Tables Informatique & Libertés

Les cahiers 2024

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

Avant-propos

La CNIL a pour mission d'éclairer l'application du Règlement Général sur la Protection des Données (RGPD) et de la Loi Informatique et Libertés, au service des individus et des responsables de traitement. Elle adopte des lignes directrices, des recommandations et des référentiels, et traite les plaintes et réclamations dont elle est saisie. Les recommandations et beaucoup des décisions de la CNIL sont publiées au Journal officiel et sur son site internet. Mais un grand nombre de ses décisions individuelles ne sont pas publiées. En outre, la bonne compréhension de la doctrine de la CNIL nécessite de la replacer dans le cadre de la jurisprudence qu'elle applique et de l'ensemble des principes de protection des données à caractère personnel.

Les Cahiers Informatique et Libertés visent ainsi à compiler, sous forme de résumés et en suivant un plan de classement thématique, l'essentiel de la jurisprudence et des décisions marquantes de la CNIL en matière de protection des données sur l'année écoulée. Ce recueil permet ainsi, en les rassemblant en un seul support, de prendre rapidement connaissance des évolutions doctrinales de l'année en matière de protection des données personnelles.

Le Cahier annuel constitue donc une extraction des Tables Informatique et Libertés. Ces Tables ont été créées afin de structurer la doctrine de la CNIL, qui se construit progressivement à partir des centaines de décisions individuelles et des milliers de réponses qui sont apportées aux usagers chaque année. Elles contribuent ainsi à garantir l'égalité de traitement entre les usagers et à assurer une meilleure sécurité juridique. Elles permettent également de faire connaître les prises de position de la CNIL en rendant publics les points de droit sur lesquels la CNIL a dû se positionner dans des décisions non publiques.

En publiant les Cahiers Informatique et Libertés, la CNIL renforce l'accessibilité de sa doctrine, répondant ainsi aux besoins des professionnels du droit des données personnelles et des associations de défense des droits individuels. Si ces Cahiers, comme les Tables, sont d'abord à destination des professionnels de la protection des données à caractère personnel, ils peuvent également servir à toute personne curieuse d'approfondir la matière.

2024 a été une année particulièrement riche pour la protection des données. Par exemple, plusieurs arrêts de la Cour de justice de l'Union européenne (CJUE) sont venus clarifier les modalités d'indemnisation des personnes concernées en cas de violation de leur droit à la protection des données (CJUE, 25 janvier 2024, *MediaMarktSaturn*, C-687/21 ; CJUE, 4 octobre 2024, *Patērētāju tiesību aizsardzības centrs*, C-507/23), la Cour de Cassation s'est prononcée à plusieurs reprises en matière de droit social, notamment sur les données opposables lors d'un licenciement (Cass, soc., 6 mars 2024, n° 22-11.016, Bull.) et le Conseil d'Etat a précisé les modalités de recours contre la clôture d'une plainte par la CNIL (CE, 10ème-9ème chambres réunies, 9 février 2024, MM. D..., n°472215) Ce n'est là qu'un simple échantillon d'une année marquée par des avancées significatives dans la protection des données personnelles et la clarification des droits des individus.

Bien que ce document aspire à couvrir toutes les décisions novatrices fixant la doctrine, certaines décisions importantes de l'année écoulée, émanant de la CNIL ou des juridictions nationales ou européennes, peuvent manquer. Des erreurs ou coquilles peuvent également subsister. Si vous décelez une erreur ou un manque, merci de le signaler à l'adresse tablesIL@cnil.fr pour correction dans la prochaine mise à jour des Tables Informatique et Libertés.

Louis Dutheillet de Lamothe

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

1.1.1 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

1.2 Droit applicable

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

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

Protection des données des personnes morales

Exception domestique

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

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

1.3.2 Données sensibles

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

1.3.3 Notion de traitement

Communication orale de données à caractère personnel – Traitement de données 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

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.

