'une vidéo de membres de la police dans un commissariat – Traitement de données à caractère personnel aux seules fins de journalisme à condition que l'enregistrement et la publication aient pour seule finalité la divulgation au public d'informations, d'opinions ou d'idées

L'article 9 de la directive 95/46 doit être interprété en ce sens que des circonstances de fait telles que celles de l'affaire au principal, à savoir l'enregistrement vidéo de membres de la police dans un commissariat, lors d'une prise de déposition, et la publication de la vidéo ainsi enregistrée sur un site Internet de vidéos sur lequel les utilisateurs peuvent envoyer, regarder et partager celles-ci, peuvent constituer un traitement de données à caractère personnel aux seules fins de journalisme, au sens de cette disposition, pour autant qu'il ressorte de ladite vidéo que ledit enregistrement et ladite publication ont pour seule finalité la divulgation au public d'informations, d'opinions ou d'idées, ce qu'il incombe à la juridiction de renvoi de vérifier.

CJUE, 14 février 2019, Buivids, C-345/17

6.10 Traitements de données à caractère personnel accessibles publiquement

Publicité obligatoire de documents dans le registre du commerce - Données non obligatoires - Droit à l'effacement – Conditions – Fourniture d'un document occulté – Absence

La directive 2017/1132 relative à certains aspects du droit des sociétés, en particulier l'article 16 de celle-ci, ainsi que l'article 17 du règlement 2016/679 du 27 avril 2016 (RGPD) doivent être interprétés en ce sens qu'ils s'opposent à une réglementation ou à une pratique d'un État membre conduisant l'autorité chargée de la tenue du registre du commerce de cet État membre à refuser toute demande d'effacement des données à caractère personnel, non requises par cette directive ou par le droit dudit État membre, figurant dans un contrat de société publié dans ce registre, lorsqu'une copie de ce contrat occultant ces données n'a pas été fournie à cette autorité, contrairement aux modalités procédurales prévues par cette réglementation.

CJUE, 4 octobre 2024, Agentsia po vpisvaniyata, C 200/23

Possibilité de communication orale à toute personne de données relatives à des condamnations pénales d'une personne physique figurant dans un fichier– 1) Illicéité – 2) Nature du demandeur de société commerciale ou un particulier – Indifférence

1) Les dispositions du règlement 2016/679, notamment l'article 6, paragraphe 1, sous e), et l'article 10 de celui-ci, doivent être interprétées en ce sens qu'elles s'opposent à ce que des données relatives à des condamnations pénales d'une personne physique figurant dans un fichier tenu par une juridiction puissent être communiquées oralement à toute personne aux fins de garantir un accès du public à des documents officiels, sans que la personne demandant la communication ait à justifier d'un intérêt spécifique à obtenir lesdites données.

2) La circonstance que cette personne soit une société commerciale ou un particulier n'ayant pas d'incidence à cet égard.

CJUE, 7 mars 2024, Endemol Shine Finland, C-740/22, point 59

Recherche effectuée à partir du nom d'une personne sur un moteur de recherche – 1) Affichage d'un lien menant vers des articles contenant des informations prétendument inexactes dans la liste de résultats – Demande de déréférencement – Conditions – 2) Résultats d'une recherche d'images de cette personne – Demande de déréférencement – Conditions

1) L'article 17, paragraphe 3, sous a), du RGPD doit être interprété en ce sens que dans le cadre de la mise en balance qu'il convient d'opérer entre les droits visés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, d'une part, et ceux visés à l'article 11 de la Charte des droits fondamentaux, d'autre part, aux fins de l'examen d'une demande de déréférencement adressée à l'exploitant d'un moteur de recherche et tendant à ce que soit supprimé de la liste de résultats d'une recherche le lien menant vers un contenu comportant des allégations que la personne ayant introduit la demande estime inexactes, ce déréférencement n'est pas soumis à la condition que la question de l'exactitude du contenu référencé ait été résolue, au moins à titre provisoire, dans le cadre d'un recours intenté par cette personne contre le fournisseur de contenu.

2) L'article 12, sous b), et l'article 14, premier alinéa, sous a), de la directive 95/46/CE et l'article 17, paragraphe 3, sous a) du règlement 2016/679doivent être interprétés en ce sens que dans le cadre de la mise en balance qu'il convient d'opérer entre les droits visés aux articles 7 et 8 de la Charte des droits fondamentaux, d'une part, et ceux visés à l'article 11 de la Charte des droits fondamentaux, d'autre part, aux fins de l'examen d'une demande de déréférencement adressée à l'exploitant d'un moteur de recherche et tendant à ce que soient supprimées des résultats d'une recherche d'images effectuée à partir du nom d'une personne physique des photographies affichées sous la forme de vignettes qui représentent cette personne, il y a lieu de tenir compte de la valeur informative de ces photographies indépendamment du contexte de leur publication sur la page Internet d'où elles sont extraites, mais en prenant en considération tout élément textuel qui accompagne directement l'affichage de ces photographies dans les résultats de recherche et qui est susceptible d'apporter un éclairage sur la valeur informative de celles-ci.

CJUE, grande chambre, 8 décembre 2022, TU et RE c/ Google LLC, C-460/20

Réglementation nationale rendant obligatoire l'accès du public aux données à caractère personnel relatives aux points de pénalité et autorisant la communication de ces données à des opérateurs économiques à des fins de réutilisation – Objectif d'intérêt général d'amélioration de la sécurité routière – Absence de caractère nécessaire de ce traitement des données à caractère personnel

Les dispositions du RGPD, notamment l'article 5, paragraphe 1, l'article 6, paragraphe 1, sous e), et l'article 10 de celui-ci, doivent être interprétées en ce sens qu'elles s'opposent à une législation

nationale qui fait obligation à l'organisme public chargé du registre dans lequel sont inscrits les points de pénalité imposés aux conducteurs de véhicules pour des infractions routières de rendre ces données accessibles au public, sans que la personne demandant l'accès ait à justifier d'un intérêt spécifique à obtenir lesdites données. L'amélioration de la sécurité routière constitue un objectif d'intérêt général reconnu par l'Union et, partant, les États membres peuvent qualifier la sécurité routière de « mission d'intérêt public ». Cependant, dans le cas d'espèce, la nécessité du régime letton de communication de données à caractère personnel relatives aux points de pénalité pour assurer l'objectif visé n'est pas établie. En effet, d'une part, le législateur letton dispose d'une multitude de voies d'actions qui lui auraient permis d'atteindre cet objectif par d'autres moyens moins attentatoires aux droits fondamentaux des personnes concernées. D'autre part, il convient de tenir compte de la sensibilité des données relatives aux points de pénalité et du fait que leur communication au public est susceptible de constituer une ingérence grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel, dès lors qu'elle peut provoquer la désapprobation de la société et entraîner la stigmatisation de la personne concernée.

La Cour considère que, compte tenu de la sensibilité de ces données et de la gravité de cette ingérence dans ces deux droits fondamentaux, ces droits prévalent tant sur l'intérêt du public à avoir accès à des documents officiels, tels que le registre national des véhicules et de leurs conducteurs, que sur le droit à la liberté d'information.

CJUE, grande chambre, 22 juin 2021, Latvijas Republikas Saeima, C-439/19, points 108-122

Directive 95/46/CE – Article 6, paragraphe 1, sous e) (durée de conservation) – Données soumises à la publicité au registre des sociétés – Première directive 68/151/CEE – Article 3 – Dissolution de la société concernée – Limitation de l'accès des tiers à ces données – Exception – Compétence des États membres

L'ingérence dans le droit à la vie privée et à la protection des données à caractère personnel qu'emporte la publicité des données nominatives contenues dans le registre des sociétés n'est pas disproportionnée eu égard au nombre de données concernées et au fait qu'elle vise à assurer la sécurité juridique dans les rapports entre les sociétés et les tiers ainsi qu'à protéger les intérêts des tiers par rapport aux sociétés par actions et aux sociétés à responsabilité limitée.

Il ne peut donc être garanti aux personnes physiques dont les données sont inscrites dans le registre des sociétés le droit d'obtenir, après un certain délai à compter de la dissolution de la société, l'effacement des données à caractère personnel les concernant.

En revanche, les États membres peuvent exceptionnellement déroger à cette exigence de publicité. Il leur appartient de déterminer si les personnes physiques, visées à l'article 2, paragraphe 1, sous d) et j) de la directive 68/151/CEE, à savoir, d'une part, les personnes qui ont le pouvoir d'engager une société à l'égard des tiers et de la représenter en justice et celles qui participent à l'administration, à la surveillance ou au contrôle de la société et, d'autre part, les liquidateurs d'une société, peuvent demander à l'autorité chargée de la tenue, respectivement, du registre central, du registre du commerce ou du registre des sociétés de vérifier, sur la base d'une appréciation au cas par cas, s'il est exceptionnellement justifié, pour des raisons prépondérantes et légitimes tenant à leur situation particulière, de limiter, à l'expiration d'un délai suffisamment long après la dissolution de la société concernée, l'accès aux données à caractère personnel les concernant, inscrites dans ce registre, aux tiers justifiant d'un intérêt spécifique à la consultation de ces données.

CJUE, 9 mars 2017, Manni, C-398/15

Protection des personnes physiques à l'égard du traitement des données à caractère personnel – Directive 95/46, articles 12 et 14 – Droit d'accès de la personne concernée aux données à caractère personnel et droit d'opposition à leur traitement – Recherche

effectuée au moyen d'un moteur de recherche à partir du nom d'une personne – Affichage d'une liste de résultats – Droit de demander de ne plus mettre cette information à la disposition du grand public

Il découle des exigences, prévues à l'article 6, paragraphe 1, sous c) à e), de la directive 95/46, que même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Ainsi, dans l'hypothèse où il est constaté, à la suite d'une demande de la personne concernée en application de l'article 12, sous b), de la directive 95/46, que l'inclusion dans la liste de résultats, affichée à la suite d'une recherche effectuée à partir de son nom, des liens vers des pages web, publiées légalement par des tiers et contenant des informations véridiques relatives à sa personne, est, au stade actuel, incompatible avec ledit article 6, paragraphe 1, sous c) à e), en raison du fait que ces informations apparaissent, eu égard à l'ensemble des circonstances caractérisant le cas d'espèce, inadéquates, pas ou plus pertinentes ou excessives au regard des finalités du traitement en cause réalisé par l'exploitant du moteur de recherche, les informations et les liens concernés de ladite liste de résultats doivent être effacés.

Dans ce contexte, la constatation d'un droit de la personne concernée à ce que l'information relative à sa personne ne soit plus liée à son nom par une liste de résultats ne présuppose pas que l'inclusion de l'information en question dans la liste de résultats cause un préjudice à la personne concernée.

La personne concernée pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, demander à ce que l'information en question ne soit plus mise à la disposition du grand public par son inclusion dans une telle liste de résultats, ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à trouver ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question.

CJUE, 13 mai 2014, Google Spain, C-131/12, points 93, 94, 96-99

Collecte et exploitation par les administrations fiscale et douanière de contenus accessibles publiquement sur les sites internet d'opérateurs de plateforme – Conditions – Conformité

Conformité à la Constitution d'un dispositif autorisant à titre expérimental et pour une durée de trois ans, les administrations fiscale et douanière à collecter et à exploiter de manière automatisée les contenus accessibles publiquement sur les sites internet de certains opérateurs de plateforme, aux fins de recherche de manquements et d'infractions en matière fiscale et douanière malgré l'atteinte au droit au respect de la vie privée dès lors que :

- le dispositif poursuit l'objectif à valeur constitutionnelle de lutte contre la fraude et l'évasion fiscale ;
- les traitements de données autorisés par les dispositions contestées peuvent être mis en œuvre, d'une part, pour les besoins de la recherche de certains manquements et de certaines infractions dont la commission est rendue possible ou favorisée par l'usage d'internet et, d'autre part, pour rechercher l'insuffisance de déclaration découlant d'un manquement aux règles de domiciliation fiscale. Si la commission de ce manquement n'est pas rendue possible ou favorisée par l'usage d'internet, il résulte des travaux parlementaires que le législateur, qui a souhaité limiter le nombre de manquements susceptibles d'être recherchés, a entendu viser un des cas les plus graves de soustraction à l'impôt, qui peut être particulièrement difficile à déceler ;
- les données susceptibles d'être collectées et exploitées doivent répondre à deux conditions cumulatives. D'une part, il doit s'agir de contenus librement accessibles sur un service de

communication au public en ligne d'une des plateformes précitées, à l'exclusion donc des contenus accessibles seulement après saisie d'un mot de passe ou après inscription sur le site en cause. D'autre part, ces contenus doivent être manifestement rendus publics par les utilisateurs de ces sites. Il en résulte que ne peuvent être collectés et exploités que les contenus se rapportant à la personne qui les a, délibérément, divulgués. En outre, les données sensibles au sens du paragraphe I de l'article 6 de la loi du 6 janvier 1978, c'est-à-dire celles qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, les données génétiques et biométriques et celles concernant la santé et la vie ou l'orientation sexuelles, ne peuvent faire l'objet d'aucune exploitation à des fins de recherche de manquements ou d'infractions ;

- d'une part, les traitements de données autorisés par les dispositions contestées ne peuvent comporter aucun système de reconnaissance faciale. D'autre part, ils ne peuvent être mis en œuvre que par des agents des administrations fiscale et douanière ayant au moins le grade de contrôleur et spécialement habilités ;
- les données qui s'avèrent manifestement sans lien avec les manquements et infractions recherchés ou qui constituent des données sensibles sont détruites au plus tard dans les cinq jours suivant leur collecte, sans aucune autre exploitation possible de ces données pendant ce délai. Les autres données doivent être détruites dans les trente jours si elles ne sont pas de nature à concourir à la constatation des manquements ou infractions. Seules peuvent être conservées les données strictement nécessaires à une telle constatation, dans la limite d'une année ou, le cas échéant, jusqu'au terme de la procédure pénale, fiscale ou douanière dans le cadre de laquelle elles sont utilisées ;
- aucune procédure pénale, fiscale ou douanière ne peut être engagée sans qu'ait été portée une appréciation individuelle de la situation de la personne par l'administration, qui ne peut alors se fonder exclusivement sur les résultats du traitement automatisé ;
- le traitement instauré par les dispositions contestées est mis en œuvre dans le respect de la loi du 6 janvier 1978, à l'exception du droit d'opposition prévu à son article 110 ;
- la mise en œuvre des traitements de données, tant lors de leur création que lors de leur utilisation, doit être proportionnée aux finalités poursuivies. Il appartiendra notamment, à ce titre, au pouvoir réglementaire, sous le contrôle du juge, de veiller à ce que les algorithmes utilisés par ces traitements ne permettent de collecter, d'exploiter et de conserver que les données strictement nécessaires à ces finalités.

CC, 2019-796 DC, 27 décembre 2019, Loi de finances pour 2020, points 84-92

Règles déontologiques – Comparateurs et notations d'avocats – Application aux tiers – Absence

Les règles professionnelles issues de l'article 15 du décret n°2005-790 du 12 juillet 2005 interdisant aux avocats d'établir des comparateurs et notations de leurs confrères à l'occasion d'opérations de publicité ou de sollicitation personnalisée ne concernent que les avocats. Les tiers ne sont pas tenus par les règles déontologiques de cette profession. Il leur appartient seulement, dans leurs activités propres, de délivrer au consommateur une information loyale, claire et transparente.

Cass. civ. 1, 11 mai 2017, n° 16-13.669, B., point 16

Droit d'accès aux documents administratifs - Communication à un tiers d'un registre de contention et d'isolement avec occultation des éléments permettant d'identifier les patients et les soignants, mais sans occultation des identifiants " anonymisés " des patients – Atteinte à la protection de la vie privée et du secret médical – Illicéité

Demande de communication d'un registre de contentieux et d'isolement au titre du droit d'accès aux documents administratifs. Dans le cas où l'identité des patients a fait l'objet d'une pseudonymisation, laquelle ne permet l'identification des personnes en cause qu'après recoupement d'informations, il appartient au juge administratif d'apprécier si, eu égard à la sensibilité des informations en cause et aux efforts nécessaires pour identifier les personnes concernées, leur communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. En l'espèce, compte tenu de la nature des informations en cause, qui touchent à la santé mentale des patients, et du nombre restreint de personnes pouvant faire l'objet d'une mesure de contention et d'isolement, facilitant ainsi leur identification, alors au demeurant que les autorités énumérées à la dernière phrase du deuxième alinéa de l'article L. 3222-5-1 du code de la santé publique peuvent accéder à l'ensemble des informations figurant sur les registres et contrôler l'activité des établissements concernés, l'identifiant dit " anonymisé " figurant dans ces registres, qu'il s'agisse, selon la pratique du centre hospitalier, de " l'identifiant permanent du patient " (IPP) ou d'un identifiant spécialement défini, doit être regardé comme une information dont la communication est susceptible de porter atteinte à la protection de la vie privée et au secret médical. Cet identifiant n'est donc communicable qu'au seul intéressé en vertu des dispositions de l'article L. 311-6 du code des relations entre le public et l'administration.

CE, 10ème chambre, 22 mars 2024, Centre hospitalier Le Vinatier, n°471369, Inédit, point 6

Annuaire national des avocats établi par le CNB – 1) Document administratif – Existence – 2) Obligations de diffusion – a) Obligation de le rendre accessible en ligne – Modalités – Inclusion – Moteur de recherche (art. 21-1 de la loi du 31 décembre 1971) – b) Obligation d'en publier en ligne le fichier – Modalités – Standard ouvert, réutilisable et exploitable (art. L. 300-4 du CRPA) – 3) Mise à disposition par moteur de recherche – a) Publication en ligne (4° de l'art. L. 311-9) – Absence – b) Diffusion publique (art. L. 312-1-1) – Absence

1) Il résulte de l'article 21-1 de la loi n° 71-1130 du 31 décembre 1971 que le législateur a entendu investir le Conseil national des barreaux (CNB) d'une nouvelle fonction, se rattachant à sa mission de service public relative à l'organisation de la profession réglementée d'avocat, consistant à constituer et à rendre accessible au public la liste à jour des avocats inscrits au tableau d'un barreau. L'annuaire national qu'il incombe à ce dernier d'établir et de mettre à jour constitue ainsi, dans son intégralité, un document administratif.

2) a) Si, en vertu de ces dispositions, il appartient au CNB de rendre accessible en ligne un annuaire national des avocats inscrits au tableau d'un barreau selon les modalités qu'il fixe, en l'absence de dispositions réglementaires les précisant, notamment, ainsi qu'il y a procédé, par le biais d'un moteur de recherche sur son site internet permettant à l'internaute d'interroger la base de données à partir de certains champs de recherche et d'obtenir des résultats extraits de l'annuaire,

b) Il ne résulte pas de ces dispositions, éclairées par les travaux préparatoires de la loi n° 2016-1547 du 18 novembre 2016 dont elles sont issues, que le législateur aurait entendu déroger aux règles de droit commun régissant la publication en ligne des documents administratifs, rappelées aux articles L. 300-2, L. 300-4, L. 311-1, L. 311-9, L. 312-1-1 et au 3° de l'article D. 312-1-3 du code des relations entre le public et l'administration (CRPA) et, en particulier, soustraire le CNB, saisi d'une demande en ce sens, à l'obligation de publier en ligne le fichier correspondant à l'annuaire national des avocats dans son intégralité dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé, ainsi que, spontanément, chaque mise à jour.

3) Lorsqu'une personne demande à accéder à l'annuaire national des avocats selon la modalité d'une publication en ligne, en application du 4° de l'article L. 311-9 du CRPA, et que le CNB n'a rendu accessible l'annuaire national des avocats qu'il établit et met à jour que par le biais d'un moteur de recherche sur son site internet, permettant à l'internaute d'interroger la base de données à partir de certains champs de recherche et d'obtenir un nombre limité de résultats,

a) une telle mise à disposition ne peut être regardée comme une publication en ligne de ce document administratif au sens de l'article L. 311-9 du CRPA

b) ni comme une diffusion publique du document au sens de l'article L. 312-1-1 du CRPA, diffusion qui est de droit pour les documents disponibles sous forme électronique communiqués en application des procédures prévues au titre 3 du CRPA, alors au surplus que cette publication en ligne n'est pas réalisée dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé, comme l'exige l'article L. 300-4 du même code.

CE, 10ème-9ème chambres réunies, 27 septembre 2022, Association Ouvre-boîte, n°450739, T., points 10, 17

Décision de justice publiée sur internet – Appréciation du bien-fondé d'une demande d'effacement - Possibilité d'anonymiser la décision sans la rendre incompréhensible ou diminuer sa valeur doctrinale pour le public – Mise en balance de l'atteinte que cette publication porte à la vie privée du demandeur avec les intérêts du responsable de traitement et l'intérêt du public à connaître de cette décision.

Dans le cas particulier d'une demande d'effacement, fondée sur une opposition au traitement, relative à certains éléments figurant dans une décision de justice publiée sur internet, il y a lieu de tenir compte de la possibilité d'anonymiser la décision sans la rendre incompréhensible ou diminuer sa valeur doctrinale pour le public. Si tel est le cas et si la publication porte atteinte à la vie privée du demandeur, il doit en principe être procédé à l'effacement des données à caractère personnel publiées. Dans les autres cas, il y a lieu de mettre en balance l'atteinte que cette publication porte à la vie privée du demandeur avec les droit et intérêts du responsable de traitement, ainsi que l'intérêt du public à connaître cette décision, au regard notamment de son apport jurisprudentiel.

En l'espèce, la requérante avait souhaité s'opposer au traitement de ses données par la publication d'une décision de justice, en application de l'article 21 du RGPD, afin d'obtenir l'effacement des données permettant de l'identifier dans la décision, sur le fondement de l'article 17 du RGPD.

CNIL, P, 22 janvier 2024, mise en demeure, Société X, décision n° MED-2024-016, non publié

Réutilisation des données publiées par l'État – Données des mutations immobilières en open data (R*112-A-1 du livre des procédures fiscales) – 1) Publication des données – Licéité – 2) Exercice du droit d'opposition – Mise en œuvre de mesures empêchant la réidentification

L'article R.*112-1-3 dispose que la réutilisation de ces informations ne doit avoir ni pour objet ni pour effet de permettre la réidentification des personnes concernées par les mutations.

1) Dès lors qu'un site internet se contente de reprendre les données en open data pour les publier, sans croisement, le traitement repose sur un intérêt légitime et est conforme à la réglementation de cette base de données.

2) En cas d'exercice du droit d'opposition, en application des articles 21 du RGPD et R.*112-1-3, les personnes qui indiquent que les données publiées, même limitées à celles publiées par l'État, ont pour effet de permettre leur réidentification (par exemple lorsqu'une recherche sur un moteur de recherche avec l'adresse du bien permet de retrouver la personne l'ayant acquis) ont le droit à ce que des mesures

soient mises en œuvre pour empêcher la réidentification. En particulier, il est possible de ne plus lier le prix du bien immobilier en question à une adresse précise mais à une zone géographique plus large.

CNIL, P, 25 octobre 2019, Courrier, Société X, 21020578, non publié

Site internet de notation individuelle des enseignants – Coexistence avec un régime de notation officiel – Risque de confusion dans l'esprit du public

La mise en ligne de la notation d'enseignants et de leur établissement d'activité est susceptible de porter atteinte à la réputation professionnelle et à la notoriété de l'enseignant de façon disproportionnée. En effet, la société proposant un système de notation des enseignants qui ne s'inscrit pas dans le cadre juridique de la notation des enseignants fixé par leurs autorités hiérarchiques mais poursuit une activité commerciale reposant sur l'audience d'un site internet qui ne lui confère aucune légitimité pour procéder ou faire procéder à une notation individuelle des enseignants est susceptible de créer une confusion, dans l'esprit du public, avec un régime de notation officiel. Faute de légitimité, ce type de traitement est susceptible de constituer un manquement à l'obligation d'adéquation, de pertinence et du caractère non excessif des données.

CNIL, P, 6 novembre 2008, Mise en demeure, Société X, n°MED-2008-432, non publié

Voir aussi : CA Paris, 14ème chambre, Section A, 25 juin 2008, n°08/04727

6.11 Traitements de vote électronique

Élection des représentants du personnel – Vote électronique par Internet – Protection du caractère personnel du vote – Modalités retenues n'offrant pas une protection du caractère personnel d'un niveau équivalent à celui des autres modalités de vote

Dans le cadre d'élections des représentants du personnel au sein des instances de représentation du personnel de la fonction publique hospitalière, si le vote électronique par internet est susceptible de constituer une modalité de vote au même titre que le vote à l'urne et le vote par correspondance, il implique, en raison de ses spécificités et des conditions de son utilisation, que des garanties adaptées soient prévues pour que le respect des principes généraux du droit électoral de complète information de l'électeur, de libre choix de celui-ci, d'égalité entre les candidats, de secret du vote, de sincérité du scrutin et de contrôle du juge soit assuré à un niveau équivalent à celui des autres modalités de vote.

Dès lors, d'une part, que l'identification du demandeur qui sollicite la mise en œuvre d'une procédure de « réassort »(nouvelles communication des éléments d'authentification nécessaires pour participer au scrutin) s'effectue par la seule vérification de ses nom, prénom, date et lieu de naissance, informations qui peuvent aisément être connues de tiers, et, d'autre part, que le moyen de communication par lequel sont envoyés l'identifiant et le nouveau mot de passe est celui qu'indique le demandeur qui sollicite ce « réassort », sans qu'il soit garanti qu'il ne serait accessible qu'à l'électeur, et alors même qu'un même numéro de téléphone ou une même adresse électronique ne peut être utilisé que pour une seule demande de réassort, les requérants sont fondés à soutenir que les modalités retenues pour le vote électronique par internet n'offraient pas une protection du caractère personnel du vote d'un niveau équivalent à celui des autres modalités de vote.

Compte tenu de l'importance du recours au vote électronique dans les scrutins en cause et de l'impossibilité de déterminer le nombre de cas dans lesquels a été mise en œuvre, pour chacune des instances concernées, la procédure dite de « réassort », les syndicats requérants sont fondés à demander l'annulation de l'ensemble des opérations électorales en vue de la désignation des représentants du personnel.

CE, 8ème–3ème chambres réunies, 26 janvier 2021, Union des syndicats CGT des agents de l'AP-HM, n° 437993, Inédit., points 18-19

Articles R.2122-49 et suivants du code du travail - Système de vote électronique prévoyant la transmission de l'ensemble matériel du vote par un canal de communication unique – Absence de conformité à la recommandation de la CNIL relative à la sécurité des systèmes de vote par correspondance électronique sauf à ce que le vote par correspondance postale soit autorisé et rendu possible par réception d'un unique courrier

Les systèmes de vote électronique sont susceptibles de présenter des risques particuliers pour les personnes, liés notamment à la difficulté d'assurer que l'identité du votant correspond bien à celle de l'électeur authentifié et qu'il émet son vote en toute indépendance, ainsi qu'à la possible divulgation d'opinions politiques ou syndicales en cas de violation de données. Par conséquent, la CNIL rappelle la nécessité de mettre en œuvre des mesures de sécurité fortes pour assurer la confidentialité du vote et la sincérité du scrutin, telles qu'elle les a définies dans sa délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

La CNIL relève que les dispositions des articles R.2122-49 et suivants du code du travail prévoient que l'ensemble du matériel de vote permettant, d'une part, le vote postal et d'autre part, l'accès à la plateforme de vote par correspondance électronique, est transmis par un unique courrier postal à l'électeur après la période lui permettant de rectifier son adresse auprès du ministère. Ces dispositions n'apparaissent pas conformes à la recommandation précitée en ce qu'elles prévoient la transmission du matériel du vote (à savoir un identifiant et un mot de passe) par un canal de communication unique.

Toutefois, ces recommandations ont vocation à permettre de garantir une sincérité absolue du scrutin dans un contexte où le vote par correspondance postale n'est pas autorisé. En l'espèce et afin de favoriser une plus grande participation au scrutin, le pouvoir réglementaire a autorisé le vote par voie postale. Dans ces conditions, la CNIL estime que l'envoi du matériel de vote par correspondance électronique est également acceptable.

CNIL, SP, 11 avril 2024, Demande d'avis relative à un projet de décret modifiant les conditions d'organisation du scrutin destiné à mesurer l'audience des organisations syndicales auprès des salariés des entreprises de moins de onze salariés

6.12 Dématérialisation et téléservices

Obligation de recourir à un téléservice pour accomplir une démarche administrative – 1) Mesure relevant, par elle-même, du domaine de la loi – Absence – 2) Légalité – a) Méconnaissance du droit à saisir l'administration par voie électronique – Absence – b) Méconnaissance, par principe, des principes d'égalité et de continuité du service public, de la convention EDH (art. 14), de la CIDPH (art. 9) et de la loi du 27 mai 2008 – Absence – c) Conditions – i) Accès normal des usagers au service public et exercice effectif de leurs droits – ii) Critères – 3) Obligation de recourir à un téléservice pour certaines demandes de titre de séjour – a) Exigence d'un accompagnement – Existence – b) Exigence d'une solution de substitution en cas d'impossibilité de recourir au téléservice malgré cet accompagnement – Existence

1) L'obligation d'avoir recours à un téléservice pour accomplir une démarche administrative auprès d'un service de l'État, et notamment pour demander la délivrance d'une autorisation, dès lors qu'elle

n'a pas pour effet de modifier les conditions légales auxquelles est subordonnée sa délivrance, ne met pas en cause, par elle-même, les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques, non plus qu'aucune autre règle ou aucun autre principe dont l'article 34 ou d'autres dispositions de la Constitution prévoient qu'ils relèvent du domaine de la loi.

2) a) Les articles L. 112-8 à L. 112-10 du code des relations entre le public et l'administration (CRPA) créent, sauf lorsqu'y font obstacle les considérations mentionnées à l'article L. 112-10, un droit, pour les usagers, de saisir l'administration par voie électronique, sans le leur imposer. Elles ne font cependant pas obstacle à ce que le pouvoir réglementaire édicte une obligation d'accomplir des démarches administratives par la voie d'un téléservice.

b) Ni les principes d'égalité devant la loi, d'égalité devant le service public et de continuité du service public, ni le droit à la compensation du handicap énoncé par l'article L. 114-1-1 du code de l'action sociale et des familles (CASF), ni le principe de non-discrimination reconnu par l'article 14 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (convention EDH), ni, en tout état de cause, les autres droits garantis par la même convention, l'article 9 de la convention des Nations Unies relative aux droits des personnes handicapées (CIDPH) ou la loi n° 2008-496 du 27 mai 2008 ne font obstacle, par principe, à ce que soit rendu obligatoire le recours à un téléservice pour accomplir une démarche administrative, et notamment pour demander la délivrance d'une autorisation.

c) i) Toutefois, le pouvoir réglementaire ne saurait édicter une telle obligation qu'à la condition de permettre l'accès normal des usagers au service public et de garantir aux personnes concernées l'exercice effectif de leurs droits. ii) Il doit tenir compte de l'objet du service, du degré de complexité des démarches administratives en cause et de leurs conséquences pour les intéressés, des caractéristiques de l'outil numérique mis en œuvre ainsi que de celles du public concerné, notamment, le cas échéant, de ses difficultés dans l'accès aux services en ligne ou dans leur maniement.

3) a) Eu égard aux caractéristiques du public concerné, à la diversité et à la complexité des situations des demandeurs et aux conséquences qu'a sur la situation d'un étranger, notamment sur son droit à se maintenir en France et, dans certains cas, à y travailler, l'enregistrement de sa demande, il incombe au pouvoir règlementaire, lorsqu'il impose le recours à un téléservice pour l'obtention de certains titres de séjour, de prévoir les dispositions nécessaires pour que bénéficient d'un accompagnement les personnes qui ne disposent pas d'un accès aux outils numériques ou qui rencontrent des difficultés soit dans leur utilisation, soit dans l'accomplissement des démarches administratives.

b) Il lui incombe, en outre, pour les mêmes motifs, de garantir la possibilité de recourir à une solution de substitution, pour le cas où certains demandeurs se heurteraient, malgré cet accompagnement, à l'impossibilité de recourir au téléservice pour des raisons tenant à la conception de cet outil ou à son mode de fonctionnement.

CE, Section, 3 juin 2022, Conseil national des barreaux, n° 452798, Rec., points 6-10

6.13 Traitements vidéo

6.13.1 Vidéoprotection

Enregistrements vidéo du dépouillement des votes dans les bureaux de vote – Acte administratif de limitation ou d'interdiction – Licéité

L'article 6, paragraphe 1, sous e), et l'article 58 du RGPD doivent être interprétés en ce sens que ces dispositions ne s'opposent pas à ce que les autorités compétentes d'un État membre adoptent un acte administratif d'application générale qui prévoit la limitation ou, le cas échéant, l'interdiction de

l'enregistrement vidéo du dépouillement du scrutin, dans les bureaux de vote lors d'élections dans cet État membre.

CJUE, 20 octobre 2022, Koalitsia « Demokratichna Bulgaria – Obedinenie », C-306/21

Système de caméra donnant lieu à un enregistrement vidéo stocké dans un disque dur – Installation sur la maison familiale d'une personne physique – Surveillance notamment de l'espace public – Traitement effectué pour l'exercice d'activité exclusivement personnelles ou domestiques – Exclusion

L'article 3, paragraphe 2, second tiret, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doit être interprété en ce sens que l'exploitation d'un système de caméra, donnant lieu à un enregistrement vidéo des personnes stocké dans un dispositif d'enregistrement continu tel qu'un disque dur, installé par une personne physique sur sa maison familiale afin de protéger les biens, la santé et la vie des propriétaires de la maison, ce système surveillant également l'espace public, ne constitue pas un traitement des données effectué pour l'exercice d'activités exclusivement personnelles ou domestiques, au sens de cette disposition.

CJUE,11 décembre 2014, Ryneš, C-212/13

Mise en œuvre et exploitation par des personnes privées de dispositifs de vidéoprotection sur la voie publique – Inconstitutionnalité

Les dispositions de l'article 18 de la loi d'orientation et de programmation pour la performance de la sécurité intérieure autorisent toute personne morale à mettre en œuvre des dispositifs de surveillance au-delà des abords « immédiats » de ses bâtiments et installations et confient à des opérateurs privés le soin d'exploiter des systèmes de vidéoprotection sur la voie publique et de visionner les images pour le compte de personnes publiques. Ce faisant, elles permettent d'investir des personnes privées de missions de surveillance générale de la voie publique. Chacune de ces dispositions rend ainsi possible la délégation à une personne privée des compétences de police administrative générale inhérentes à l'exercice de la « force publique » nécessaire à la garantie des droits. Elles méconnaissent l'article 12 de la Déclaration de 1789.

CC, 2011-625 DC, 10 mars 2011, Loi d'orientation et de programmation pour la performance de la sécurité intérieure, points 18-19

Garanties relatives à la mise en œuvre de systèmes de vidéosurveillance – Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité – 1) Droit d'accès aux enregistrements – 2) Régime d'autorisation d'installation

1) La loi a ouvert à toute personne intéressée le droit de s'adresser au responsable d'un système de vidéosurveillance[1] afin d'obtenir un accès aux enregistrements qui la concernent ou d'en vérifier la destruction dans un délai maximum d'un mois. Cet accès est de droit, sous réserve que soient opposés des motifs « tenant à la sûreté de l'État, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, ou

[1] Le terme « vidéosurveillance » employé dans cette décision du Conseil constitutionnel de 1995 serait aujourd'hui remplacé celui de « vidéoprotection ».

au droit des tiers ». La référence au « droit des tiers » doit être regardée comme ne visant que le cas où une telle communication serait de nature à porter atteinte au secret de leur vie privée.

2) Concernant le régime d'autorisation d'installation de systèmes de vidéosurveillance, le législateur a prévu que « l'autorisation sollicitée est réputée acquise à défaut de réponse dans un délai de quatre mois ». Compte tenu des risques que peut comporter pour la liberté individuelle l'installation de systèmes de vidéosurveillance, la loi ne peut subordonner à la diligence de l'autorité administrative l'autorisation d'installer de tels systèmes sans priver alors de garanties légales des principes constitutionnels.

CC, 94-352 DC, 18 janvier 1995, Loi d'orientation et de programmation relative à la sécurité, points 8-12

---

1) Utilisation en matière de vidéoprotection – Licéité – Conditions – 2) Finalité de réponse aux réquisition judiciaires – Licéité – Absence.

1) Si les articles L. 233-1 et L. 233-1-1 du code de la sécurité intérieure autorisent les seuls services des douanes, de police et de gendarmerie nationales à mettre en œuvre les dispositifs de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants pour les finalités qu'ils prévoient, ils n'ont pas pour effet d'interdire aux autorités compétentes de mettre en œuvre, sur le fondement de l'article L. 251-2 de ce même code, des dispositifs de lecture automatisée des plaques d'immatriculation des véhicules. Toutefois, ces autorités ne peuvent le faire que pour l'une des finalités énumérées par cet article et dans le respect du titre V du livre II de ce même code.

2) La mise en œuvre d'un dispositif de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants aux seules fins de répondre aux éventuelles réquisitions des forces de l'ordre pour l'exercice de leurs missions de police judiciaire ne constitue pas une finalité déterminée et n'est pas au nombre des finalités justifiant la mise en place d'un tel dispositif visées par l'article L.251-2 du CSI.

CE, 10ème–9ème chambres réunies, 30 avril 2024, °472864, Inédit, points 4 et 5

---

1) Finalités légales de la vidéoprotection (art. L. 251-2 du CSI) – Exclusion – Mise à la disposition de la gendarmerie nationale des données collectées – 2) Dispositifs de contrôle automatisé des données signalétiques des véhicules (art. L. 233-1 du CSI) – Gestionnaires autorisés – Services des douanes, de police et de gendarmerie nationales uniquement

1) L'article L. 251-2 du code de la sécurité intérieure (CSI) liste les finalités pour lesquelles la transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes. Mettre les données collectées à la disposition de la gendarmerie nationale pour l'exercice de ses missions de police judiciaire, qui n'est pas aux nombres des finalités visées par cet article, ne constitue pas, pour un dispositif de transmission et d'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection, une finalité légitime.

2) L'article L. 233-1 du CSI autorise les seuls services des douanes, de police et de gendarmerie nationales à mettre en œuvre les dispositifs de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants pour les finalités qu'il prévoit. Par suite, une commune ne saurait mettre en œuvre un tel dispositif, alors mêmes que les données collectées seraient destinées à être mises à la disposition de la gendarmerie nationale à des fins d'aide à l'identification des auteurs d'infractions.

CE, 10ème–9ème chambres réunies, 27 juin 2016, Commune de Gujan-Mestras, n°385091, Rec., points 3-4, 6

1) Mentions d'information obligatoires et droit d'accès à certaines informations - 1) Emplacement des caméras de surveillance – Absence - 2) Cas d'espèce

1) Il résulte des articles 13 et 15 du RGPD, des dispositions des titres II et III de la loi informatique et libertés relatives aux obligations d'information et au droit d'accès, et des dispositions du code de la sécurité intérieure régissant spécifiquement la vidéoprotection, notamment l'article R. 253-6, que le responsable de traitement, s'il est tenu d'informer, d'une façon adaptée au contexte et aux objectifs poursuivis, sur l'existence de la vidéoprotection d'un territoire, d'une zone ou d'un bâtiment, et de fournir l'ensemble des mentions et informations prévues par ces textes, n'est pas tenu à ce titre de communiquer l'emplacement exact de chaque caméra.

2) En l'espèce, la commune, qui a mis en place un grand nombre de panneaux d'information, situés à proximité des caméras et des grands axes de circulation, lesquels contiennent un renvoi vers une information disponible sur le site web de la ville, a satisfait à l'obligation d'information telle que prévue par les dispositions de l'article 13 du RGPD. La commune n'était pas tenue d'informer les personnes sur l'emplacement des caméras de surveillance ni de communiquer ces informations à l'auteur de la plainte au titre de son droit d'accès au sens de l'article 15 du RGPD. En effet, ni l'article 13 ni l'article 15 n'exige la communication de telles informations.

CNIL, P, 29 mai 2024, Courrier présidente, non publié

Syndic de copropriété – Système de vidéoprotection filmant incidemment la voie publique – Exception propre aux dispositifs déployés par les commerçants – Absence

Lorsqu'un dispositif filme même incidemment, la voie publique ou des lieux accessibles au public, il doit être regardé comme un système de vidéoprotection. Or, la mise en œuvre d'un tel système est régie par le code de la sécurité intérieure, et notamment l'article L.251-2 de ce code qui dispose que « la transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes » ou « dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol ». Par exception, « après information du maire de la commune concernée et autorisation des autorités publiques compétentes, des commerçants peuvent mettre en œuvre sur la voie publique un système de vidéoprotection aux fins d'assurer la protection des abords immédiats de leurs bâtiments et installations, dans les lieux particulièrement exposés à des risques d'agression ou de vol ». Un syndic de copropriété ne pouvant être regardé comme un commerçant, cette exception ne lui est pas applicable et il ne peut mettre en œuvre, de manière licite, un système de vidéoprotection filmant la voie publique, même de manière incidente aux abords immédiats de la copropriété.

CNIL, P, 13 mars 2023, Mise en demeure, Société X, n°2023-012, non publié

6.13.2 Vidéosurveillance

1) Communication et exploitation par les enquêteurs d'enregistrements issus des caméras de surveillance installées par le propriétaire ou le gestionnaire d'un ensemble d'habitations dans les parties communes – Procédé de captation d'images relevant de l'article 706-96 code de procédure pénale – Exclusion – 2) Système de vidéosurveillance installé et en fonctionnement préalablement aux réquisitions – a) Demande de mise à disposition pour plusieurs mois – Installation permanente et

conservation permanente des images par le propriétaire – b) Gravité des infractions poursuivies – Atteinte à la vie privée justifiée

1) La communication aux enquêteurs, et l'exploitation par ces derniers, des enregistrements des caméras de surveillance installées par le propriétaire ou le gestionnaire d'un ensemble d'habitations, dans les parties communes de l'immeuble concerné, n'est pas assimilable à un procédé de captation d'images relevant de l'article 706-96 du code de procédure pénale.

2) En l'espèce, le système de vidéosurveillance était en place et fonctionnait préalablement aux réquisitions délivrées par les enquêteurs au propriétaire, en vertu de l'autorisation générale qui leur avait été délivrée à cette fin par le procureur de la République.

a) Le fait que les enquêteurs aient inscrit dans le temps et pour les mois à venir leur demande de mise à disposition des enregistrements de vidéosurveillance n'est pas critiquable puisque, d'une part, cette installation technique était permanente, antérieure aux réquisitions des enquêteurs et était faite pour fonctionner au-delà de ces réquisitions et sans lien avec celles-ci, d'autre part, les enregistrements étaient de toute façon conservés par le propriétaire et à sa seule initiative.

b) En outre, eu égard à la gravité des infractions poursuivies, caractérisée par l'ampleur et la durée du trafic, la nature des produits concernés, et l'existence d'une organisation structurée avec de nombreux protagonistes dont certains déjà condamnés à de multiples reprises, l'exploitation des vidéosurveillances critiquées, qui ne portent que sur sept jours en 2020 et vingt-sept jours en 2021, dont seulement dix-sept concernent M. [I], constitue une atteinte à sa vie privée non seulement justifiée pour permettre la manifestation de la vérité, mais aussi proportionnée à un trafic de stupéfiants de cette ampleur.

Cass, crim., 8 novembre 2023, n°23-81.636, B., points 9-13

Utilisation par un employeur d'un dispositif de vidéosurveillance pour le contrôle des règles d'hygiène et de sécurité – Disproportion – Inopposabilité au salarié des enregistrements issus de cette vidéosurveillance dans le cadre d'une procédure de licenciement

Aux termes de l'article L. 1121-1 du code du travail, nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

La cour d'appel a constaté que le salarié, qui exerçait seul son activité en cuisine, était soumis à la surveillance constante de la caméra qui y était installée. Elle en a déduit à bon droit que les enregistrements issus de ce dispositif de surveillance, attentatoire à la vie personnelle du salarié et disproportionné au but allégué par l'employeur de sécurité des personnes et des biens, n'étaient pas opposables au salarié et a, par ces seuls motifs, légalement justifié sa décision.

Cass, soc., 23 juin 2021, n°19-13.856, B., points 5-6

Vidéosurveillance sur la voie publique – Pouvoir du procureur de la République – Conformité

Le procureur de la République tient des articles 39-3 et 41 du code de procédure pénale le pouvoir de faire procéder, sous son contrôle effectif et selon les modalités qu'il autorise s'agissant de sa durée et de son périmètre, à une vidéosurveillance sur la voie publique, aux fins de rechercher la preuve des infractions à la loi pénale. L'ingérence dans la vie privée qui résulte d'une telle mesure présentant par sa nature même un caractère limité et étant proportionnée au regard de l'objectif poursuivi, elle n'est pas contraire à l'article 8 de la Convention européenne des droits de l'homme.

Cass, crim., 8 décembre 2020, n° 20-83.885, B., points 9-10

Utilisation par un employeur d'un dispositif de vidéosurveillance continue pour lutter contre des vols susceptibles d'être perpétrés par ses propres salariés – Disproportion en l'espèce

Est disproportionné et peut légalement faire l'objet d'une sanction un dispositif de vidéosurveillance plaçant sous surveillance en permanence au moins un salarié. En l'espèce, la circonstance que la société ait voulu lutter contre des vols susceptibles d'être perpétrés par ses propres salariés ne permet pas de considérer que le dispositif était proportionné alors qu'en outre il était installé dans des locaux sécurisés, dont l'entrée ne peut s'effectuer qu'après autorisation et vérification d'identité.

CE, 10ème/9ème SSR, 18 novembre 2015, Société PS Consulting, n° 371196, Inédit., points 9-12

Durée de conservation des images issues d'un dispositif de vidéosurveillance - Obligation de supprimer ou d'anonymiser ces images au bout de quelques jours - Exception : survenance d'un incident justifiant la conservation des images pertinentes

En vertu de l'article 5-1-e du RGPD, il incombe au responsable de traitement de définir une durée de conservation conforme à la finalité du traitement. Lorsque cette finalité est atteinte, les données doivent être supprimées ou anonymisées ou faire l'objet d'un archivage intermédiaire pour les seules données pertinentes, lorsque leur conservation est nécessaire, par exemple pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses notamment. Au-delà des durées de conservation des données versées en archives intermédiaires, les données à caractère personnel doivent, sauf exception, être supprimées ou anonymisées.

A ce titre, la CNIL recommande une durée de conservation des images issues de la vidéosurveillance de quelques jours. Lorsqu'un incident est survenu et le justifie, les images pertinentes peuvent être conservées plus longtemps. La durée de conservation des images issues d'un dispositif de vidéoprotection, est quant à elle fixée à un mois maximum en application de l'article L 252-5 du code de la sécurité intérieure.

CNIL, P, 11 juillet 2024, mise en demeure, Association X, décision n° MED 2024-104, non publié

---

1) Application du principe de minimisation du dispositif de vidéosurveillance au regard de la finalité poursuivie – 2) Cas des lieux fréquentés majoritairement par des mineurs – 3) Cas des établissements scolaires

1) Pour apprécier le respect du principe de collecte de données adéquates, pertinentes et limitées en matière de vidéosurveillance, il convient de procéder à une analyse des conditions de mise en œuvre du dispositif concerné au regard de la finalité poursuivie, du nombre de caméras installées, de leur emplacement, leur orientation, leur fonctionnalité, leur période de fonctionnement et des caractéristiques propres à l'établissement concerné.

2) Si la CNIL ne remet pas en cause la légitimité de traitement ayant pour finalité d'assurer la sécurité des personnes et des biens, cette finalité ne saurait justifier de filmer, en permanence, des personnes qui sont en grande partie des mineurs.

3) S'agissant des établissements scolaires, la CNIL considère de manière constante que des caméras peuvent filmer les accès de l'établissement (entrées et sorties) et les espaces de circulation (couloirs). Elle estime en revanche que, eu égard à la sensibilité d'images qui filmeraient la vie quotidienne de

mineurs, parfois dans des moments d'intimité, dans un lieu déjà soumis à l'autorité du chef d'établissement et à la surveillance organisée par son personnel, les lieux de vie (tels que les salles de classe, la cour de récréation, la cantine et les toilettes) ne sauraient être filmés en continu, pendant les heures principales d'utilisation, sauf circonstances exceptionnelles.

CNIL, P, 1er septembre 2023, Mise en demeure, Association X, n MED-2023-070, non publié

Communication d'images issues du système de vidéosurveillance d'une copropriété aux forces de police – Conditions

Lorsque la finalité du système de vidéosurveillance installé dans une copropriété est la prévention et la poursuite des atteintes aux personnes et aux biens, la copropriété peut licitement, eu égard aux finalités du traitement et au regard du considérant 50 du RGPD, communiquer à son initiative les images issues du système de vidéosurveillance aux forces de l'ordre, si cette communication est utile aux finalités du traitement, notamment lorsqu'il s'agit de faits relevant d'une qualification pénale. Dans un tel cas, les forces de l'ordre interviennent en tant que destinataires du traitement et l'information sur le traitement prévu à l'article 13 du RGPD doit le mentionner. En toute autre hypothèse, et notamment si la communication se fait à la demande des forces de l'ordre ou pour des faits ne relevant pas des finalités du traitement définies par le syndic de copropriété, les forces de l'ordre doivent être regardées comme accédant aux données en qualité de tiers autorisé. Dans ce cadre, la communication de données à caractère personnel ne peut intervenir que sur réquisition judiciaire, dans le respect des dispositions pertinentes du code de procédure pénale.

CNIL, P, 13 mars 2023, Mise en demeure, Société X, n°2023-012, non publié

Dispositif de vidéosurveillance de salariés – 1) a) Exigences de minimisation des données et de proportionnalité – b) Illicéité de la surveillance permanente d'un salarié, sauf exception – 2) Cas d'un dispositif filmant en permanence des traducteurs destiné à protéger des documents traduits

1) a) La mise en œuvre d'un système de vidéosurveillance de salariés n'est licite qu'à condition de ne collecter que les données nécessaires à l'objectif poursuivi et de ne pas porter une atteinte disproportionnée aux droits et libertés de ceux-ci, ainsi qu'en dispose l'article L. 1121-1 du code du travail. Le nombre, l'emplacement, l'orientation, les périodes de fonctionnement des caméras ou la nature des tâches accomplies par les personnes concernées, sont autant d'éléments à prendre en compte lors de l'installation du système.

b)Si la surveillance de zones sensibles peut être justifiée par des impératifs de sécurité, le placement sous surveillance permanente de salariés, attentatoire à leur vie privée, ne peut toutefois intervenir que dans des circonstances exceptionnelles tenant, par exemple, à la nature de la tâche à accomplir. Il en est ainsi lorsqu'un employé manipule des objets de grande valeur ou lorsque le responsable de traitement est à même de justifier de vols ou de dégradations commises sur ces zones.

2) En l'espèce, est manifestement disproportionnée l'utilisation d'un dispositif de vidéosurveillance conduisant à placer des traducteurs assermentés sous une surveillance permanente en vue de protéger des documents traduits. En effet, si la nature des documents peut justifier la mise en place de mesures particulières de protection, il convient d'envisager des procédés alternatifs tels que la sécurisation des accès sur le lieu de travail.

CNIL, FR, 13 juin 2019, Sanction, Société X, n°SAN-2019-006, publié, points 31-36

Dispositif de vidéosurveillance filmant en permanence des salariés – Locaux exigus – Justification – Absence en l'espèce

Le placement sous surveillance continue des postes de travail des salariés n'est possible que s'il est justifié par une situation particulière ou un risque particulier auxquels sont exposées les personnes objets de la surveillance. Il appartient au responsable du traitement de justifier de ces circonstances et de la proportionnalité du traitement. En l'espèce, l'utilisation de dispositifs de vidéoprotection et vidéosurveillance constitue une réponse adaptée au risque de sécurité qui pèse sur les salariés du groupe dont les établissements ont subi un nombre important de cambriolages. Néanmoins, quand bien même l'objectif de sécurité assigné au dispositif est parfaitement légitime, les seules difficultés liées à l'exigüité des locaux ne peuvent justifier une atteinte disproportionnée à la vie privée des salariés ou leur mise sous surveillance constante.

CNIL, FR, 17 juillet 2014, Sanction, Société X, n°2014-307, publié, points 14-22

Voir aussi : CNIL, FR, 14 octobre 2014, Mise en demeure, Société X exploitant les magasins Y, n°2014-051, publié

6.13.3 Vidéo augmentée

Déploiement de dispositifs de caméras augmentées dans l'espace public poursuivant une finalité dite « police -justice » - Interdiction en l'absence de cadre légal spécifique

L'article 4, paragraphe 1, de la loi no 78-17 du 6 janvier 1978 dispose que les données à caractère personnel doivent être « traitées de manière licite, loyale ».

Par leur fonctionnement même, reposant sur la détection et l'analyse en continu et en temps réel des attributs ou des comportements des individus, les dispositifs de « caméras augmentées » présentent, par nature, des risques pour les personnes concernées. En outre, les dispositifs de « caméras augmentées » mis en oeuvre dans l'espace public à des fins de police administrative générale ou de police judiciaire sont susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques, raison pour laquelle un encadrement législatif apparaît nécessaire, en application de l'article 34 de la Constitution du 4 octobre 1958.

Dès lors, les dispositifs de caméras augmentées qui poursuivent une finalité dite de « police-justice » dans l'espace public sont interdits en l'absence de cadre légal spécifique.

En l'espèce, la commune utilisait de tels dispositifs en l'absence de cadre légal, notamment afin d'alerter les forces de l'ordre suite à la détection de véhicules roulant à contre-sens sur la chaussée et de détecter des attroupements lorsque le nombre de personnes détectées dans une zone définie dépassait un seuil préfixé.

CNIL, P, 24 juillet 2024, mise en demeure, Commune de X, décision n° MED 2024-109, non publié

6.14 Véhicules connectés

Géolocalisation d'un véhicule de location – Analyse de la proportionnalité de la collecte suivant chaque finalité de traitement – 1) Gestion de la flotte de véhicules et des contrats de location – 2) Lutte contre le vol de véhicules – 3) Localisation du véhicule en cas d'accident – Principe de minimisation des données

Le traitement de collecte et de conservation quasi permanente des données de géolocalisation d'un véhicule de location s'analyse au regard de la nécessité et de la proportionnalité de chacune de ses finalités.

1) S'agissant de la gestion de la flotte de véhicules et des contrats de location, l'activation de la géolocalisation quand l'utilisateur allume ou coupe le moteur peut être utile pour déterminer si le véhicule est de retour à son point de départ. *A contrario,* la collecte et la conservation des données de géolocalisation pendant le reste du trajet n'est pas nécessaire pour déterminer si le véhicule est de retour à sa station de départ en vue d'être restitué. En outre, s'agissant de l'usage de la géolocalisation pour contrôler l'entrée et la sortie d'un véhicule d'une zone de péage urbain, traitement qui n'est susceptible de s'appliquer en l'espèce que dans une seule ville de l'Union européenne, une collecte et conservation quasi permanente des données de géolocalisation sur l'ensemble des véhicules loués, sur le fondement de l'intérêt légitime, apparaissent disproportionnées par rapport à la finalité avancée qui est celle d'une facturation immédiate et automatisée des frais aux clients.

2) S'agissant de la lutte contre le vol de véhicules, les cas où, d'une part, la géolocalisation est le seul moyen de connaître la dernière position connue du véhicule et où, d'autre part, cette dernière position connue est effectivement proche de la localisation du véhicule, apparaissent limités. Dans ces situations, la CNIL ne remet pas en cause l'utilité de connaître la dernière position connue du véhicule grâce à la dernière donnée de géolocalisation. Cependant, cette hypothèse ne suffit pas à justifier la collecte et la conservation de l'ensemble des données de géolocalisation de l'ensemble des trajets des utilisateurs. Au surplus, d'autres mesures de sécurité pourraient être mises en place pour prévenir le vol des véhicules. Il en résulte que le fait de procéder systématiquement à cette collecte et conservation des données de géolocalisation pour les cas d'usages où elle pourrait être effectivement utile, alors que d'autres moyens de prévention et de lutte contre le vol existent, sur le fondement de l'intérêt légitime de la société, porte une atteinte disproportionnée à la vie privée des utilisateurs.

3) S'agissant de la localisation du véhicule en cas d'accident, la CNIL estime que la géolocalisation tous les 500 mètres de l'ensemble des véhicules au cours de toute la durée de location, avec conservation des données, préalablement à toute information relative à un accident, n'est pas nécessaire pour porter assistance à un utilisateur.

Lorsqu'aucune des finalités avancées par le responsable du traitement n'est susceptible de justifier une collecte et la conservation des données de géolocalisation, ces opérations de traitement constituent un manquement à l'article 5.1.c du RGPD

CNIL, FR, 7 juillet 2022, Sanction, Société X, n°SAN-2022-015, publié, points 42,45, 55, 60

7. Actes administratifs encadrant des traitements particuliers

7.1 Actes réglementaires créant des traitements publics

7.1.1 Obligation d'encadrer un traitement par une loi ou un règlement

Données personnelles des membres d'équipage – Directive (UE) 2016/681 – Surtransposition – Disposition ne relevant pas du périmètre de la directive – Possible création par voie réglementaire d'un traitement relatif à ces données

Le Conseil d'État (section de l'intérieur) saisi d'un projet de décret relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire), lui donne un avis favorable, sous réserve des dispositions relatives à la collecte et au traitement des données d'enregistrement et d'embarquement (données API) des membres d'équipage.

Il relève que si la directive (UE) 2016/681 relative à l'utilisation des données des dossiers passagers (PNR), autorise expressément la collecte des données API, ne sont concernées que les données des passagers dont est expressément exclu le personnel d'équipage conformément à la définition donnée par l'article 3.

Le Conseil d'État estime que s'il est loisible au Gouvernement de créer, par voie réglementaire, un traitement automatisé de données à caractère personnel relatives aux données des membres d'équipage, seule une modification de nature législative serait de nature à mettre à la charge des transporteurs aériens l'obligation de transmettre de telles données.

CE, Section de l'intérieur, 26 juin 2018, Avis n° 394649, Projet de décret relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure

---

Enquêtes administratives – Relevés signalétiques, dont empreintes digitales – Compétence du pouvoir réglementaire – Existence

L'article 116 de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale a introduit, dans le code de la défense, un article L. 2381-1. Le I de cet article prévoit que, dans le cadre d'une opération mobilisant des capacités militaires se déroulant sur un théâtre d'opérations extérieures, des membres des forces armées et des formations rattachées pourront procéder à des relevés signalétiques ou à des prélèvements biologiques destinés à établir, dans certaines hypothèses, l'identification de personnes décédées ou capturées au cours des combats. Le II du même article a pour objet de permettre à l'autorité militaire, sur ces mêmes théâtres d'opérations extérieures, lors des enquêtes préalables à une décision de recrutement ou d'accès à une zone protégée, de consulter les données collectées en application du I. Le législateur a renvoyé à un décret en Conseil d'État le soin de fixer la liste des enquêtes qui donneront lieu à cette consultation ainsi que les modalités d'information des personnes concernées.

Saisi d'un projet de décret relatif à ces enquêtes administratives, le Conseil d'État (section de l'administration) souligne que le II de l'article L. 2381-1 du code de la défense ne permet pas aux autorités militaires de pratiquer, lors de telles enquêtes, des prélèvements d'empreintes biologiques, cette disposition se bornant à autoriser l'autorité militaire à consulter les données collectées sur le fondement du I. Les cas dans lesquels il est permis de pratiquer des prélèvements d'empreintes génétiques sont définis de manière limitative à l'article 16-11 du code civil. Par ailleurs, le Conseil d'État rappelle que si le pouvoir réglementaire peut, même dans le silence de la loi, imposer pour les

besoins des enquêtes des relevés signalétiques, notamment la prise d'empreintes digitales, la Commission nationale de l'informatique et des libertés doit alors être préalablement saisie et rendre un avis motivé et publié.

Une telle disposition réglementaire aurait en effet pour objet et pour effet d'autoriser un traitement « de données à caractère personnel mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes » au sens du 2 du I de l'article 27 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

CE, Section de l'administration, 6 décembre 2016, Avis n° 392250, Projet de décret relatif à certaines enquêtes administratives prévues par le code de la défense

---

Acte réglementaire régissant un traitement au nom de l'Etat – 1) Compétence de la formation restreinte à l'égard de toutes les administrations de l'Etat intervenant dans le traitement – Existence – 2) Application au TAJ

1) S'agissant des traitements de l'Etat, lorsqu'un acte réglementaire le régissant désigne le ou les ministères exerçant la responsabilité de traitement au nom de l'Etat, cela ne fait pas obstacle à la compétence de la CNIL pour contrôler et, le cas échéant, prononcer une injonction à l'égard des autres administrations de l'Etat à qui l'acte réglementaire confie un rôle dans la mise en œuvre de traitement.

2) S'agissant du traitement des antécédents judiciaires (TAJ), l'article R. 40-23 du code de procédure pénale dispose que le ministère de l'intérieur exerce la responsabilité de traitement. Cependant, la responsabilité du traitement relevant, in fine, de l'Etat, la formation restreinte estime qu'elle est compétente pour adresser un rappel aux obligations et une injonction aux administrations de l'Etat qui ne relèvent pas du ministre de l'intérieur auxquelles le code de procédure pénale confie un rôle dans la mise en œuvre du traitement. Elle s'estime donc compétente pour prononcer ces mesures à l'égard du ministère de la justice, à qui les articles 230-8, 230-9 et R. 40-31 et suivants du code de procédure pénale confient, au sein de l'Etat, un rôle pour assurer le respect par le traitement des règles fixées par la loi Informatique et libertés.

CNIL, FR, 17 octobre 2024, Sanction, Ministère de l'intérieur et des Outre-Mer et ministère de la justice, no SAN-2024-017, publié

Exclusion du droit d'opposition par une « mesure législative » (art. 23 RGPD) – 1) Autorités pouvant écarter le droit d'opposition par voie réglementaire – Collectivités territoriales et établissements publics – Inclusion – 2) Conditions et garanties

1) L'article 23 du RGPD permet de limiter ou d'écarter le droit d'opposition à un traitement, à certaines conditions, par une « mesure législative ». Le considérant 41 du RGPD précise que cette « mesure législative » n'est pas nécessairement un acte adopté par le Parlement, mais doit être déterminée par le droit national de chaque État membre. En France, il peut en particulier s'agir d'un acte réglementaire. La CNIL estime que, s'agissant des traitements participant de l'exécution d'une mission d'intérêt public, tant l'État que les collectivités territoriales ou les établissements publics peuvent, dans leurs domaines de compétence respectifs et s'ils disposent d'un pouvoir réglementaire, limiter ou exclure le droit d'opposition.

2) Cependant, l'exercice de cette faculté est soumis à une double limite : d'une part, s'agissant de la compétence, ne pas empiéter sur le domaine réservé à la loi en application de l'article 34 de la Constitution ; d'autre part, veiller à ce que les conditions prévues à l'article 23 soient respectées. Dans ses lignes directrices 10/2020 du 13 octobre 2021 sur l'article 23, le Comité européen pour la protection des données a notamment rappelé l'obligation pour le responsable de traitement de veiller au caractère strictement nécessaire et proportionné de la limitation envisagée au regard de l'objectif

poursuivi. Il a également souligné que l'acte écartant l'opposition doit faire l'objet d'une publicité suffisante et être accessible.

CNIL, SP, 16 février 2023, Avis sur projet de décision, Création d'un fichier central des titres permanents du permis de chasser, n°2023-015, publié, point 16

7.1.2 Éléments devant figurer dans le texte portant création d'un traitement

Traitement ayant pour finalités de garantir le droit au séjour des ressortissants étrangers en situation régulière et de lutter contre l'entrée et le séjour irrégulier en France – Contenu du décret – 1) Rappel des principes du RGPD – Absence – 2) Modalités de délivrance de l'information aux personnes concernées – Absence

1) Dans le cadre d'un traitement automatisé autorisé par la loi et ayant pour finalités de garantir le droit au séjour des ressortissants étrangers en situation régulière et de lutter contre l'entrée et le séjour irréguliers en France des ressortissants étrangers, un décret se bornant à apporter à ce traitement les modifications nécessaires pour les besoins du téléservice n'a pas à rappeler les principes relatifs au traitement des données à caractère personnel énoncés par l'article 5 du RGPD, ni les obligations du responsable de traitement fixées par l'article 24 du même règlement.

2) Le droit d'information n'impose pas que l'acte portant création du traitement automatisé de données à caractère personnel, ni l'acte modifiant ses caractéristiques, fixe les modalités d'une telle information.

CE, Section, 3 juin 2022, Conseil national des barreaux, n° 452798, Rec., points 14-15

Exploitation ultérieure de données dans d'autres traitements – Obligation d'indiquer la nature et l'objet des traitements ultérieurs concernés

Le décret n°2020-151 du 20 février 2020 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « application mobile de prise de notes » (GendNotes) autorise le ministre de l'intérieur à mettre en œuvre un traitement automatisé de données à caractère personnel dénommé GendNotes.

L'une des finalités du traitement est de « faciliter le recueil et la conservation « en vue de leur exploitation ultérieure dans d'autres traitements de données » » notamment par le biais d'un système de pré-renseignement des données collectées.

Le Conseil d'État annule ledit décret au motif que le traitement ne satisfait pas à l'exigence « déterminée, explicite et légitime ». En effet, dès lors qu'un décret prévoit, au titre des finalités du traitement, sa mise en relation avec d'autres traitements, il doit comporter des indications quant à la nature ou à l'objet des traitements concernés ou aux conditions d'exploitation, dans ces autres traitements, des données collectées par le traitement initial, afin de satisfaire pas à l'exigence d'une finalité « déterminée, explicite et légitime » énoncée au 2° de l'article 4 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

CE, 10ème-9ème chambres réunies, Ligue des droits de l'homme, 13 avril 2021, n°439360, Inédit., points 8, 14-15

Secret médical (art. L. 1110-4 du CSP) – Accès aux données du dossier médical des patients – 1) Accès des commissaires aux comptes – Méconnaissance, en tant que ne sont pas prévues des mesures techniques et organisationnelles propres à garantir le respect du secret médical – 2) Accès des prestataires extérieurs – Illégalité, en tant qu'il n'est pas assorti de garanties suffisantes pour assurer que l'accès n'excède pas celui strictement nécessaire à l'exercice de leur mission

Décret n° 2018-1254 du 26 décembre 2018 prévoyant l'accès des commissaires aux comptes, dans le cadre de leur mission légale de certification des comptes des établissements publics de santé, et de prestataires extérieurs, aux fins de traitement des données, aux données du dossier médical des patients, lesquelles portent sur l'identité du patient, son lieu de résidence, ses pathologies et les actes de diagnostic et de soins réalisés au cours de son séjour dans l'établissement.

1) Il résulte de l'article L. 823-9 du code de commerce que les commissaires aux comptes doivent seulement, pour l'accomplissement de leur mission légale de certification des comptes des établissements publics de santé, être en mesure de justifier que les comptes annuels de ces établissements sont réguliers et sincères et donnent une image fidèle du résultat des opérations de l'exercice écoulé ainsi que de leur situation financière et de leur patrimoine.

Il ressort des pièces du dossier, notamment des observations de caractère général présentées par le Haut Conseil du commissariat aux comptes (H3C) en application de l'article R. 625-3 du code de justice administrative, que l'accès à l'ensemble des données de santé, issues du dossier médical des patients, mentionnées à l'article R. 6113-1 du code de la santé publique (CSP), est nécessaire à l'accomplissement de cette mission, pour un échantillon de dossiers permettant de vérifier par sondage la fiabilité et la traçabilité des données utilisées pour le calcul des recettes de l'établissement, depuis l'admission du patient jusqu'à la facturation.

En revanche, il n'en ressort pas que cette mission ne puisse être accomplie à partir de données faisant l'objet de mesures de protection techniques et organisationnelles adéquates, telles que - à défaut du recours, à titre d'expert, à un médecin responsable de l'information médicale dans un autre établissement - la pseudonymisation des données, dont l'article 25 du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD) prévoit la mise en œuvre pour protéger les droits de la personne concernée et garantir, à cette fin, que les personnes dont les données sont traitées ne puissent être identifiées.

Par suite, si le décret attaqué a pu, sans méconnaître la portée de l'article L. 6113-7 du CSP, pour encadrer les conditions dans lesquelles les commissaires aux comptes ont accès à ces données, se borner, d'une part, à prévoir qu'ils peuvent seulement les consulter, dans le cadre de leur mission légale, sans création ni modification de données, avec une information adaptée des patients, en en limitant la conservation à la durée strictement nécessaire à cette mission et en rappelant l'obligation de secret à laquelle ils sont soumis et, d'autre part, à limiter leur accès aux seules données « nécessaires (...) dans la stricte limite de ce qui est nécessaire à leurs missions », sans exclure par principe leur accès à aucune de ces données, il est en revanche entaché d'illégalité en tant qu'il ne prévoit pas de mesures techniques et organisationnelles propres à garantir la protection du droit de la personne concernée au respect du secret médical rappelé par l'article L. 1110-4 du CSP.

2) En se bornant à prévoir que les prestataires extérieurs qui contribuent au traitement des données à caractère personnel mentionnées à l'article R. 6113-1 du CSP sont placés sous la responsabilité du médecin responsable de l'information médicale, qu'ils interviennent dans le cadre de leur contrat de sous-traitance, qu'ils sont soumis à l'obligation de secret, dont la méconnaissance est punie conformément aux articles 226-13 et 226-14 du code pénal, qu'ils peuvent accéder « aux seules données à caractère personnel nécessaires (...) dans la stricte limite de ce qui est nécessaire à leurs missions » et qu'ils ne peuvent conserver les données mises à disposition par l'établissement au-delà de la durée strictement nécessaire aux activités qui leur ont été confiées par contrat, sans prévoir de mesures techniques et organisationnelles propres à assurer que seules sont traitées, avec des garanties suffisantes, les données identifiantes qui sont nécessaires au regard des finalités du traitement ni de dispositions destinées à garantir qu'ils accomplissent effectivement ces activités sous l'autorité du praticien responsable de l'information médicale, quel qu'en soit le lieu, le décret attaqué n'a pas prévu

de garanties suffisantes pour assurer que l'accès aux données n'excède pas celui qui est strictement nécessaire à l'exercice de la mission qui leur est reconnue par la loi.

CE, 1ère-4ème chambres réunies, 25 novembre 2020, Conseil national de l'ordre des médecins, n° 428451, T., points 10, 13

Acte créant le traitement – Obligation d'information des personnes concernées – Application sans que l'acte n'ait à le rappeler

L'obligation de fournir aux personnes dont certaines données à caractère personnel sont collectées une information « concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant » prévue au 1 de l'article 12 du RGPD s'impose sans que l'acte créant le traitement n'ait à le rappeler.

CE, 1ère-4ème chambres réunies, 5 février 2020, Unicef France et autres, n° 428478, T., point 23

Fichier « Système d'information d'identification unique des victimes » – Acte réglementaire – Obligation de prévoir des durées de conservation

L'article L. 3131-9-1 du code de la santé publique, introduit par l'article 60 de la loi n° 2016-1827 du 23 décembre 2016 de financement de la sécurité sociale pour 2017, a posé le cadre d'un système d'information unique permettant l'identification et le suivi de la prise en charge des victimes dans le cadre d'une situation sanitaire exceptionnelle.

Il prévoit notamment que « les informations strictement nécessaires à l'identification des victimes et à leur suivi, notamment pour la prise en charge de leurs frais de santé, sont recueillies dans un système d'identification unique des victimes » et qu'« un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, précise la nature des données recueillies et fixe les modalités de cette transmission dans le respect des règles garantissant la protection de la vie privée ».

Le projet de décret présenté par le Gouvernement pris pour l'application de ces dispositions ne contenait pas de dispositions limitant dans le temps la conservation des données collectées et traitées. Le Conseil d'État (section sociale) a estimé que la limitation de la durée de conservation de ces données était une mention indispensable puisqu'en vertu de l'article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les données à caractère personnel ne peuvent être conservées que pendant la durée nécessaire aux finalités pour lesquelles elles ont été collectées et traitées. Il a donc introduit une telle limitation à l'article 2 du projet.

CE, Section sociale, 13 février 2018, Avis n° 394140, Projet de décret pris pour l'application de l'article L. 3131-9-1 du code de la santé publique

---

Renvoi de l'acte réglementaire à un arrêté ministériel pour préciser la nature des données susceptibles d'être enregistrées – Exclusion

L'acte réglementaire créant un traitement de données à caractère personnel ne peut en principe, en ce qui concerne la nature des données à caractère personnel susceptibles d'être enregistrées, renvoyer à un arrêté ministériel. Mais le Conseil d'État constate que la CNIL a pu, dans le cadre de l'avis qu'elle a rendu sur le projet de décret, prendre connaissance du contenu de l'arrêté auquel renvoyait le projet. Il estime dès lors qu'il était possible de mentionner dans le décret lui-même les catégories de données prévues, et qu'elles seront précisées par un arrêté ministériel.

CE, Section de l'intérieur, 17 janvier 2017, Avis n° 392228, Projet de décret pris pour l'application des articles L. 744-6 et L. 744-7 du code de l'entrée et du séjour des étrangers et du droit d'asile et portant création du traitement automatisé de donnée à caractère personnel

---

Durée de conservation des empreintes digitales relevées lors d'une demande de carte nationale d'identité – Durée illimitée faute de dispositions expresses la régissant – Illégalité

Faute de dispositions expresses la régissant, la durée de conservation des empreintes digitales relevées sur le fondement de l'article 5 du décret du 22 octobre 1955 est illimitée. Une telle durée de conservation ne peut être regardée comme nécessaire aux finalités du fichier, eu égard à la durée de validité de la carte nationale d'identité et au délai dans lequel tout détenteur d'une carte nationale d'identité périmée peut en solliciter le renouvellement. Elle est donc illégale.

CE, 10ème/9ème SSR, 18 novembre 2015, Mme T... et Mme M..., n°372111, Rec., point 6

Conservation des données pour une durée de huit ans pour une finalité non précisée par le décret (conduite éventuelle de contentieux) – Conséquence – Absence de limitation de l'accès à ces données au seul besoin d'en connaitre au regard de cette finalité – Illégalité – Existence

Décret créant un traitement nominatif relatif aux détenus comportant notamment des données relatives à leurs antécédents médicaux ayant pour finalité l'exécution des sentences pénales et des décisions de justice s'y rattachant, la gestion de la détention des personnes placées sous main de justice et écrouées, la sécurité des personnes détenues et des personnels et la mise en œuvre du « parcours pluridisciplinaire de la personne détenue ».

Eu égard à la finalité du fichier ayant notamment trait à la gestion des contentieux entre l'administration pénitentiaire et les personnes placées sous main de justice, la durée de conservation de deux ans prévue à l'article R. 57-9-21 à compter de la date de levée d'écrou n'est pas excessive. En revanche, la conservation ultérieure de ces données pour un délai de huit ans, qui poursuit, selon la garde des sceaux, la conduite éventuelle de contentieux, est dépourvue de fondement légal dès lors que cette finalité n'est pas explicitée par le décret attaqué et que la durée de conservation ainsi définie ne s'y rattache pas spécifiquement.

CE, 10ème/9ème SSR, 9 novembre 2015, Conseil national de l'ordre des médecins, n° 383313, Inédit., point 8

Accédants au traitement–Formule à privilégier dans l'acte réglementaire

Lorsque l'acte réglementaire désigne les personnes qui opèrent le traitement sous l'autorité du responsable de traitement, dites « accédants au traitement », la Commission invite le ministère, pour éviter toute ambiguïté, à ne pas utiliser une formule indiquant « qu'ils accèdent à tout ou partie des données », dès lors qu'ils sont généralement également appelés à enregistrer ou effacer des données. Elle invite le Gouvernement à utiliser une autre formule, par exemple en indiquant qu'ils « accèdent au traitement ».

CNIL, P, 20 octobre 2022, Avis sur projet de décret, « Système Informatisé de Recoupement, d'Orientation et de Coordination des procédures de Criminalité Organisée » (SIROCCO), n° 2022-105, publié, point 33

Traitements publics encadrés par un acte réglementaire – 1) Obligation d'inscrire l'archivage intermédiaire dans l'acte réglementaire – Appréciation d'espèce – 2) Obligation d'inscrire l'archivage définitif dans l'acte réglementaire – Absence

Cas d'un traitement de l'État permettant d'enregistrer des informations sur les ressortissants français et leurs ayants droit ainsi que documents relatifs à une situation de crise à l'étranger en vue d'en faciliter la gestion et d'informer et associer les personnes concernées.

1) Une fois que les données ne sont plus utilisées dans le cadre de la gestion opérationnelle liée à l'évènement survenu à l'étranger ou pour réaliser les statistiques prévues, il est recommandé de mettre en place un archivage intermédiaire afin de limiter la consultation de ces données à des personnes spécifiquement habilitées. Eu égard à l'écart entre la durée d'utilisation opérationnelle des données et leur durée de conservation en base intermédiaire (10 ans), le principe d'un tel archivage intermédiaire devrait en l'espèce être inscrit dans le décret portant création du traitement, à titre de garantie apportée aux personnes concernées.

2) S'agissant de l'archivage définitif au titre de l'application des règles régissant les archives publiques issues du code du patrimoine, un acte réglementaire régissant un traitement public réserve toujours implicitement l'application des obligations du code du patrimoine et l'archivage définitif n'a pas besoin d'être expressément prévu par l'acte réglementaire.

CNIL, P, 21 avril 2022, Avis sur projet de décret, n° 2022-051, non publié

Décret précisant les modalités et les conditions de recevabilité de la saisine d'une institution par voie de pétition – Système de journalisation permettant une traçabilité des opérations de consultation, création et modification des données prévu dans le texte – Obligation de mise en place par l'administration

Dans le cadre d'un décret précisant les modalités et les conditions de recevabilité de la saisine d'une institution par voie de pétition, définissant notamment les règles relatives à l'accès aux informations collectées, la mise en place d'un système de journalisation, permettant de conserver une trace des opérations de consultation, création et modification des données est indispensable, conformément à la délibération de la CNIL n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation.

En particulier, une durée de conservation des journaux de six à douze mois est préconisée, et ces journaux doivent faire l'objet d'un contrôle automatique régulier, afin de détecter les comportements anormaux et de générer des alertes le cas échéant. Le traitement proactif de ces journaux est d'autant plus pertinent que les données relatives à une pétition ont vocation à être traitées rapidement et peuvent conduire à des prises de décisions significatives pour l'institution et la société.

Si aucune disposition du RGPD n'impose effectivement de prévoir un système de journalisation dans l'acte réglementaire créant le traitement, le fait de le prévoir dans le décret oblige l'administration à le mettre en place et constitue une garantie importante. Il est d'ailleurs à noter que de nombreux décrets et arrêtés réglementant des traitements de données à caractère personnel le prévoient.

CNIL, P, 17 février 2022, Avis sur projet de décret, CESE, n° 2022-023, publié, point 18

Notions d'accédants et de destinataires – Habilitations des accédants

Le terme « accédant », que n'utilise ni le RGPD, ni la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés mais qui a été créé par la doctrine, désigne, s'agissant d'un traitement automatisé de données mis en œuvre par une administration et encadré par un acte

réglementaire, les personnes qui, au sein du responsable de traitement, seront appelées à effectuer les diverses opérations de traitement et, à ce titre, à accéder au système informatique en cause.

Les habilitations des différents accédants peuvent être définies par l'acte réglementaire, et ne se limitent généralement pas à la seule consultation des données mais incluent aussi l'enregistrement, la correction ou l'effacement des données.

Par ailleurs, au sens de la réglementation, et notamment du RGPD, les « destinataires » sont les personnes à qui le responsable de traitement peut être amené à communiquer les données et sur lesquelles il doit fournir une information aux personnes concernées. En pratique, cette communication peut prendre plusieurs formes, qu'il s'agisse d'une transmission d'un extrait des données ou d'une simple faculté de consultation par un accès sécurisé au système informatique.

Lorsqu'un projet de décret mentionne des personnes comme « accédants aux données » alors qu'elles ne seront pas seulement chargées de consulter les données mais également de décider de leur recueil, ce point doit être précisé pour éviter toute ambiguïté.

CNIL, P, 13 janvier 2022, Avis sur projet de décret, Caméras installées sur des aéronefs circulant sans personne à bord, n° 2022-006, publié, points 26-27

Voir aussi : CNIL, P, 20 janvier 2022, Avis sur projet de décret, Titre IV du livre II du code de la sécurité intérieure, n° 2022-005, publié

Logiciels de rédaction d'actes relatifs aux procédures de la gendarmerie nationale 1) Imprécision de la catégorie de données « éléments issus des constatations et investigations strictement nécessaires à la conduite et à la résolution de la procédure judiciaire » – Admissibilité en l'espèce – 2) a) Mises en relation de traitements – Finalité propre et distincte ou unique – Obligation de mentionner l'objet de ces mises en relation – Conditions – b) Mention non obligatoire de toutes les interconnexions, rapprochements ou autres mises en relation – Recommandation aux responsables de traitement – c) Conditions de licéité des mises en relation

1) La catégorie de données « éléments issus des constatations et investigations strictement nécessaires à la conduite et à la résolution de la procédure judiciaire » est en principe trop imprécise pour fournir un encadrement satisfaisant à un traitement régi par un acte réglementaire. Néanmoins, dans le cas particulier d'un logiciel de rédaction d'actes relatifs aux faits les plus divers en lien avec toutes les procédures auxquelles participe la gendarmerie nationale, et eu égard à la difficulté particulière qui s'attache à l'énumération de toutes les catégories de données à caractère personnel pouvant être traitées dans un tel cadre, une telle formulation peut être admise.

2) a) Une mise en relation de traitements ne constitue pas en elle-même une finalité d'un traitement, qui devrait alors figurer expressément dans l'acte réglementaire en autorisant la mise en œuvre, mais un moyen concourant à une finalité du traitement. Lorsque la mise en relation avec un autre traitement poursuit une finalité propre et distincte des finalités précisées dans l'acte autorisant la mise en œuvre du traitement en cause ou lorsque cette mise en relation constitue l'unique finalité de ce traitement, les articles 4 et 35 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés impose de mentionner l'objet de ces mises en relation dans l'acte réglementaire de manière suffisamment explicite et précise.

b) Si la liste de toutes les interconnexions, rapprochements ou autres mises en relation ne doit pas nécessairement figurer dans l'acte autorisant la création d'un traitement, leur mention peut néanmoins constituer une bonne pratique dans certains cas particuliers, notamment lorsque ces mises en relation sont étroitement liées aux finalités du traitement concerné. À défaut d'une telle mention, il est recommandé aux responsables de traitements autorisés par acte réglementaire, en particulier pour les traitements correspondant à des bases de données importantes, de décrire sur leur site web l'ensemble des mises en relation réalisées avec d'autres bases de données.

c) Lorsque des traitements mis en relation sont encadrés par des actes réglementaires, la mise en relation doit respecter les dispositions régissant les traitements concernés, que cette mise en relation soit ou non mentionnée dans les actes autorisant la création de ces traitements. En particulier, l'opération de mise en relation doit être conforme aux finalités, aux catégories de données et aux accédants ou destinataires fixés par les actes réglementaires concernés. Pour être licite, le transfert de données d'une base vers une autre doit ainsi s'inscrire ou concourir aux finalités poursuivies par la base d'origine ou à celles associées aux transmissions à des destinataires, les données transférées doivent être autorisées à figurer dans la base de destination et au moins une personne habilitée à alimenter la base de destination doit constituer un accédant ou un destinataire de la base d'origine.

CNIL, SP, 27 mai 2021, Avis sur projet de décret, LRPGN, n° 2021-061, publié, point 28

Voir aussi : CE, 10ème-9ème chambres réunies, 13 avril 2021, Ligue des droits de l'homme et autres, n° 439360, Inédit.

Traitements de données personnelles mis en œuvre pour la sécurité d'un traitement source – Absence d'obligation de figurer dans le décret – Mention dans l'analyse d'impact

Lorsqu'un utilisateur se connecte à l'application StopCovid France, l'adresse IP de l'ordiphone est collectée dans le cadre de la solution anti DDOS de la société ORANGE, la collecte de cette donnée à caractère personnel ayant comme seule finalité, en l'espèce, d'assurer la sécurité du dispositif.

Dans la mesure où la solution anti DDOS est une solution de sécurité du dispositif, qui n'a pas à figurer dans le décret du 29 mai 2020, les données traitées par cette solution n'ont pas non plus à figurer dans ce décret. La collecte des adresses IP dans ce cadre n'est donc pas irrégulière. En revanche, dès lors que cette solution de sécurité entraine une collecte de données à caractère personnel, la description de cette opération de traitement doit apparaître dans l'analyse d'impact réalisée par le responsable de traitement.

CNIL, P, 15 juillet 2020, Mise en demeure, X, n °MED-2020-015, publié, points 45-48

7.1.3 Procédure d'autorisation particulière

Recherche et développement en matière de capacités techniques de recueil et d'exploitation des renseignements – Dispositions expresses prévoyant un mécanisme d'autorisation de mise en œuvre de tels traitements – Conséquence – Application du régime d'autorisation préalable de la loi Informatique et Libertés – Absence

Des dispositions législatives spéciales peuvent déroger au régime de formalités préalables prévu par la loi du 6 janvier 1978 modifiée. Les dispositions des titres I et IV de la loi du 6 janvier 1978 modifiée ont vocation à s'appliquer aux traitements intéressant la sûreté de l'État, tel que le traitement des données collectées par le biais de techniques de recueil de renseignement à des fins de recherche et de développement en matière de capacités techniques de recueil et d'exploitation des renseignements, sous réserve des dispositions spéciales du code de la sécurité intérieure y dérogeant. À cet égard, dès lors que des dispositions expresses prévoient un mécanisme spécifique d'autorisation de mise en œuvre de tels traitements, les programmes de recherche ne nécessitent pas l'autorisation par arrêté ministériel ou décret en Conseil d'État pris après avis de la Commission prévue par l'article 31 de la loi précitée.

CNIL, SP, 8 avril 2021, Avis sur projet de loi, PJL Renseignement, n° 2021-040, publié, points 38-40

7.2 Cas des traitements régis par les articles 31 et 32 de la loi Informatique et Libertés

Traitement relevant de la directive « Police-Justice » susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques et mis en œuvre pour le compte de l'État – Analyse d'impact devant être réalisée et transmise à la CNIL avant l'édiction de l'acte définissant le traitement

Il résulte de l'article 90 de la loi du 6 janvier 1978 applicable aux traitements de données à caractère personnel relevant de la directive (UE) 2016/80 du 27 avril 2016, mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, que, lorsqu'est exigée une analyse d'impact préalablement à la création ou à la modification d'un tel traitement mis en œuvre pour le compte de l'État, il appartient à l'administration, à peine d'irrégularité de l'acte instituant ou modifiant ce traitement, de la réaliser et de la transmettre à la Commission nationale de l'informatique et des libertés (CNIL) dans le cadre de la demande d'avis prévue à l'article 33 de la loi du 6 janvier 1978.

CE, 10ème-9ème chambres réunies, 24 décembre 2021, Ligue des droits de l'homme et autres, n° 447513, T., point 12

Voir aussi : CE, 10ème–9ème chambres réunies, 24 décembre 2021, Ligue des droits de l'homme et autres, n° 447515, Inédit.

Mention des modalités d'information des personnes dont les données sont recueillies – Absence d'obligation

Il ne résulte pas des dispositions des articles 29 et 32 de la loi du 6 janvier 1978 que l'acte portant création d'un traitement de données à caractère personnel doive mentionner les modalités d'information des personnes dont les données sont recueillies.

CE, 10ème-9ème chambres réunies, 4 octobre 2019, Association Cercle de réflexion et de proposition d'actions sur la psychiatrie, n° 421329, 422497, 424818, Rec., point 22

Traitement relevant du RGPD ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou des mesures de sûreté (art. 31 de la loi du 6 janvier 1978) – Notion – Traitement ayant pour finalité le transfert de données fiscales vers l'administration fiscale américaine – Inclusion

Accord conclu le 14 novembre 2013 entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et de mettre en œuvre la loi relative au respect des obligations fiscales concernant les comptes étrangers (dite « loi FATCA »). Traitement d'échange automatique d'informations organisant notamment la collecte et le transfert de données à caractère personnel aux autorités fiscales américaines créé pour la mise en œuvre de cet accord.

Si le traitement créé par l'arrêté du 5 octobre 2015 a pour finalité de lutter contre la fraude et l'évasion fiscales et relève à ce titre du RGPD et non de la directive n° 2016/680, il doit être regardé comme ayant parmi ses objets la prévention, la recherche, la constatation ou la poursuite des infractions

pénales. Il s'ensuit, eu égard à cet objet, qu'il est au nombre des traitements visés à l'article 31 de la loi n° 78-17 du 6 janvier 1978.

CE, Assemblée, 19 juillet 2019, Association des Américains accidentels, n°424216, Rec., point 8

Traitement mis en œuvre par l'administration fiscale, permettant à des tiers de consulter les données fiscales d'un particulier pour vérifier l'authenticité des données que celui-ci leur a fournies – Définition insuffisamment précise des personnes susceptibles de consulter ce traitement – Conséquence – Méconnaissance de l'article 29 de la loi du 6 janvier 1978 dans sa rédaction applicable au litige

Arrêté créant un traitement ayant pour objet de permettre à des tiers à qui un contribuable a communiqué une copie de son avis d'impôt sur le revenu ou de son justificatif d'impôt sur le revenu, de vérifier l'authenticité des données qui y figurent au moyen d'une consultation directe du justificatif d'impôt sur le revenu du contribuable certifié par l'administration fiscale.

Les destinataires du traitement ne sont définis, par les dispositions de l'arrêté attaqué, que comme les personnes ayant besoin, dans le cadre de leurs activités, de connaître et de vérifier l'authenticité des informations contenues dans le justificatif d'impôt sur le revenu d'un contribuable. Une telle définition ne peut être regardée, eu égard à l'importance des données en cause, comme précisant suffisamment les destinataires ou catégories de destinataires habilités à en recevoir communication, comme l'exige l'article 29 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et Libertés. Dès lors que les dispositions en cause ne sont pas divisibles du reste de l'arrêté attaqué, celui-ci doit être déclaré illégal.

CE, 10ème-9èmechambres réunies, 24 avril 2019, Caisse d'épargne et de prévoyance Languedoc-Roussillon, n°419498, T., point 8

Traitement destiné au recensement, à la gestion et au suivi des déclarations rectificatives – Mise en conformité avec la législation fiscale – Création subordonnée à la prise d'un arrêté du ministre compétent après avis de la CNIL

Doit être regardé comme ayant parmi ses objets celui de prévenir la continuation et la réitération d'infractions pénales, au sens des dispositions du 2° du I de l'article 26 de la loi du 6 janvier 1978 applicable au litige, le traitement destiné au recensement, à la gestion et au suivi des déclarations rectificatives faites spontanément par les contribuables en vue de la mise en conformité avec la législation fiscale de leurs avoirs détenus à l'étranger non déclarés à l'administration fiscale, qui contribue à éviter la continuation et la réitération de comportements susceptibles d'être constitutifs de fraude fiscale et pouvant, le cas échéant, faire l'objet de poursuites pénales. Par suite, la création d'un tel traitement ne peut résulter que d'un arrêté du ministre compétent, pris après avis motivé de la CNIL.

CE, 10ème-9ème chambres réunies, 23 octobre 2017, Conseil national des barreaux, n° 394474, Rec., point 5

Traitements mis en œuvre pour le compte de l'État relatif à la sûreté de l'État, la défense ou la sécurité publique faisant apparaître directement ou indirectement des données sensibles – Autorisation par décret en Conseil d'État pris après avis motivé et publié de la CNIL – Caractère consultatif de ces avis

Les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, qui intéressent la sûreté de l'État, la défense ou la sécurité publique et qui portent sur des données à

caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci, sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la CNIL. Cet avis ne saurait lier l'autorité administrative, mais celle-ci doit en toute hypothèse respecter les exigences de la loi du 6 janvier 1978 et les intérêts que le législateur a entendu protéger.

CE, 10ème/9ème SSR, 11 avril 2014, Union générale des syndicats pénitentiaires CGT, n° 355624, Inédit., point 7

7.3 Consultation obligatoire de la CNIL

Modification du projet d'acte après l'avis de la CNIL – Modification posant une « question nouvelle » – Obligation de nouvelle consultation de la CNIL

L'organisme dont une disposition législative ou réglementaire prévoit la consultation avant l'intervention d'un texte doit être mis à même d'exprimer son avis sur l'ensemble des questions soulevées par ce texte. Dans le cas où, après avoir recueilli son avis, l'autorité compétente pour prendre ce texte envisage d'apporter à son projet des modifications qui posent des questions nouvelles, elle doit le consulter à nouveau.

En l'espèce, le Gouvernement a saisi la CNIL d'un projet de décret autorisant le traitement de données relatives aux « activités politiques, philosophiques, religieuses ou syndicales ». Or le décret publié autorise le traitement de données qui révèleraient des opinions politiques, des convictions philosophiques ou religieuses, ou une appartenance syndicale, alors même qu'elles ne procèderaient pas d'activités politiques, philosophiques, religieuses ou syndicales. L'extension du champ des données sensibles collectées à laquelle procède le décret attaqué, en permettant la collecte de données relatives aux opinions et non, comme dans le projet de décret sur lequel la CNIL avait été consultée, de données relatives aux activités, soulevait une question nouvelle qui requérait une nouvelle consultation de la Commission, à laquelle il n'a donc pas été procédé. Annulation de la disposition en cause.

CE, 10ème-9ème chambres réunies, 24 décembre 2021, Ligue des droits de l'homme et autres, n° 447515, Inédit., point 12

Voir aussi : CE, 10ème–9ème chambres réunies, 24 décembre 2021, Ligue des droits de l'homme et autres, n° 447518, Inédit.

Détermination de la juridiction compétente pour connaître du contentieux de l'accès aux données contenues dans un traitement – Contentieux ne relevant pas de la formation spécialisée du Conseil d'État en matière de contentieux des fichiers intéressant la sûreté de l'État et la défense nationale – Incidence sur la protection des données à caractère personnel – Consultation obligatoire de la CNIL

Saisi d'un projet de décret modifiant l'article R. 841-2 du code de la sécurité intérieure et le décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiant l'article R. 841-2 du code de la sécurité intérieure qui fixe la liste des traitements ou parties de traitements de données à caractère personnel intéressant la sûreté de l'État, le Conseil d'État (section de l'intérieur) lui donne un avis favorable, à l'exception de ses dispositions attribuant le contentieux relatif au traitement de données de Tracfin, Startrac, à la formation spécialisée du Conseil d'État en matière de contentieux

des fichiers intéressant la sûreté de l'État et la défense nationale. En effet, le traitement de données Startrac, qui contient notamment les déclarations de soupçon adressées à Tracfin par les professionnels qui y sont tenus aux termes de l'article L. 561-2 du code monétaire et financier, n'intéresse pas uniquement la sûreté de l'État et la défense nationale. Startrac étant un fichier mixte, le Conseil d'État estime que l'article R. 841-2 du code de la sécurité intérieure, qui dispose que « Le Conseil d'État est compétent pour connaître, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, des requêtes concernant la mise en œuvre de l'article 118 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, pour les traitements ou parties de traitements intéressant la sûreté de l'État dont la liste est fixée par décret en Conseil d'État », fait obstacle à ce que le contentieux de l'accès aux données qu'il contient, dont certaines n'intéressent pas la sûreté de l'État, soit unifié en premier ressort au profit de la formation spécialisée du Conseil d'État.

CE, Section de l'intérieur, 4 mai 2021, Avis n°402612, Projet de décret modifiant l'article R. 841-2 du code de la sécurité intérieure et le décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiant l'article R. 841-2 du code de la sécurité intérieure

---

Différence entre le décret adopté et la version soumise pour avis à la CNIL – Régularité en l'absence de question nouvelle

Lorsque l'avis de la CNIL est réputé donné en vertu de l'article 6-1 du décret du 20 octobre 2005, la circonstance que le décret adopté diffère de la version soumise à la CNIL n'emporte pas son irrégularité si cette nouvelle version ne soulève aucune question nouvelle.

CE, 10ème-9ème chambres réunies, 24 octobre 2019, Fédération des transports et de la logistique FO-UNCP, n° 422583, Inédit., point 3

Obligation de consulter la CNIL sur un projet d'ordonnance fixant les caractéristiques essentielles d'un traitement – Au titre de l'article 8 de la loi Informatique et Libertés – Absence – Au titre de de l'article 36, paragraphe 4, du RGPD – Existence

Il résulte tant du paragraphe 4 de l'article 36 du règlement général sur la protection des données (RGPD) que de l'article 8 de la loi du 6 janvier 1978, que la CNIL doit être préalablement consultée sur tout projet de loi ou de décret qui détermine, dans leurs caractéristiques essentielles, les conditions de création ou de mise en œuvre d'un traitement de données à caractère personnel.

Si un projet d'ordonnance n'est pas un projet de loi ou de décret, seuls soumis à l'obligation de consultation de la CNIL en vertu de l'article 8 de la loi du 6 janvier 1978, le Conseil d'État (section des finances) estime, toutefois, que ce projet d'ordonnance doit être regardé comme entrant dans le champ d'application du paragraphe 4 de l'article 36 du RGPD selon lequel « les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ». Il estime donc qu'eu égard à la nature et à la portée du projet d'ordonnance relatif à l'expérimentation de la dématérialisation des actes de l'état civil établi par le ministère des affaires étrangères, la consultation de la CNIL, qui a rendu un avis le 13 juin 2019 sur ce projet, était requise au titre du paragraphe 4 de l'article 36 du RGPD.

CE, Section des finances, 18 juin 2019, Avis n° 397691, Projet d'ordonnance relatif à l'expérimentation de la dématérialisation des actes de l'état civil établi par le ministère des affaires étrangères

Formalités préalables à la mise en œuvre des traitements – Autorisation de la CNIL

Il résulte tant du paragraphe 4 de l'article 36 du RGPD que de la première phrase du a) du 4° de l'article 11 de la loi n°78-17 du 6 janvier 1978, dans sa rédaction résultant de la loi n° 2018-493 du 20 juin 2018, que la CNIL doit être préalablement consultée sur tout projet de loi ou de décret qui détermine, dans leurs caractéristiques essentielles, les conditions de création ou de mise en œuvre d'un traitement de données à caractère personnel.

A été réservée par le Conseil d'État (section des travaux publics) la question de savoir si cet article doit être interprété comme limitant la portée matérielle de la consultation obligatoire prévue par le paragraphe 4 de l'article 36 du RPGD aux seuls projets de décret déterminant les caractéristiques essentielles d'un traitement relevant de ceux, mentionnés aux paragraphes 3 et 4 de l'article 35 du même règlement, qui sont susceptibles d'engendrer, compte tenu de leur nature, de leur portée, de leur contexte et des finalités poursuivies, « un risque élevé pour les droits et libertés des personnes physiques » ou bien de l'étendre à l'ensemble des traitements dont la mise en œuvre repose sur un texte législatif ou réglementaire qui en définit les caractéristiques essentielles, sans qu'il y ait lieu de distinguer à ce stade entre ceux présentant un risque élevé et les autres

CE, Section des travaux publics, 9 octobre 2018, Avis n° 395259

Consultation obligatoire sur les projets de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données – 1) Notion – Projet portant sur le cadre général de la protection des droits et libertés des personnes ou déterminant les caractéristiques essentielles d'un traitement ou d'une catégorie de traitement – 2) Application – Décret prévoyant que les déclarations incombant aux professionnels sont transmises par voie électronique à l'autorité administrative compétente – Consultation obligatoire – Absence

1) Il résulte du a) du 4° de l'article 11 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction issue de la loi n° 2016-1321 du 7 octobre 2016, que la Commission nationale de l'informatique et des libertés (CNIL) doit être préalablement consultée sur tout projet de loi ou de décret comportant des dispositions, soit qui portent sur le cadre général de la protection des droits et libertés des personnes s'agissant de leurs données à caractère personnel ou du traitement de ces données, soit qui déterminent, dans certaines de leurs caractéristiques essentielles, les conditions de création ou de mise en œuvre d'un traitement ou d'une catégorie de traitements de données à caractère personnel.

2) Le décret n° 2016-1788 du 19 décembre 2016, relatif à la transmission de données de cession des médicaments utilisés en médecine vétérinaire comportant une ou plusieurs substances antibiotiques, prévoit que les déclarations auxquelles sont soumis les professionnels concernés sont transmises par voie électronique à l'autorité administrative compétente. Si ces dispositions, qui ne portent pas sur le cadre général de la protection des droits et libertés des personnes s'agissant de leurs données à caractère personnel ou du traitement de ces données, impliquent la mise en œuvre d'un traitement automatisé de données à caractère personnel, elles ne déterminent pas elles-mêmes les formalités de création ou les conditions de mise en œuvre de ce traitement. Par suite, le Premier ministre n'était pas tenu de consulter la CNIL.

CE, 1ère-4ème chambres réunies, 20 juin 2018, Syndicat national des vétérinaires d'exercice libéral et autres, n° 408185, 408192, T., points 2, 4

Voir aussi : CE, 2ème-7ème chambres réunies, 8 juillet 2020, Fédération française du transport de personnes sur réservation et autres, n°431063, T.

Projet d'ordonnance relatif à l'expérimentation de la dématérialisation des actes de l'état civil – Obligation de consultation de la CNIL– Au titre de l'article 8 de la loi Informatique et Libertés – Absence – Au titre de de l'article 36(4) RGPD – Existence

Il résulte tant du paragraphe 4 de l'article 36 du RGPD que de l'article 8 de la loi n°78-17 du 6 janvier 1978 dite loi Informatique et Libertés, que la CNIL doit être préalablement consultée sur tout projet de loi ou de décret qui détermine, dans leurs caractéristiques essentielles, les conditions de création ou de mise en œuvre d'un traitement de données à caractère personnel.

Si un projet d'ordonnance n'est pas un projet de loi ou de décret, seuls soumis à l'obligation de consultation de la CNIL en vertu de l'article 8 de la loi Informatique et Libertés, le Conseil d'État estime, toutefois, que ce projet d'ordonnance doit être regardé comme entrant dans le champ d'application du paragraphe 4 de l'article 36 du RGPD selon lequel «les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».

Il estime donc qu'eu égard à la nature et à la portée du projet d'ordonnance relatif à l'expérimentation de la dématérialisation des actes de l'état civil établi par le ministère des affaires étrangères, la consultation de la CNIL, qui a rendu un avis le 13 juin 2019 sur ce projet, était requise au titre du paragraphe 4 de l'article 36 du RGPD.

CE, Section des finances, 18 juin 2019, Avis n° 397691, Projet d'ordonnance relatif à l'expérimentation de la dématérialisation des actes de l'état civil du service central d'état civil et des autorités diplomatiques ou consulaires

Déclaration obligatoire de certaines maladies (article R.3113-2 du code de la santé publique) – Suppression de l'avis préalable de la CNIL pour un arrêté du ministre de la santé sur les données cliniques, biologiques et sociodémographiques

Selon l'article R. 3113-2 du code de la santé publique, les données cliniques, biologiques et sociodémographiques destinées à la surveillance épidémiologique que comporte la notification des maladies sont arrêtées par le ministre chargé de la santé après avis de la CNIL.

Si le projet de décret relatif aux déclarations obligatoires de certaines maladies supprime cet avis préalable, le Conseil d'État (section sociale) relève que la CNIL a émis un avis favorable à cette suppression. Surtout, il considère qu'il ne résulte d'aucune disposition de la loi n°78-17 du 6 janvier 1978, ni d'aucune autre disposition législative que cette consultation préalable soit obligatoire avant l'adoption d'un tel texte réglementaire. L'arrêté en question ne constitue pas une autorisation de mise en œuvre du traitement, laquelle relève au demeurant d'une décision de la Commission. Constatant que cette suppression n'aura pas pour effet de soustraire ces informations de tout contrôle de la CNIL, le Conseil d'État (section sociale) émet un avis favorable.

CE, Section sociale, 20 mars 2018, Avis n° 394296, Projet décret relatif aux déclarations obligatoires de certaines maladies

Fichier organisant les modalités selon lesquelles les agents chargés du contrôle de la recherche d'emploi ont accès à certaines données dont le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (art. R. 351-30 du code du travail) – Consultation obligatoire de la CNIL

Les dispositions de l'article R. 351-30 du code du travail issues du décret n° 2005-1624 du 22 décembre 2005 relatif au suivi de la recherche d'emploi, qui organisent les modalités selon

lesquelles les agents chargés du contrôle de la recherche d'emploi par les travailleurs involontairement privés d'emploi ont accès, pour l'exercice de leur mission, à certaines de ces données, parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, autorisent des traitements de données à caractère personnel et relèvent ainsi, eu égard à la nature des données en cause, des dispositions de l'article 27 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

En conséquence, le Gouvernement était tenu de recueillir l'avis motivé de la Commission nationale de l'informatique et des libertés, dès lors que les modifications apportées au traitement antérieurement autorisé par décret en Conseil d'État, qui portent tant sur le champ des personnes ayant accès à ces données que sur les finalités de ce traitement, étaient substantielles.

CE, Section, 2 juillet 2007, Association AC ! et autres, n° 290593, Rec., point 4

7.4 Contentieux relatifs aux actes réglementaires portant création de traitements

Les obligations du responsable du traitement en matière de sécurité ne peuvent être utilement invoquées contre l'acte par lequel le traitement est autorisé.

Les dispositions de l'article 121 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, selon lesquelles « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès », qui sont relatives aux obligations du responsable du traitement quant à l'utilisation de ce dernier, ne peuvent être utilement invoquées à l'appui de conclusions dirigées contre l'acte par lequel le traitement est autorisé.

CE, 10ème–9ème chambres réunies, 24 septembre 2021, Médecins du Monde et autres, n° 441317, Inédit., point 10

Article 31 de la loi Informatique et Libertés – Publication de l'avis de la CNIL postérieure à celle du décret – Illégalité – Absence

Les dispositions du II de l'article 31 de la loi n°78-17 du 6 janvier 1978, qui régissent les modalités de publication des avis de la CNIL sur les décrets autorisant la mise en œuvre de certains traitements de données à caractère personnel mis en œuvre pour le compte de l'État, sont sans incidence sur la légalité de ce décret. Par suite, un requérant ne peut utilement soutenir que la circonstance que l'avis de la CNIL ait été publié quelques jours après la publication du décret entacherait ce dernier d'irrégularité.

CE, 10ème–9ème chambres réunies, 27 mai 2021, M. A... B..., n° 441977, Inédit., point 3

Analyse d'impact devant être effectuée par le responsable d'un traitement de données (art. 35 du RGPD) – 1) Obligation relevant de la mise en œuvre du traitement – 2) Conséquence – Circonstance que cette analyse n'a pas été réalisée avant l'édiction de l'acte définissant le traitement – Circonstance sans incidence sur la légalité de cet acte

1) L'article 35 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) prévoit que le responsable du traitement effectue une analyse d'impact relative à la protection

des données lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Si cette analyse incombe au responsable du traitement, sa réalisation est en principe préalable à la mise en œuvre du traitement et l'analyse doit être actualisée après le lancement effectif du traitement afin de garantir en permanence une prise en compte adaptée des risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel.

2) Ainsi, alors que la réalisation d'une analyse d'impact d'un traitement de données personnelles, dont l'absence peut donner lieu à des sanctions par la CNIL en application de l'article 20 de la loi n° 78-17 du 6 janvier 1978, est liée à la mise en œuvre de ce traitement, la seule circonstance qu'elle n'aurait pas été réalisée avant la signature de l'instruction définissant les caractéristiques du traitement n'est pas de nature à entacher celle-ci d'illégalité.

CE, 2ème–7ème chambres réunies, 6 novembre 2019, Fédération des acteurs de la solidarité et autres, n° 434376, T., point 13

Obligation de sécurisation du traitement – Invocation à l'appui de conclusions dirigées contre l'acte précisant les modalités de mise en œuvre des traitements – Inopérance

Les dispositions de l'article 34 de la loi n°78-17 du 6 janvier 1978 relatives aux obligations de sécurité des responsables des traitements (dispositions reprises à l'article 32 du RGPD) ne peuvent être utilement invoquées à l'appui de conclusions dirigées contre l'acte précisant les modalités de mise en œuvre de ces traitements.

CE, 10ème–9ème chambres réunies, 6 avril 2018, Association nationale des supporters et autres, n° 406664, T., point 7

Obligation d'informer toute personne concernée dès l'enregistrement de données à caractère personnel dans le traitement – Invocation contre l'acte portant création du traitement en cas de méconnaissance – Exclusion

S'il incombe au responsable d'un traitement de données à caractère personnel de fournir à toute personne concernée par l'inscription de données personnelles dans ce traitement, dès leur enregistrement, l'ensemble des informations prévues au I de l'article 32 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction applicable au litige , y compris quand ces données personnelles ne sont pas recueillies auprès de la personne concernée elle-même, la méconnaissance de ces obligations par le responsable d'un traitement ne peut en tout état de cause être utilement invoquée à l'appui de conclusions dirigées contre l'acte portant création de ce traitement.

CE, 9ème/10ème SSR, 17 juin 2015, Syndicat national des industries des peintures enduits et vernis, n° 375853, Rec., point 23

Conclusions à fin d'injonction de destruction de données illégalement recueillies dans un traitement de données à caractère personnel – 1) Éléments pris en compte par le juge pour déterminer si l'exécution de sa décision implique nécessairement une telle destruction – Possibilité d'une régularisation appropriée – À défaut, mise en balance des motifs de l'illégalité constatée et des conséquences de la destruction des données pour l'intérêt général – 2) Application de ces principes en l'espèce – Injonction de détruire les données – Absence

1) Lorsque le juge administratif est saisi de conclusions à fin d'injonction de destruction de données illégalement recueillies dans un traitement de données à caractère personnel, il lui appartient, pour déterminer, en fonction de la situation de droit et de fait existant à la date à laquelle il statue, si l'exécution de sa décision implique nécessairement la destruction des données illégalement recueillies, de rechercher d'abord si, eu égard notamment aux motifs de la décision, une régularisation appropriée est possible. Dans la négative, il lui revient ensuite de prendre en considération, d'une part, les motifs de l'illégalité constatée, d'autre part, les conséquences de la destruction des données pour l'intérêt général, et d'apprécier, en rapprochant ces éléments, si la destruction des données n'entraîne pas une atteinte excessive à l'intérêt général.

2) En l'espèce, depuis l'introduction de la requête, un décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés et portant création d'un traitement de données à caractère personnel relatif à la gestion informatisée des détenus en établissement a été publié au Journal officiel et autorise la collecte et le traitement des données initialement contenues dans le fichier contesté. Compte tenu de l'intérêt éminent qui s'attache à la conservation des données litigieuses, notamment pour ce qui concerne la prévention des risques suicidaires en détention, il n'y a pas lieu d'enjoindre au ministre de la justice de supprimer les données recueillies dans le traitement contesté.

CE, 10ème–9ème chambres réunies, 4 juin 2012, SFOIP, n° 334777, T., point 8

Demande d'annulation d'une décision portant création d'un traitement de données à caractère personnel – Existence de ce traitement et de cette décision non établie devant le Conseil d'État – Conséquences – Renvoi de l'intéressé devant la CNIL pour lui demander de faire usage de ses pouvoirs de vérification de la licéité de traitements – Rejet en l'état des conclusions à fin d'annulation

Requérant demandant l'annulation d'une décision portant création d'un traitement de données à caractère personnel et produisant à l'appui de sa demande des éléments qui ne permettent, en l'état, ni de regarder comme établie l'existence d'un tel traitement ni, par suite, d'identifier une éventuelle décision de le créer. Il appartient au requérant, s'il estime cependant que ces éléments sont de nature à faire présumer de l'existence d'un traitement de données personnelles et s'il s'y croit fondé, de demander à la Commission nationale de l'informatique et des libertés (CNIL) de faire usage des pouvoirs qu'elle détient pour vérifier la licéité de traitements au regard des dispositions de la loi n° 78-17 du 6 janvier 1978. En l'état, rejet des conclusions à fin d'annulation présentées par le requérant.

CE, 10ème/9ème SSR, 16 avril 2012, Comité harkis et vérité, n° 335140, T., point 16

---

8. Règles applicables aux avis et décisions de la CNIL

8.1 Avis rendus par la CNIL

Pouvoir réglementaire du Premier ministre – Décret d'application d'une loi pris après avis conforme de la CNIL – Censure

Dispositions relatives à un fichier prévoyant que le décret d'application de la loi est pris après avis public conforme de la Commission nationale de l'informatique et des libertés. Or, en vertu de l'article 21 de la Constitution et sous réserve de son article 13, le Premier ministre exerce le pouvoir réglementaire à l'échelon national. Ces dispositions n'autorisent pas le législateur à subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire. Censure, dès lors, du « conforme ».

CC, 2020-800 DC, 11 mai 2020, Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, points 35-38

Voir aussi : CC, 2006-544 DC, 14 décembre 2006, Loi de financement de la sécurité sociale pour 2007

Forme des avis de la CNIL – Signature du seul président de la Commission – Légalité – Absence d'obligation d'autres signatures ou de mentions

La seule circonstance qu'un avis rendu par la CNIL ne comporte que la signature de son président ne suffit pas à établir qu'il n'aurait pas été rendu en formation plénière dès lors qu'aucune disposition ni aucun principe n'impose d'autres signatures ni ne prévoit de mentions obligatoires devant assortir l'avis. Lorsque l'avis a la forme d'une « délibération » et mentionne qu'il a été rendu par la Commission, il ne saurait été regardé, en l'absence d'élément contraire, comme émanant du seul président de la commission.

CE, 10ème–9ème chambres réunies, 30 décembre 2021, Société B... Avocat Victimes et Préjudices et autres, n° 440376, Inédit., point 7

Voir aussi : CE, 10ème-9ème chambres réunies, 13 avril 2021, Ligue des droits de l'homme, n° 439360, Inédit.

Traitement relevant de la directive « Police-Justice » susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques et mis en œuvre pour le compte de l'État – Analyse d'impact devant être réalisée et transmise à la CNIL avant l'édiction de l'acte définissant le traitement

Il résulte de l'article 90 de la loi n° 78-17 du 6 janvier 1978, applicable aux traitements de données à caractère personnel relevant de la directive (UE) 2016/80 du 27 avril 2016, mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, que, lorsqu'est exigée une analyse d'impact préalablement à la création ou à la modification d'un tel traitement mis en œuvre pour le compte de l'État, il appartient à l'administration, à peine d'irrégularité de l'acte instituant ou modifiant ce traitement, de la réaliser et de la transmettre à la Commission nationale de l'informatique et des libertés (CNIL) dans le cadre de la demande d'avis prévue à l'article 33 de la loi du 6 janvier 1978.

CE, 10ème–9ème chambres réunies, 24 décembre 2021, Ligue des droits de l'homme et autres, n° 447513, T., point 12

Voir aussi : CE, 10ème–9ème chambres réunies, 24 décembre 2021, Ligue des droits de l'homme et autres, n° 447515, Inédit.

Avis rendus sur le fondement du d) de l'article 11 de la loi Informatique et Libertés dans sa version applicable au litige – Obligation de publication préalable à l'adoption d'un texte ayant fait l'objet d'un tel avis – Absence

Aucune disposition de la loi n°78-17 du 6 janvier 1978 ni aucune autre disposition ni aucun principe n'impose la publication d'un avis rendu par la CNIL sur le fondement du d) de l'article 11 sur un projet d'arrêté préalablement à son adoption.

CE, 1ère-6ème chambres réunies, 17 novembre 2017, Fondation Jérôme Lejeune, n° 401212, Inédit., point 8

Consultation de la CNIL (articles 26 et 27 de la loi du 6 janvier 1978) – Avis implicite favorable (article 28 de la loi du 6 janvier 1978) – Obligation de motivation – Absence

En application des dispositions de l'article 28 de la loi n° 78-17 du 6 janvier 1978 dans sa rédaction applicable au litige, un avis implicite favorable naît du silence gardé par la Commission nationale de l'informatique et des libertés (CNIL) pendant les deux mois qui suivent la réception d'une saisine effectuée sur le fondement des articles 26 ou 27 de cette même loi. La loi a ainsi prévu que soient rendus des avis favorables implicites qui, par leur nature même, ne sauraient être motivés.

CE, 10ème/9ème SSR, 5 octobre 2014, Union nationale du personnel en retraite de la gendarmerie et autres, n° 358876, T., point 6

Modalités de consultation – Avis émis par le président sans que la CNIL ait délibéré en formation plénière – Irrégularité

Il résulte des dispositions de l'article 15 de la loi du 6 janvier 1978 que, si la commission peut déléguer à son président ou à son vice-président certaines de ses attributions, seule la commission réunie en formation plénière peut régulièrement émettre un avis sur les projets de texte qui lui sont soumis par le Gouvernement.

CE, Section, 2 juillet 2007, Association AC ! et autres, n° 290593, Rec., point 6

Avis de la CNIL sur les projets de lois ou d'actes réglementaires – Actes ne constituant pas des décisions susceptibles de recours

L'avis que formule la CNIL sur les projets qui lui sont soumis ne constitue pas une décision administrative faisant grief et n'est dès lors pas susceptible d'être déférée au juge de l'excès de pouvoir. Il en est de même du refus de formuler un avis défavorable.

CE, 10ème/7ème SSR, 23 juin 1993, Syndicat CGT du personnel de l'hôpital Dupuytren, n° 114983, Inédit., point 2

Avis rendus sur le fondement du 6° de l'article 44 de la loi Informatique et libertés (projet de recherche publique impliquant le traitement de données sensibles) – 1) Création et exploitation par une université d'un entrepôt de données à des fins de recherche publique – Avis unique de la CNIL – 2) Cas de l'utilisation de l'entrepôt de données par des chercheurs externes à cette même université – Traitements distincts non couverts par la demande et devant faire l'objet de nouveaux avis de la CNIL

1) En vertu du 6° de l'article 44 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi Informatique et libertés, la CNIL peut rendre un avis unique à la fois pour la création par une université d'un entrepôt de données et pour les recherches qui seront réalisées en son sein dans le cadre indiqué dans la demande émanant de cette université.

2) En revanche, les recherches mises en œuvre par des chercheurs externes à l'université et qui ne sont rattachés à aucun laboratoire de celle-ci, à des fins de recherche publique, à partir des données contenues dans l'entrepôt, constituent des traitements distincts, non couverts par la demande et devant faire l'objet de nouveaux avis au titre de cette même disposition.

CNIL, SP, 16 mars 2023, Avis sur projet de mise en œuvre d'un traitement de données à caractère personnel, n°2023-025, non publié

Pérennisation d'un traitement de données à caractère expérimental – Éléments accompagnant une saisine pour avis – Rapport d'évaluation

Pour pouvoir se prononcer sur la pérennisation d'un traitement de données à caractère personnel expérimental, il est nécessaire pour la Commission de disposer avec la saisine d'une évaluation des bénéfices tirés du dispositif expérimental, pour les comparer à l'atteinte à la vie privée qu'implique une généralisation du dispositif. Ce rapport doit permettre d'apprécier si le traitement mis en œuvre à titre expérimental a permis de répondre aux finalités poursuivies.

CNIL, P, 3 mars 2022, Avis sur projet de loi, LOPMI, n° 2022-028, publié, points 9-10

8.2 Traitements soumis à un régime de déclaration ou d'autorisation préalable par la CNIL

Traitement soumis à autorisation – Délibérations de la CNIL – Obligation de motivation

Les délibérations par lesquelles la Commission nationale de l'informatique et des libertés (CNIL), sur le fondement des dispositions du III de l'article 8 de la loi n°78-17 du 6 janvier 1978, qui définissent les possibilités de dérogation à l'interdiction de principe posée au I du même article, autorise, compte tenu de leurs finalités, certaines catégories de traitement de données sensibles, sont au nombre des actes devant obligatoirement être motivés en vertu de l'article 2 de la loi n° 79-587 du 11 juillet 1979.

CE, 10ème/9ème SSR, 26 mai 2014, Société IMS Health, n° 354903, T., point 5

Recherche et développement en matière de capacités techniques de recueil et d'exploitation des renseignements – Dispositions expresses prévoyant un mécanisme

d'autorisation de mise en œuvre de tels traitements – Conséquence – Application du régime d'autorisation préalable de la loi Informatique et Libertés – Absence

Des dispositions législatives spéciales peuvent déroger au régime de formalités préalables prévu par la loi du 6 janvier 1978 modifiée. Les dispositions des titres I et IV de la loi du 6 janvier 1978 modifiée ont vocation à s'appliquer aux traitements intéressant la sûreté de l'État, tel que le traitement des données collectées par le biais de techniques de recueil de renseignement à des fins de recherche et de développement en matière de capacités techniques de recueil et d'exploitation des renseignements, sous réserve des dispositions spéciales du code de la sécurité intérieure y dérogeant. À cet égard, dès lors que des dispositions expresses prévoient un mécanisme spécifique d'autorisation de mise en œuvre de tels traitements, les programmes de recherche ne nécessitent pas l'autorisation par arrêté ministériel ou décret en Conseil d'État pris après avis de la Commission prévue par l'article 31 de la loi précitée.

CNIL, SP, 8 avril 2021, Avis sur projet de loi, PJL Renseignement, n° 2021-040, publié, points 38-40

8.3 AIPD

Contrôle local des données – Absence d'échange de données avec un serveur central – Risques limités d'accès illégitime, de modification non désirée ou de disparition des données concernées – Saisine obligatoire de la CNIL pour avis sur une AIPD – Absence

Le juge des référés refuse de suspendre l'application du Passe sanitaire. Le choix d'offrir un système décentralisé limitant la constitution de traitements ou bases nationales de données de santé, au prix de la conservation, par la personne concernée, sur son propre téléphone mobile, de certaines de ses propres données de santé, remplit un motif d'intérêt public dans le domaine de la santé publique et n'est pas manifestement contraire au principe de minimisation des données.

En outre, le choix de ne pas saisir la CNIL de l'analyse d'impact préalable à la mise en œuvre du traitement n'entache la mise en œuvre du passe sanitaire d'aucune illégalité manifeste. En effet, le traitement TousAntiCovid Vérif repose sur un contrôle local des données contenues par les justificatifs. Il n'y a pas d'échange de données avec le serveur central de la société prestataire lors de la vérification des justificatifs. Il apparaît donc qu'il y a peu de risques d'accès illégitime, de modification non désirée ou de disparition des données concernées. Enfin, le passe est de nature à permettre, par la limitation des flux et croisements de personne qu'il implique, de réduire la circulation du virus de la Covid-19 dans le pays. Son usage est restreint à des situations précises et reste facultatif. Les personnes sont également libres de produire leur justificatif par voie papier ou sur tout autre support numérique.

CE, Juge des référés, 6 juillet 2021, n°453505, Inédit., points 9, 12-13

8.4 Code de conduite

8.5 Certification

8.6 Règles d'entreprises contraignantes

8.7 Actes de droit souple

Prise de position de la CNIL dans une « foire aux questions » mise en ligne sur son site internet – Acte susceptible de recours – Existence, eu égard à sa teneur

Par la question - réponse n° 12 mise en ligne le 18 mars 2021 sur le site internet de la Commission nationale de l'informatique et des libertés (CNIL), cette autorité a fait part aux responsables de traitement et personnes concernées de son interprétation de l'article 82 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés quant à la portée et au champ d'application des exemptions à l'obligation de consentement préalable au dépôt des traceurs de connexion, en ce qui concerne les opérations dites d'affiliation. Eu égard à sa teneur, cette prise de position, émise par l'autorité de régulation sur son site internet, est susceptible de produire des effets notables sur la situation des personnes qui se livrent à des opérations d'affiliation et des utilisateurs et abonnés de services électroniques. Il suit de là que cette question-réponse n° 12 et le refus de la CNIL de la retirer sont susceptibles de faire l'objet d'un recours pour excès de pouvoir.

CE, 10ème–9ème chambres réunies, 8 avril 2022, Syndicat national du marketing à la performance (SNMP), n° 452668, Rec., point 8

Voir aussi : CE, Assemblée, 21 mars 2016, Société X, n° 368082, Rec. ; CE, Section, 12 juin 2020, Groupe d'information et de soutien des immigré.e.s (GISTI), n° 418142, Rec.

Compétence – 1) Champ – Tout traitement de données, à caractère personnel ou non, relevant du champ d'application de la loi du 6 janvier 1978 – 2) Modalités d'exercice – a) Possibilité de recourir à un instrument de droit souple – b) Illustrations – c) Limite – Liberté du consentement – Possibilité pour la CNIL d'interdire le blocage d'accès à un site en cas de refus des cookies (« cookie walls ») par un acte de droit souple – Absence

1) Il résulte de l'économie générale de la loi n° 78-17 du 6 janvier 1978 et, en particulier, de ses articles 8, 16, 20 et 82 que la Commission nationale de l'informatique et des libertés (CNIL) est chargée de veiller à la conformité de tout traitement de données relevant de son champ d'application, qu'il concerne ou non des données à caractère personnel, à ses dispositions ainsi qu'aux obligations résultant du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD).

2) a) La CNIL dispose, pour l'accomplissement de ses missions, du pouvoir de mettre en œuvre ses prérogatives selon les modalités qu'elle juge les plus appropriées, y compris en recourant à des instruments de droit souple.

b) Par suite, la CNIL était compétente pour adopter des « lignes directrices » applicables, de manière générale, aux cookies et autres traceurs de connexion.

Ces lignes directrices ont légalement pu préconiser des durées limites d'usage de cookies de mesure d'audience de nature afin de permettre le réexamen périodique de leur nécessité au regard des dérogations à la règle du consentement prévues à l'article 82 de la loi du 6 janvier 1978 ou favoriser

la diffusion de bonnes pratiques mais ne sauraient imposer de nouvelles obligations non prévues par la loi ou fixer une durée limite de validité aux cookies de mesure d'audience.

c) La CNIL affirme, à l'article 2 de la délibération attaquée, que la validité du consentement est soumise à la condition que la personne concernée ne subisse pas d'inconvénient majeur en cas d'absence ou de retrait de son consentement, un tel inconvénient majeur pouvant consister, selon elle, dans l'impossibilité d'accéder à un site Internet, en raison de la pratique des « cookies walls », qui consiste à bloquer l'accès à un site web ou à une application mobile pour qui ne consent pas à être suivi.

En déduisant pareille interdiction générale et absolue de la seule exigence d'un consentement libre, posé par le RGPD, la CNIL a excédé ce qu'elle peut légalement faire, dans le cadre d'un instrument de droit souple, édicté sur le fondement du 2° du I de l'article 8 de la loi du 6 janvier 1978.

CE, 10ème–9ème chambres réunies, 19 juin 2020, Association des agences-conseil en communication et autres, n° 434684, T., points 5, 10, 16-17

Prise de position publique de la CNIL sur le maniement de ses pouvoirs, notamment de sanction, pour veiller au respect des règles relatives à la protection des données à caractère personnel – Acte susceptible de faire l'objet d'un recours pour excès de pouvoir

Les avis, recommandations, mises en garde et prises de position adoptés par les autorités de régulation dans l'exercice des missions dont elles sont investies, peuvent être déférés au juge de l'excès de pouvoir lorsqu'ils revêtent le caractère de dispositions générales et impératives ou lorsqu'ils énoncent des prescriptions individuelles dont ces autorités pourraient ultérieurement censurer la méconnaissance. Ces actes peuvent également faire l'objet d'un tel recours, introduit par un requérant justifiant d'un intérêt direct et certain à leur annulation, lorsqu'ils sont de nature à produire des effets notables, notamment de nature économique, ou ont pour objet d'influer de manière significative sur les comportements des personnes auxquelles ils s'adressent.

L'acte révélé par deux communiqués de presse qui présentent le plan d'actions élaboré par la CNIL dans le domaine du ciblage publicitaire en ligne constitue une prise de position publique de la commission quant au maniement des pouvoirs dont elle dispose, en particulier en matière répressive, pour veiller au respect des règles applicables au recueil du consentement au dépôt de cookies et autres traceurs. Elle doit être regardée comme ayant pour objet d'influer sur le comportement des opérateurs auxquels elle s'adresse et comme étant de nature à produire des effets notables tant sur ces opérateurs que sur les utilisateurs et abonnés de services électroniques. Elle est donc susceptible de faire l'objet d'un recours contentieux.

CE, 10ème–9ème chambres réunies, 16 octobre 2019, La Quadrature du Net et Caliopen, n° 433069, Rec., points 3-4

8.8 Plaintes

Missions de l'autorité de contrôle – Notions de (1) "demande" et de (2) "demandes excessives" – (3) Exigence de paiement de frais raisonnables ou refus de donner suite aux demandes en cas de demandes manifestement infondées ou excessives – Conditions

L'article 57, paragraphe 4, du règlement général sur la protection des données doit être interprété en ce sens que :

1) la notion de « demande » qui y figure recouvre les réclamations visées à l'article 57, paragraphe 1, sous f), et à l'article 77, paragraphe 1, de ce règlement.

2) des demandes ne peuvent être qualifiées d'« excessives », au sens de l'article 57, paragraphe 4, de ce règlement, uniquement en raison de leur nombre pendant une période déterminée, l'exercice de la faculté prévue à cette disposition étant subordonné à la démonstration, par l'autorité de contrôle, de l'existence d'une intention abusive de la part de la personne ayant introduit ces demandes.

3) lorsqu'elle est confrontée à des demandes excessives, une autorité de contrôle peut choisir, par une décision motivée, entre exiger le paiement de frais raisonnables basés sur les coûts administratifs ou refuser de donner suite à ces demandes, en tenant compte de l'ensemble des circonstances pertinentes et en s'assurant du caractère approprié, nécessaire et proportionné de l'option choisie.

CJUE, 9 janvier 2025, Österreichische Datenschutzbehörde, C-416/23

Réclamation fondée sur un grief à l'article 14 du RGPD – Vérifications du respect de l'article 32 - Absence

Les obligations consacrées à l'article 32 du RGPD, qui doivent être respectées en toute hypothèse et indépendamment de l'existence ou non d'une obligation d'information en vertu de l'article 14 de ce règlement, sont de nature et de portée différentes par rapport à l'obligation d'information prévue à cet article 14. Ainsi, en cas de réclamation au titre de l'article 77, paragraphe 1, du RGPD, au motif que le responsable du traitement a invoqué, à tort, l'exception prévue à l'article 14, paragraphe 5, sous c), de ce règlement, l'objet des vérifications à effectuer par l'autorité de contrôle est circonscrit par le champ d'application du seul article 14 dudit règlement, le respect de l'article 32 de celui-ci ne faisant pas partie de ces vérifications.

CJUE, 28 novembre 2024, Másdi, C-169/23, points 72, 73

Pouvoir d'appréciation de la CNIL de la suite à donner aux plaintes qui lui sont adressées

La Commission nationale de l'informatique et des libertés, autorité administrative indépendante chargée de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978, dispose du pouvoir d'apprécier la suite à donner aux plaintes qui lui sont adressées, quelle que soit la décision prise ensuite par les autorités judiciaires, saisies en application des articles 21, 4°, de ladite loi et 40 du code de procédure pénale.

Cass, crim., 3 février 1998, n° 96-82.665, B., point 6

Respect d'une procédure contradictoire préalable à la décision de la CNIL clore une plainte - Absence d'obligation

Ni les dispositions de l'article L. 121-1 du code des relations entre le public et l'administration, qui prévoit la mise en œuvre d'une procédure contradictoire préalable à certaines décisions « exception faite des cas où il est statué sur une demande », ni aucun autre texte ou principe n'impose, à l'égard de l'auteur d'une plainte adressée à la CNIL, le respect d'une procédure contradictoire préalablement à la décision de cette commission de la clore.

CE, 10ème-9ème chambres réunies, 9 février 2024, MM. D..., n°472215, Rec., points 7-8

---

1) Réclamation auprès d'une autorité de contrôle introduite par une personne concernée – Informations à fournir par l'autorité de contrôle, notamment la possibilité d'exercer un recours juridictionnel – 2) Réclamation auprès de la CNIL – Décision implicite de rejet en cas de silence gardé – Réponse avant l'échéance du délai de trois mois – Exclusion

1) En application de l'article 77 du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD), toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle si elle considère que le traitement de données à caractère personnel la concernant constitue une violation de ce règlement. Cette autorité de contrôle informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'exercer un recours juridictionnel en vertu de l'article 78 lorsque l'autorité de contrôle compétente ne traite pas sa réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de sa réclamation.

2) En application du d du 2° du I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) traite les réclamations et plaintes introduites par une personne concernée, examine ou enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête est nécessaire. L'article 10 du décret n° 2019-536 du 29 mai 2019 précise que le silence gardé pendant trois mois par la commission sur une réclamation vaut décision de rejet. Une personne concernée à laquelle la Commission a adressé une réponse, avant l'échéance de ce délai de trois mois, l'informant de la saisine du délégué à la protection des données de la société faisant l'objet de la réclamation et de ce qu'elle serait tenue informée de la suite réservée à cette réclamation, et dont la plainte a finalement été clôturée par une décision répondant à l'ensemble de ses demandes, n'est pas fondée à soutenir qu'une décision implicite de rejet serait née du silence gardé par la CNIL sur ses demandes.

CE, 10ème-9ème chambres réunies,24 juillet 2023, M. A... D..., n°465229, T., points 2-4

Contestation par l'auteur d'une plainte ou réclamation des suites données à celle-ci par la CNIL – 1) Intérêt à déférer au juge de l'excès de pouvoir le refus d'engager une procédure sur le fondement de l'article 20 de la loi du 6 janvier 1978 – Existence – 2) Cas où la formation restreinte a été saisie (III de l'art. 20) – a) Intérêt à contester la décision prise à l'issue de la procédure – Absence – b) Cas où le plaignant invoque la méconnaissance, par un responsable de traitement, de droits légalement garantis à l'égard de données personnelles le concernant – Intérêt à demander l'annulation du refus du président de la CNIL de mettre en demeure le responsable de satisfaire à sa demande ou du refus de la formation restreinte de lui enjoindre d'y procéder – Existence

1) L'auteur d'une plainte peut déférer au juge de l'excès de pouvoir le refus du président de la CNIL d'engager une procédure sur le fondement de l'article 20 de la loi n° 78-17 du 6 janvier 1978 et, notamment, de saisir la formation restreinte sur le fondement du III de cet article, y compris lorsque la commission a procédé à des mesures d'instruction, constaté l'existence d'un manquement aux dispositions de cette loi et pris l'une des mesures prévues au I et II de ce même article.

2) a) En revanche, lorsque le président de la CNIL a saisi la formation restreinte sur le fondement du III de cet article, l'auteur de la plainte n'a pas intérêt à contester la décision prise à l'issue de cette procédure, quel qu'en soit le dispositif.

b) Toutefois, lorsque l'auteur de la plainte se fonde sur la méconnaissance par un responsable de traitement des droits garantis par la loi à la personne concernée à l'égard des données à caractère personnel la concernant, notamment les droits d'accès, de rectification, d'effacement, de limitation et d'opposition mentionnés aux articles 49, 50, 51, 53 et 56 de la loi du 6 janvier 1978, celui-ci, s'il ne peut contester devant le juge l'absence ou l'insuffisance de sanction une fois que la formation restreinte a été saisie, est toujours recevable à demander l'annulation du refus du président de la CNIL de mettre en demeure le responsable de traitement de satisfaire à la demande dont il a été saisi par cette personne ou du refus de la formation restreinte de lui enjoindre d'y procéder.

CE, 10ème–9ème chambres réunies, 27 mars 2023, Mme D... E..., n°467774, T., points 4-5

Obligation de motivation – 1) Rejet d'une plainte relative à la méconnaissance d'un droit individuel reconnu par le RGPD – Existence – 2) Rejet d'une plainte relative à la méconnaissance d'une autre disposition du RGPD – Absence

1) Le refus de la Commission nationale de l'informatique et des libertés (CNIL) de donner suite à une plainte fondée sur la méconnaissance d'un des droits individuels reconnus par le RGPD est au nombre des décisions administratives individuelles défavorables qui refusent un avantage dont l'attribution constitue un droit pour les personnes qui remplissent les conditions légales pour l'obtenir, au sens et pour l'application du 6° de l'article L. 211-2 du code des relations entre le public et l'administration (CRPA), et qui doivent, à ce titre, être motivées.

2) En revanche, la décision de ne pas donner suite à une plainte fondée sur de potentiels manquements aux règles relatives au délégué à la protection des données au titre des articles 38 et 39 du RGPD n'est pas au nombre des décisions individuelles défavorables énumérées à l'article L. 211-2 du CRPA et n'a pas, dès lors, à être motivée.

CE, 10ème–9ème chambres réunies, 21 octobre 2022, Mme A...C..., n° 459254, Rec., points 6-7

Plainte fondée sur la méconnaissance de l'article 40 Loi Informatique et Libertés – Pouvoir d'appréciation de la CNIL sous contrôle du juge

Lorsque l'auteur d'une plainte se fonde sur la méconnaissance des droits qu'il tient du I de l'article 40 de la loi du 6 janvier 1978, notamment du droit de rectification de ses données personnelles, le pouvoir d'appréciation de la CNIL pour décider des suites à y donner s'exerce, eu égard à la nature des droits individuels en cause, sous l'entier contrôle du juge de l'excès de pouvoir.

CE, 10ème–9ème chambres réunies, 3 octobre 2018, M. A... B..., n° 405939, T., point 3

---

1) Contestation par l'auteur d'une plainte des suites données à celle-ci par la CNIL – Intérêt à déférer au juge de l'excès de pouvoir le refus de la CNIL d'engager une procédure de sanction sur le fondement du I de l'article 45 de la loi du 6 janvier 1978, y compris en cas de mesures d'instruction ou de constat d'un manquement – Existence – 2) Intérêt à contester la décision prise à l'issue de la procédure de sanction prévue à cet article et le sort réservé à sa plainte – Absence – Intérêt à contester devant le juge de l'excès de pouvoir le refus de la CNIL de lui fournir des informations des suites données à sa plainte – Existence

1) L'auteur d'une plainte peut déférer au juge de l'excès de pouvoir le refus de la CNIL d'engager à l'encontre de la personne visée par la plainte une procédure de sanction, y compris lorsque la CNIL procède à des mesures d'instruction ou constate l'existence d'un manquement aux dispositions de la

loi du 6 janvier 1978. Il appartient au juge de censurer ce refus en cas d'erreur de fait ou de droit, d'erreur manifeste d'appréciation ou de détournement de pouvoir.

2) En revanche, lorsque la CNIL a décidé d'engager une telle procédure, l'auteur de la plainte n'a intérêt à contester ni la décision prise à l'issue de cette procédure, quel qu'en soit le dispositif, ni le sort réservé à sa plainte à l'issue de cette dernière. Il est toutefois recevable à déférer, dans tous les cas, au juge de l'excès de pouvoir le défaut d'information par la CNIL des suites données à sa plainte.

CE, 10ème–9ème chambres réunies, 21 juin 2018, M. B... A..., n° 416505, T., point 2

Voir aussi : CE, 10ème–9ème chambres réunies, 3 octobre 2018, M. A... B..., n° 405939, T., point 2

Contestation par l'auteur d'une plainte des suites données à celle-ci par la CNIL – 1) Intérêt à déférer au juge de l'excès de pouvoir le refus de la CNIL de donner suite à cette plainte – Existence – Intérêt à contester la décision prise à l'issue de l'instruction de la plainte – Absence – 2) Application au cas dans lequel une sanction a été prononcée après instruction de la plainte – Intérêt de l'auteur de la plainte à contester la sanction prononcée, en tant qu'elle n'est pas assez sévère –Absence – Intérêt à contester devant le juge de l'excès de pouvoir le refus de la CNIL de lui fournir des informations relatives à la clôture de sa plainte – Existence

1) L'auteur d'une plainte peut déférer au juge de l'excès de pouvoir le refus de la Commission nationale de l'informatique et des libertés (CNIL) d'y donner suite. Il appartient au juge de censurer ce refus en cas d'erreur de fait ou de droit, d'erreur manifeste d'appréciation ou de détournement de pouvoir. En revanche, lorsque la CNIL a décidé d'instruire une plainte, l'auteur de celle-ci n'a intérêt à contester ni la décision prise à l'issue de cette instruction, quel qu'en soit le dispositif, ni la clôture de sa plainte prononcée subséquemment.

2) Il s'ensuit que l'auteur d'une plainte n'est pas recevable à demander l'annulation de la sanction prononcée par la CNIL à l'encontre d'un tiers à l'issue de l'instruction de la plainte qu'il a formée, en tant que celle-ci ne serait pas assez sévère. En revanche, l'auteur d'une plainte est recevable à déférer au juge de l'excès de pouvoir le refus de la CNIL de lui fournir les informations relatives aux suites données à sa plainte auxquelles il a droit en application des dispositions de l'article 11 2° c) de la loi n°78-17 du 6 janvier 1978. Il résulte de ces dispositions que, lorsque la plainte conduit à sanctionner la personne mise en cause, la complète information de son auteur comprend nécessairement, y compris lorsque la sanction a été rendue publique, la communication de la nature des manquements retenus et de la teneur de la sanction prononcée, sous la réserve des secrets protégés par la loi.

CE, 10ème–9ème chambres réunies, 19 juin 2017, M. A, n°398442 , T., points 3-5

Possibilité de rejeter une plainte comme abusive – Existence, même sans texte – Condition – Examen préalable de la plainte

La Commission nationale informatique et libertés (CNIL) dispose, dans le cadre de la mission qui lui est confiée par le c du 2° de l'article 11 de la loi n°78-17 du 6 janvier 1978, de la faculté, ouverte même sans texte, de rejeter, sous le contrôle du juge, les plaintes dont elle est saisie qui présentent un caractère abusif. Si les dispositions de l'article 19 de la loi n° 2000-321 du 12 avril 2000 (loi DCRA) dispensent les autorités administratives d'accuser réception des demandes abusives dont elles sont saisies, la CNIL ne peut cependant rejeter ainsi des plaintes sans examen préalable de chacune d'elles.

CE, 10ème/9ème SSR, 10 avril 2015, M. A, n° 376575, T., point 5