1) 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, Affaire C-205/21

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

2.3 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

2.3.1 Obligation légale

Conditions d'application de cette base 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 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

2.4.1 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

2.5 Sécurité

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, 6 août 2024, Mise en demeure, Société X, n°MED-2024-112, 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, décision 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, no SAN-2023-023, publié

2.6 Conditions de licéité du traitement de catégories particulières de données

2.6.1 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

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, décision n° MED 2024-056, non publié

2.6.2 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

2.6.3 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

2.7 Conditions de licéité des traitements algorithmiques

Droit de la personne concernée de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé – Décision individuelle automatisée – Notion – 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

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

2.8 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

2.9 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

---

3 Droits des personnes

3.1 Information

3.1.1 Dans le champ du RGPD

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, no SAN-2023-023, 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, Affaire C-169/23

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

3.2 Accès

3.2.1 Généralités

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 chambre, 31 décembre 2024, n°488201, Inédit, point 5.

3.2.2 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

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, Chambre sociale, 8 mars 2023, n° 21-12.492, points 5-10

3.3 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, M.-A. A., C-4/23

3.4 Effacement

3.4.1 Portée

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

3.4.2 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.

CJUE, 14 mars 2024, Újpesti Polgármesteri Hivatal, C-46/23

3.5 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

3.6 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, Affaire 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.

CJUE, 25 janvier 2024, MediaMarktSaturn, C-687/21

Fonction compensatoire du droit à réparation – Existence – Fonction dissuasive de ce même droit– Exclusion - 2) Condition – Existence d'une faute du responsable de 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

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

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

---

4 Règles spéciales et applications sectorielles

4.1 Police-Justice

4.1.1 Règles principales et obligations particulières

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

4.1.1 Autres fichiers et traitements

Traitement des antécédents judiciaires (TAJ)

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

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, 30/04/2024, n°472864, Inédit., point 4, 5.

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 œuvre 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

4.2 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

4.3 Traitements économiques et fiscaux

4.3.1 Champ Fichier des incidents de remboursement des crédits aux particuliers FICP

1) Consultation obligatoire du FICP Base légale – 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

4.4 Directive ePrivacy et chapitre III loi Informatique et Libertés, sauf prospection

4.4.1 Annuaire (article 12, ePrivacy)

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

4.4.2 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

4.4.3 Limitations, conservation et accès aux données de connexion

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), 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 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 2024, Procura della Repubblica presso il Tribunale di Bolzano, Affaire C-178/22

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., Affaire C-349/21

4.5 Travail

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, Chambre sociale, 8 mars 2023, n° 21-12.492, points 5-10

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, décision 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

4.6 Traitements mis en œuvre à des fins journalistiques

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

4.7 Traitements de données à caractère personnel accessibles publiquement

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

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

4.8 Traitements de vote électronique

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

4.9 Traitements vidéo

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

4.9.1 Vidéoprotection

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, 30/04/2024, n°472864, Inédit., point 4, 5.

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

4.9.2 Vidéosurveillance

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

5. Actes administratifs encadrant des traitements particuliers

5.1 Actes réglementaires créant des traitements publics

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

6. Règles applicables aux avis et décisions de la CNIL

6.1 Certification

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

6.2 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, Österreische Datenschutzbehörde, Affaire C-416/23

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, Affaire C-169/23, points 72, 73

6.3 Vérifications opérées dans le cadre de l'exercice indirect des droits

Exercice des droits de la personne concernée par l'intermédiaire de l'autorité de contrôle – Décision de clôture de la vérification - Droit au recours contre cette décision – Existence

L'article 17 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 l'article 46, paragraphe 1, sous g), l'article 47, paragraphes 1 et 2, et l'article 53, paragraphe 1, de cette directive ainsi qu'avec l'article 8, paragraphe 3, et l'article 47 de la charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens que lorsque les droits d'une personne ont été exercés, en application dudit article 17, par l'intermédiaire de l'autorité de contrôle compétente et que cette autorité informe ladite personne du résultat des vérifications opérées, cette dernière doit disposer d'un recours juridictionnel effectif contre la décision de ladite autorité de clôturer le processus de vérification.

CJUE, 16 novembre 2023, Ligue des droits humains, C-333/22

Commission nationale
de l'informatique et des libertés
3, Place de Fontenoy
TSA 80715
75 334 PARIS CEDEX 07
Tél. 01 53 73 22 22

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles