Droit des libertés fondamentales

Leçon 8 : Partie 2 : Les libertés dans le temps : Le temps des secrets

Xavier BIOY

Table des matières

Le droit au respect de la vie privée est énoncé à l'article 12 de la DUDH de 1948 et à l'article 17 du PIDCP de 1966. L'article 8 paragraphe 1 de la Convention EDH consacre également ce principe en précisant: « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* », alors que l'article 8 paragraphe 2 expose les conditions d'une limitation de ce droit en soulignant : « *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». La CDFUE consacre également le droit de toute personne « *au respect de sa vie privée et familiale, de son domicile et de ses communications* » (art. 7).

Section 1 : La vie privée

D'abord conçue comme synonyme d'intimité, la vie privée s'est étendue aux choix de vie et leur expression en public et dans la vie professionnelle. Le secret est devenue une affirmation publique de soi.

§1. Notion

« *La notion de vie privée est* ***une notion large non susceptible d'une définition exhaustive*** », écrit la CEDH dans l'**affaire Pretty** (CEDH, 29 avr. 2002, req. n° 2346/02, § 61). La vie privée est un concept juridique qui rassemble de multiples manifestations de la protection de l'intimité de l'individu et de l'expression de ses choix de vie dans un cadre public ou professionnel. En droit français, la décision n° 99-416 DC du 23 juillet 1999 portant sur la couverture maladie universelle confirme l'ancrage de la vie privée à l'article 2 de la Déclaration de 1789, c'est-à-dire son affiliation à la liberté personnelle, alors que pour la CEDH cette autonomie personnelle est inhérente au respect de la vie privée et familiale de l'article 8. Dès lors, la protection de la vie privée apparaît moins comme un problème de moyen que comme une question de détermination de frontière. Dans un contexte libéral de séparation des sphères publique et privée, face à la montée des identités et des communautarismes qui se conjugue pour d'autres avec la montée de l'individualisme vers le goût du secret, **la vie privée apparaît comme une notion tout à fait contradictoire : « droit à la différence et à l'indifférence »**. Traditionnellement, la France a une conception étroite fondée sur le secret (champ couvert par la loi du 17 juillet 1970 qui a créé l'article 9 du Code civil) et traitant à part, comme éléments intéressant l'État et l'ordre public, les questions d'identité, de sexe, de famille, de libre disposition de soi. **L'intimité fait l'objet d'une protection pénale** par les articles 226-1 et suivants du Code pénal. Il sanctionne ainsi la simple interception à l'insu des personnes d'informations relatives à leur vie privée (écoutes téléphoniques illicites, enregistrements effectués à l'insu des personnes, photographies volées dans des lieux privés, montages réalisés avec la parole ou l'image d'une personne sans son consentement, violation des correspondances, accès frauduleux à un système de traitement de données...).

La CEDH a une conception extensive de la notion de vie privée qui la conduit à inclure le lieu de travail dans la mesure où il est conçu comme le lieu de liens avec le monde extérieur et rejoint ainsi le droit de nouer des relations avec autrui (CEDH, 23 nov. 1992, Niemietz c. Allemagne, n° 13710/88). Le droit européen conduit donc à placer sur le terrain de la vie privée de nombreux aspects qui ne relèvent qu'indirectement de la protection du secret de l'intimité comme **la protection de la santé (CEDH, 6 févr. 2001, Bensaid c. Royaume-Uni, req. n° 44599/98), le droit de vivre dans un environnement sain (CEDH, 9 déc. 1994, Lopez Ostra c. Espagne, req. n° 16798/90), le droit à un mode de vie traditionnel (CEDH, 18 janv. 2001, Chapman c. RU, req. n° 27238/95), le droit de se voir restituer le corps d'un membre de sa famille (CEDH, 30 oct. 2001, Pannullo et Forte c. France, req. n° 37794/97) ou encore le droit au nom (CEDH, 22 févr. 1994, Burghartz c. Suisse, req. n° 16213/90) et un droit au prénom (CEDH, 24 oct. 1996, Guillot c. France, req. n° 15774/89)**. Le droit à la vie privée implique aussi l'accès à l'eau potable (sans discrimination) (CEDH, 10 mars 2020, Hudorovi# et autres c. Slovénie, req. n^{os} 24816/14 et 25140/14).

> ***Exemple***
>
> Exemplaire à ce titre est l'arrêt **Sidabras et Dziautas c. Lituanie** (CEDH, 27 juill. 2004, req. n^{os} 55480/00 et 59330/00) : les requérants se plaignaient de l'interdiction qui leur a été faite de travailler dans le secteur privé de 1999 à 2009 au motif qu'ils ont été agents du KGB. La CEDH accepte de pénétrer de plain-pied sur le terrain des droits sociaux pour consacrer, le droit de gagner sa vie par un travail librement choisi : l'État compromet les possibilités de développer des relations avec le monde extérieur, ce qui cause de graves difficultés pour gagner sa vie et a des répercussions évidentes sur le respect de la vie privée. Dans cette affaire, comme dans d'autres, la Cour combine en outre l'article 8 avec d'autres afin de renforcer certains interdits. Ainsi, l'arrêt *M.C. c. Bulgarie*, du 4 décembre 2003, se fonde à la fois sur l'article 3 et l'article 8 pour reconnaître comme insuffisante **la protection offerte par le droit interne contre le viol**. L'action combinée de la vie privée et du principe de non-discrimination (art. 14) emporte des conséquences potentiellement illimitées en conduisant à la reconnaissance d'un vrai droit à la différence exigeant l'acceptation par la collectivité de tous les choix individuels que la personne estime constitutifs de sa personnalité. Depuis son arrêt *X et Y c. Pays-Bas* du 26 mars 1985, **la Cour impose aux États des obligations positives qui peuvent « *impliquer l'adoption de mesures visant au respect de la vie privée*, *jusque dans les relations des individus entre eux* ».** Ainsi, le droit à la vie privée peut imposer à un État d'aider un étranger à établir son statut, voire à lui conférer sa nationalité (CEDH, 26 avril 2018, Hoti c. Croatie, req. n° 63311/14) : s'agissant d'un enfant né en Croatie de parents en situation irrégulière et qui vit en Croatie depuis plus de cinquante ans sans pouvoir prouver son apatridie et donc régulariser sa situation. Il n'a pu, ni ne peut construire aucune vie, ni travailler, etc.). Il exige aussi que des responsabilités soient établies en cas de préjudice lié à une opération chirurgicale (CEDH, 6 juin 2017, Erdinç Kurt et autres c. Turquie, n° 50772/11). L'obligation d'informer les autorités de lutte contre le dopage des différents lieux de résidence des athlètes pour pouvoir effectuer des contrôles constitue une ingérence proportionnée (CEDH, 18 janvier 2018, Fédération Nationale des associations et des syndicats Sportifs (FNASS) et autres c. France, n^{os} 48151/11 et 77769/13).

En 1976 (Com. EDH, 13 mai 1976, X. c. Islande), la Commission des droits de l'homme lie le droit au respect de la vie privée avec « ***le droit d'établir et d'entretenir des relations avec d'autres êtres humains, notamment dans le domaine affectif pour le développement et l'accomplissement de sa propre personnalité*** ». Cette position **fait écho à celle de la Cour de cassation qui protège au titre de la vie privée l'ensemble des relations sentimentales** (Cass. 2ème civ., 26 nov. 1975, Soc. Éditions parisiennes associées c. G.). Mieux encore, « *la garantie offerte par l'article 8 de la Convention est principalement destinée à assurer le développement, sans ingérences extérieures, de la personnalité de chaque individu dans les relations avec ses semblables* » (CEDH, 24 févr. 1998, Botta c. Italie, req. n° 21439/93). Ce besoin de socialisation peut également sauver un étranger menacé d'éloignement vers un pays dont il a la nationalité sans y avoir aucune attache, ayant vécu sans interruption depuis la naissance dans le pays qui l'expulse où il a toutes « *ses relations personnelles, sociales et économiques* » et analyse les mesures d'éloignement comme une ingérence dans la « vie privée sociale » des intéressés (CEDH, 9 oct. 2003, Slivenko c. Slovénie, req. n° 48321/99). **Le Conseil d'État semble faire droit à cette conception.** Il a annulé ainsi certaines dispositions du décret du 30 septembre 2010 portant code de déontologie du service pénitentiaire en ce qu'il interdit, de manière trop générale et absolue, aux agents d'avoir des relations avec les anciens détenus (CE, 11 juillet 2012, déc. n° 347148, Section française de l'Observatoire international des prisons).

§2. Composantes

A - Le domicile

Le « lieu privé » est celui dans lequel nul ne peut pénétrer sans l'autorisation de celui qui l'occupe. La notion est plurielle, connaissant différentes définitions selon le domaine fiscal, commercial, etc. Du point de vue de la vie privée, **il faut l'entendre comme le lieu de résidence** (CC, 29 déc. 1983, déc. n° 83-164 DC). Étonnamment, preuve que le régime vient avant le concept et le besoin de protéger avant la cohérence, la notion européenne de domicile inclut le lieu où s'exerce une activité professionnelle.

Déterminer le lieu de sa résidence relève du droit à la vie privée et peut même concrétiser un mode de vie identitaire (CEDH, 18 janv. 2001, Chapman c. Royaume-Uni, req. n° 27238/95). Cela n'en comporte pas moins des limites tenant au droit de propriété, aux règles d'urbanisme, au respect de la dignité et de la décence du logement et bien sûr de la liberté contractuelle. Dans le cas d'une gouvernante licenciée, dont le contrat de travail stipulait l'obligation d'habiter à moins de 200 mètres de son lieu de travail mais qui avait déménagé au-delà, la Cour de cassation (Cass. soc., 28 févr. 2012, pourvoi n° 10-18.308, Mme C. c/ Association Maison départementale de la famille) a considéré, au visa des articles 8 de la Convention EDH, 9 du Code civil et L. 1121-1 du Code du travail, que toute personne dispose de la liberté de choisir son domicile et que nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir et proportionnées au but recherché.

L'article 66 de la Constitution réserve en principe à l'autorité judiciaire la protection de l'inviolabilité du domicile (CC, 29 déc. 1983, déc. n° 83-164 DC), même lorsque la visite domiciliaire est ordonnée par la préfecture. Si le lien entre sûreté et domicile n'est pas évident, le Conseil constitutionnel persiste à réserver à l'autorité judiciaire le contrôle des perquisitions, visites domiciliaires et saisies de nuit (CC, 2 mars 2004, déc. n° 2004-492 DC). L'intervention de l'autorité judiciaire doit être prévue; elle doit vérifier de façon concrète le bien-fondé de la demande de perquisition. La nuit protège davantage la tranquillité du domicile.Selon l'article 59 du Code de procédure pénale, « *Sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures* ».Le trafic de stupéfiants ou le terrorisme permettent ces visites de nuit, sous contrôle du juge des libertés et de la détention, sur requête du procureur de la République, lorsqu'il existe un risque immédiat de disparition des preuves ou indices matériels. Une perquisition s'effectue selon des règles strictes : en présence de l'habitant ou d'un représentant de son choix ou de deux témoins requis par l'officier de police judiciaire (le bâtonnier pour le domicile ou le cabinet d'un avocat), avec autorisation par une commission rogatoire du juge d'instruction (sauf en cas de crime ou de délit flagrant puni d'emprisonnement). Une pièce saisie lors d'une perquisition illégale ne peut être utilisée à l'appui de poursuites pénales.

L'État s'autorise maintes fois à pénétrer au domicile des particuliers (perquisitions judiciaires, fiscales, douanières, de renseignement). Selon le Conseil constitutionnel, le législateur peut prévoir la possibilité d'opérer des perquisitions, visites domiciliaires et saisies de nuit **dans le cas où un crime ou un délit relevant de la criminalité et de la délinquance organisées vient de se commettre**, à condition que l'autorisation de procéder à ces opérations émane de l'autorité judiciaire, gardienne de la liberté individuelle, et que le déroulement des mesures autorisées soit assorti de garanties procédurales appropriées (CC, 2 mars 2004, déc. n° 2004-492 DC).

Le Conseil constitutionnel dans sa décision du 30 juillet 2010 (déc. n° 2010-19/27 QPC, Époux P. et autres) a admis la constitutionnalité du cadre légal des visites et saisies effectuées par les agents de l'administration fiscale. Pour lui, elles ne sont pas contraires au droit à un recours juridictionnel effectif car elles n'affectent aucune situation légalement acquise. Cette décision peut d'ailleurs se réclamer de l'arrêt Ravon c. France du 21 février 2008 par lequel la CEDH avait jugé les dispositions antérieures contraires à l'article 6 § 1 dans la mesure où les contrôles juridictionnels n'étaient pas suffisants.

La loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme permet aussi de nouveaux types de perquisitions et saisies administratives sous le contrôle du juge des libertés et de la détention du tribunal de grande instance de Paris.Le nouvel article L. 229-1 permet ainsi au préfet d'« *autoriser la visite d'un lieu ainsi que la saisie des documents, objets ou données qui s'y trouvent, aux seules fins de prévenir la commission d'actes de terrorisme et lorsqu'il existe des raisons sérieuses de penser qu'un lieu est fréquenté par une personne dont le comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes* ».Il s'agit donc de permettre à l'État de remonter à la source et de trouver des portes d'entrées dans les réseaux, sans attendre la révélation d'une infraction pénale et dans l'espoir d'en découvrir une.

B - La correspondance

Pour tribunal correctionnel de Paris, « *l'envoi de messages électroniques de personne à personne constitue de la correspondance privée* » (Trib. corr. Paris, 2 nov. 2000). Selon une circulaire du 17 février 1988, « *Il y a correspondance privée lorsque le message est exclusivement destiné à une (ou plusieurs) personne, physique ou morale, déterminée et individualisée* ». La loi du 10 juillet 1991 précise dans son article 1er « *le secret des correspondances émises par la voie des télécommunications est garanti par la loi* ». La loi pour la confiance dans l'économie numérique du 21 juin 2004 y assimile les messages électroniques. Le secret des correspondances est reconnu par le Conseil constitutionnel comme un élément autonome, composante de la liberté personnelle (CC, 2 mars 2004, déc. n° 2004-492 DC). Il en est de même pour la CEDH alors même qu'il peut aussi s'agir, dans l'absolu, d'une violation de la liberté d'expression.

Le Code pénal punit d'une peine d'un an d'emprisonnement et de 45 000 euros d'amende « *le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance* » (art. 226-15, CP) ; peines aggravées lorsque l'auteur de l'indiscrétion est dépositaire de l'autorité publique ou chargé d'une mission de service public (trois ans d'emprisonnement, art. 432-9, CP). Toutefois, une enquête judiciaire menée par un juge d'instruction peut passer outre ce secret (art. 81 et 97, CPP).

C - La voix

La voix constitue l'un des attributs de la personnalité et peut bénéficier de la protection instituée par l'article 9 dans la mesure où une voix caractéristique peut être rattachée à une personne identifiable (CA Pau, 1ère ch., 22 janv. 2001). Pour la CEDH, toute écoute téléphonique ou enregistrement d'une conversation, à l'insu des protagonistes, est constitutive d'une violation de l'article 8 de la Convention à moins qu'elle ne soit prévue par la loi, nécessaire dans une société démocratique à la poursuite d'un but légitime et proportionnée à cet objectif (CEDH, 6 sept. 1978, Klass c. Allemagne, req. n° 5029/71). Les articles 226-1 à 226-9 du Code pénal répriment le fait de fixer, d'enregistrer ou de transmettre sans consentement les paroles d'une personne prononcées à titre privé ou confidentiel et l'image d'une personne se trouvant dans un lieu privé. Est puni encore le fait de conserver ces informations, de les porter ou laisser porter à la connaissance du public ou d'un tiers ou de les utiliser, a fortiori par la voie de la presse.

Concernant les écoutes téléphoniques, il existe donc depuis la loi n° 91-646 du 10 juillet 1991 d'un côté les « interceptions de sécurité » qui reposent sur les nécessités de la sécurité publique et d'un autre les « écoutes judiciaires » dans le cadre d'une enquête judiciaire. La loi du 10 juillet 1991, modifiée par celle du 9 mars 2004, permet au juge d'instruction (et parfois aux officiers de police judiciaire sous contrôle des magistrats) d'écouter dans le cadre de l'enquête préliminaire ou de l'enquête de flagrance sur autorisation du juge des libertés et de la détention, délivrée à la requête du procureur de la République pour une durée de quinze jours renouvelables.

Diligentées par le Premier ministre, à la demande écrite et motivée des ministres concernés (ministres de la Défense, de l'Intérieur et ministre chargé des douanes), elles ont « *pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées* » (art. 3 de la loi du 10 juillet 1991). Le mécanisme de la loi du 10 juillet 1991, permettant d'écouter les conversations à l'insu des personnes a été dépassé et étendu par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.Cette loi a en partie été censurée par le Conseil constitutionnel eu égard à l'atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances. Des dispositions permettaient en effet, en cas d'urgence « opérationnelle », de déroger à l'autorisation préalable de l'autorité publique et à l'avis du Premier ministre et de la commission de contrôle. La loi n'avait pas non plus rempli sa compétence concernant la « surveillance internationale »,

notamment quant à la durée de conservation des renseignements ainsi obtenus. D'où le vote d'une seconde loi, le 30 novembre 2015, relative aux mesures de surveillance des communications électroniques internationales.

Désormais, **la loi soumet la mise en œuvre des techniques de renseignement** (par la Direction générale de la sécurité extérieure (DGSE), la direction de la protection et de la sécurité de la défense (DPSD), la direction du renseignement militaire (DRM), la Direction générale de la sécurité intérieure (DGSI), la Direction nationale du renseignement et des enquêtes douanières et Tracfin (service de renseignement rattaché aux ministères financiers)) à une **autorisation du Premier ministre**, après avis d'une nouvelle autorité administrative indépendante : la Commission nationale de contrôle des techniques de renseignement (CNCTR). La CNCTR succède à la Commission nationale de contrôle des interceptions de sécurité. Elle est composée de deux députés, deux sénateurs, deux membres du Conseil d'État, deux magistrats de la Cour de cassation et un représentant de l'Autorité de régulation des communications électroniques et des postes (ARCEP). Elle peut demander communication de toutes les informations utiles pendant et après la mise en œuvre de la technique. La loi instaure en outre un droit de recours spécial devant le Conseil d'État.

La loi définit un cadre dans lequel les services de renseignement sont autorisés à recourir à des techniques d'accès à l'information, en respectant les principes de proportionnalité et de subsidiarité. Les finalités sont larges, mais liées au terrorisme : la sécurité nationale, les intérêts essentiels de la politique étrangère et l'exécution des engagements internationaux de la France, les intérêts économiques et scientifiques essentiels de la France, la prévention du terrorisme, la prévention de la criminalité et de la délinquance organisées, la prévention de la prolifération des armes de destruction massive, la prévention des violences collectives de nature à porter gravement atteinte à la paix publique.

Des techniques de recueil de renseignements aujourd'hui permises dans un cadre judiciaire seront étendues aux services de renseignement : par exemple, le balisage de véhicule, les micros et caméras dans des lieux privés, l'accès aux réseaux des opérateurs de télécommunications (en cas de menace terroriste) ou le contrôle des communications des détenus. Pour la captation de données informatiques dans le cadre de la lutte antiterroriste, un dispositif d'analyse automatique des données par les fournisseurs d'accès à internet surveillera le trafic. Les hébergeurs ne communiqueront que les données de connexion (métadonnées) et non les contenus.

La loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme vise « *toute personne à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes* ».
A leur égard, peuvent être autorisées les interceptions de correspondances échangées au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs (sont visées les moyens de communication à courte portée utilisant des techniques de cryptage entre utilisateurs identifiés, les communications par *private mobile radio* (PMR), aujourd'hui principalement les *talkies walkies* numériques, et les transmissions entre objets connectés). La loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement a renforcé le contrôle préalable de la CNCTR pour l'ensemble des techniques de renseignement sur le territoire national et donné un caractère contraignant est donné à ses avis.

D - L'image

Le problème de l'image est moins celui de sa captation que celui de sa diffusion : Cass. 2ème civ., 30 juin 2004, pourvoi n° 02-19.599 : « *Toute personne a sur son image un droit exclusif et absolu et peut s'opposer à sa fixation, à sa reproduction ou à son utilisation sans autorisation préalable* ». Le seul fait de permettre l'identification d'une personne à travers son image est donc constitutif d'une atteinte à la vie privée (CEDH, 21 févr. 2002, Schüssel c. Autriche). L'image protégée par la vie privée est donc celle qui a été captée dans

un lieu privé, sans consentement pour cela ou pour sa diffusion. Les risques sont aujourd'hui démultipliés par les sites internet sociaux. L'image captée dans un lieu dont l'accès est contrôlé doit être autorisée (ou tout au moins tolérée par celui qui se sait photographié).

Il résulte des articles 9 du Code civil et 8 de la Convention européenne des droits de l'homme que **le droit à l'image d'une personne interdit, en l'absence de son autorisation, sa captation au même titre que sa conservation, sa reproduction ou son utilisation commerciale, et que la seule constatation d'une atteinte à ce droit lui donne droit à réparation** (Cass. 1ère civ., 2 juin 2021, pourvoi n° 20-13.753).

> ***Remarque***
> Après que la Cour de cassation a décidé, selon une interprétation stricte de la loi pénale, que la diffusion d'une photo intime, prise avec le consentement de la personne (en l'occurrence une femme nue alors qu'elle était enceinte, photographiée par son ex-compagnon) n'est pas pénalement réprimé, le législateur est intervenu : la loi pour une République numérique du 7 octobre 2016 a introduit un nouvel article 226-2-1 dans le Code pénal qui, d'une part, aggrave la répression des contenus à caractère sexuel (paroles ou images présentant un caractère sexuel prises dans un lieu public ou privé) ; d'autre part, « *punit des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1* ».

Plus largement, **un lieu où on se sent dans l'intimité, à l'abri des regards, peut être jugé privé**. À l'inverse, l'image captée dans un lieu public (accessible à tous sans autorisation) est présumée acceptée par le modèle même si la diffusion ne peut avoir lieu sans l'accord des personnes aisément identifiables et qui font l'objet de révélations relevant de la sphère privée. L'absence de refus explicite n'équivaut pas un consentement lorsque la personne est identifiable.

> ***Exemple***
> CA Paris, 20 févr. 2001, cas de l'attentat dans le RER.

Le droit au respect de la vie privée peut s'opposer aussi, bien sûr, à **la vidéosurveillance par les forces de l'ordre**. Les caméras fixes ne peuvent pas filmer les entrées d'immeubles, encore moins les intérieurs. Le Conseil constitutionnel a même censuré une atteinte à la vie privée pour les caméras embarquées à bord de drones ou véhicules qui peuvent suivre des personnes dans leurs déplacements ou filmer les propriétés privées. Ces systèmes, pour être compatibles avec la Constitution, doivent fixer des conditions de nécessité et d'information du public sans que la police ne puisse invoquer des circonstances formulées très vaguement, pour s'en dispenser. De même, la décision de recourir à des caméras embarquées relève des seuls agents des forces de sécurité intérieure et des services de secours (CC, 20 mai 2021, n° 2021-817 DC - Loi pour une sécurité globale préservant les libertés).

Section 2 : Les données personnelles

Dans un arrêt du 17 décembre 2009, Gardel c. France (req. n° 16428/05), la CEDH écrit que « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacrée par l'article 8 de la Convention* ». De même, l'article 8 de la Charte des droits de l'Union européenne proclame que « *1. Toute personne a droit à la protection des données à caractère personnel la concernant.*

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Le grand danger des *big data* est le « profilage », c'est-à-dire « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* » (règlement européen n° 2016/679 du 27 avril 2016 dit RGPD, art. 4).

Selon le règlement européen de 2016, les « données à caractère personnel », sont « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Parmi les données personnelles certaines sont plus « sensibles ».Selon l'article 9 du RGPD, « *le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.* »
Mais les exceptions sont nombreuses.

§1. Les sources

Autrefois accessoire de la vie privée, la question de la protection des données personnelles dans le domaine de l'informatique s'autonomise. Après avoir rattaché cette question à la vie privée par l'arrêt *Rotaru c. Roumanie* (CEDH, 17 décembre 2009, Rotaru c. Roumanie, req. n° 16428/05), la CEDH précise que « ***la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacrée par l'article 8 de la Convention*** ».

De même, **l'article 8 de la Charte des droits de l'Union européenne** proclame que :
« *1. Toute personne a droit à la protection des données à caractère personnel la concernant.*

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

***3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.* »**

L'article 16 du Traité sur le fonctionnement de l'Union européenne énonce le droit de toute personne « *à la protection des données à caractère personnel la concernant* » et habilite l'Union à fixer des règles relatives à la protection des personnes physiques à l'égard des données à caractère personnel par les institutions, organes et organismes de l'Union et les États membres dans le champ d'application du droit de l'Union.

A - Pour la Constitution, la liberté personnelle (article 2 de la DDHC) implique le droit au respect de la vie privée et des données personnelles. Par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif. Par la création du registre national des crédits aux particuliers, le législateur a poursuivi un motif d'intérêt général de prévention des situations de surendettement. Dans sa décision relative à ce fichier, le Conseil estime que la grande quantité de données personnelles, leur durée de conservation et l'obligation de consultation qu'ont les banques avant l'octroi d'un crédit à la consommation, conduisent à juger que cela porte atteinte au droit au respect de la vie privée de manière disproportionnée au but poursuivi. Plus récemment, il a censuré également les dispositions, incluses dans la loi relative à la confiance dans la vie publique, donnant à la Haute autorité pour la transparence de la vie publique un droit de communication de certains documents ou renseignements, notamment la communication de métadonnées de connexion jusqu'ici reconnu à l'administration fiscale. **Il s'assure que la loi limite la conservation aux données adéquates et nécessaires.**

B - La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés connaît, depuis quelques années, un destin formidable. Suscitée à l'époque par le projet Safari qui créait un fichier rassemblant des informations relatives aux individus et des interconnexions avec d'autres fichiers accessibles par un identifiant unique, cette loi sert désormais de base à l'ensemble de droits relatifs à la protection des personnes face aux usages de l'informatique, c'est-à-dire pour l'essentiel les fichiers. Cette loi a fait l'objet d'une révision importante par la loi du 29 juillet 2004, laquelle a fait l'objet d'un contrôle de constitutionnalité qui en a validé le dispositif à l'exception d'une nouvelle modalité permettant la lutte contre le piratage des œuvres de l'esprit en autorisant la constitution de fichiers de connexion, permettant aux sociétés de défense de droits d'auteur de traiter les données personnelles relatives aux infractions et aux condamnations en matière de contrefaçon (après autorisation de la CNIL et du juge judiciaire).

C - La loi de 1978 a, par la suite, transposé le droit communautaire dont le principal objectif demeure la libre circulation des données dans l'espace européen. Il est concrétisé par la directive 95/46/CE du 24 octobre 1995 relative aux données personnelles, la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, et enfin par la directive 2006/24/CE du 15 mars 2006 relative à la conservation des données générées aux traités dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication. La loi de 1978 s'applique à l'ensemble des fichiers non seulement automatisés mais également manuels, qu'ils soient du secteur public ou du secteur privé. La loi du 6 août 2004 a supprimé la distinction entre les fichiers des personnes publiques et ceux des personnes privées. Elle n'en continue pas moins à faciliter l'établissement des fichiers des autorités publiques mis en œuvre pour le compte de l'État dans le domaine de la sécurité, lesquels se voient autorisés par arrêté ministériel. La vraie distinction désormais est celle qui sépare le régime de droit commun de la simple déclaration et le régime d'autorisation relatif aux traitements de données présentant des risques particuliers pour la vie privée. Elle ne s'applique pas en revanche pour l'exercice d'activités exclusivement personnelles ou domestiques (tenue de carnets d'adresses...), c'est-à-dire non professionnelles, non politiques ou non associatives (Délibération de la CNIL n° 2005-284 du 22 nov. 2005).

D - Le règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (pleinement applicable à partir du 25 mai 2018) 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, insuffle une nouvelle approche du problème. Il renonce à une administration publique à la mode française et met en avant l'autorégulation des détenteurs de fichiers sous réserve d'un système de contrôle et de sanctions a posteriori. Le rôle des autorités de contrôle qui composent actuellement le G29 sera

donc redéfini et leur indépendance devra être mieux garantie. Ces autorités pourront proposer des codes de conduite (ce que la CNIL fait peu actuellement) et des référentiels adaptés à chaque secteur d'activité.
Le règlement est complété par la Directive 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. Elle s'applique aux fichiers de police et de justice.
Le règlement met ainsi en place une architecture institutionnelle enfin harmonisée dans toute l'Union. Si les États demeurent en première ligne pour l'application du règlement, la Commission européenne devra adopter un certain nombre d'actes d'exécution concernant la certification des mécanismes de protection des données et les échanges de données entre autorités de contrôle. De même, si le règlement fait confiance à l'instrument contractuel pour réguler la matière, il impose des règles de contenu et les contrats de sous-traitance des données devront comporter des clauses-type. Les autorités de contrôle, après l'abandon des formalités préalables à la mise en œuvre du traitement, auront ainsi à valider les documents d'autorégulation.

Le RGPD s'applique à tout transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, même si ces données sont susceptibles d'être traitées à des fins de sécurité publique, de défense et de sûreté de l'État. On se référera à un certain nombre de critères, au nombre desquels l'adhésion à la convention de 1981 du Conseil de l'Europe, et l'adoption de BCR (*Binding Corporate Rules*), c'est-à-dire des règles contraignantes pour toutes les entreprises d'un groupe et qui profitent aux tiers, de nature réglementaire, déterminées par les acteurs du secteur et reconnues par un acte d'exécution révisable. On généralisera aussi les codes de conduite, les mécanismes de certification et les clauses-types de protection des données approuvés par la Commission. Tout cela remplace les demandes d'autorisation nationales, trop lentes et trop onéreuses.

Cependant, dans l'arrêt du 16 juillet 2020, Facebook Ireland et Schrems, la Cour de justice a condamné le système. Pour elle, la directive 95/46/CE fixe les règles applicables au transfert de données à caractère personnel des États membres vers des pays tiers, dans la mesure où ces transferts relèvent de son champ d'application. L'évaluation de l'équivalence des protections doit prendre en compte tant les stipulations contractuelles entre l'exportateur et le destinataire, les éléments pertinents du système juridique du pays tiers, notamment un éventuel accès des autorités publiques aux données transférées que l'existence d'une voie de recours devant un organe offrant des garanties équivalentes de nature à assurer l'indépendance de l'organisme indépendant de règlement des litiges (médiateur) étranger.
Côté sanctions aussi, le règlement décide de devenir contraignant à l'égard des géants américains et asiatiques du secteur (jusqu'à 4 % du chiffre d'affaires mondial ou 20 millions d'euros – première harmonisation européenne). De nouvelles définitions et de nouveaux droits sont posés que l'on verra plus loin. Il est également créé un Comité européen à la protection des données (qui institutionnalise le G29) et un contrôleur européen à la protection des données personnelles en charge de la publication de recommandations et de règlement des litiges.

E - Le **règlement (UE) 2023/2854 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (dit « *Data Act* »)** a été publié au Journal officiel de l'Union européenne (22 décembre 2023, entré en vigueur le 11 janvier 2024) s'applique aux utilisateurs d'appareils connectés. Il contient diverses mesures qui offrent un niveau adéquat de protection **des secrets d'affaires et des droits de propriété intellectuelle**, préviennent l'utilisation de clause abusive dans les contrats de partage de données, et permettent aux organismes du secteur public et aux organes de l'Union d'accéder aux données détenues par le secteur privé et de les utiliser lorsque cela est nécessaire dans des circonstances exceptionnelles, notamment en cas d'urgence publique, ou lors de l'accomplissement d'une mission d'intérêt public. Il **facilite le changement de service de traitement de données, l'introduction de garanties contre l'accès illicite de tiers à des données à caractère non personnel et le développement de normes d'interopérabilité** pour les données auxquelles il doit être accédé, qui doivent être transférées et qui doivent être utilisées.
Deux règlements ont été adoptés en 2024 et ont des effets sur l'usage des données. Le **règlement 2022/1925 sur les marchés numériques** dit **DMA** (pour *Digital Markets Act*), qui entend prévenir les abus de position dominante des géants du numérique et offrir un plus grand choix aux consommateurs européens ; le **règlement**

2022/2065 sur les services numériques dit **DSA** (pour *Digital Services Act*), qui prévoit de lutter contre les contenus et produits illégaux en ligne (haine, désinformation, contrefaçons...). L'objectif est de faire d'internet un espace plus sûr pour les utilisateurs. Ils seront étudiés avec la liberté d'expression.

§2. Les droits de la personne fichée

La personne concernée par le fichage informatique dispose d'un certain nombre de droits qui concrétisent la protection de sa vie privée. Il s'agit tout d'abord du droit d'être informé de la mise en place du traitement automatisé des données. L'information délivrée concerne l'identité du responsable du traitement, la finalité de ce traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des données, les droits dont la personne dispose, les éventuels transferts à l'étranger. Cette obligation d'information ne s'applique pas à la conservation des données à des fins historiques, statistiques ou scientifiques. Systématisant la philosophie du droit des données, le règlement européen du 27 avril 2016 fixe le respect de la vie privée comme principe cardinal « dès la conception » et « par défaut ». Les entreprises auront donc l'obligation de prendre en compte le risque pour la vie privée tout au long du processus d'élaboration d'un nouveau produit ou service et d'adopter des mécanismes permettant de s'assurer que, par défaut, seul un minimum de données personnelles soit collecté, utilisé et conservé. Le règlement prévoit un renforcement de l'information des particuliers par les responsables de traitement qui devront notamment bénéficier d'informations complémentaires sur le traitement de leurs données mais également les obtenir sous une forme claire, accessible et compréhensible.

Le responsable du traitement ne peut s'affranchir de ce consentement qu'en cas d'obligation légale, en cas de sauvegarde de la vie de la personne concernée, pour l'exécution d'une mission de service public ou d'un contrat auquel la personne concernée est partie. En matière de *spamming* (ce que l'on traduit en français par pollu-postage, c'est-à-dire de messages publicitaires non sollicités), le principe demeure celui du consentement préalable des personnes physiques (interdit repris par la loi du 21 juin 2004). De même, pour les « cookies », la directive européenne et la loi du 6 août 2004 impliquent que les sites qui se livrent à ce placement de mouchards dans les ordinateurs privés doivent justifier de leur utilisation et en avertir les internautes.

> Le règlement européen du 27 avril 2016 redéfinit le consentement pour en renforcer le caractère explicite : « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

Il doit être distinct de toute autre démarche désormais. La charge de la preuve de ce consentement incombe au responsable du traitement le cas échéant. Le RGPD exige que l'utilisateur de services (téléphonie ou internet) soit mis en mesure de donner son consentement de façon libre, spécifique, éclairée et univoque au traitement de ses données personnelles (opérations de lecture et d'écriture dans le terminal d'un utilisateur), ce qui suppose une présentation claire et distincte de l'ensemble des utilisations qui seront faites des données recueillies.

> ***Exemple***
> La CNIL a encore sanctionné le réseau social TikTok pour un montant total de 5 M€ parce que ses utilisateurs ne pouvaient pas refuser les cookies aussi facilement que les accepter (plusieurs clics étaient nécessaires pour refuser tous les cookies, contre un seul pour les accepter) et qu'ils n'étaient pas informés de façon suffisamment précise des objectifs des différents cookies (CNIL, communiqué, 12 janv. 2023).
>
> Le Conseil d'État (CE, 19 juin 2020, Société Google LLC, déc. n° 430810) a ainsi confirmé une sanction de 50 millions d'euros à la charge de Google car l'utilisateur qui souhaite créer un compte Google pour utiliser le système Android est d'abord invité à accepter que ses informations soient traitées conformément à un paramétrage par défaut, incluant un ciblage publicitaire au milieu d'informations relatives à d'autres finalités. Il a aussi (CE, 28 janvier 2022, soc. Google LLC, déc. n° 449209) confirmé deux amendes d'un montant total de 100 millions d'euros infligées par la CNIL à l'encontre de Google qui n'a pas respecté ses obligations en matière de recueil du consentement de ses utilisateurs pour le dépôt de cookies (article 82 de la loi informatique et libertés, transposant la directive européenne *e-Privacy* de 2002) : absence d'information claire et complète des utilisateurs, défaut de recueil préalable de leur consentement et mécanisme défaillant d'opposition aux cookies publicitaires.
> Le Conseil d'Etat (CE, 27 juin 2022, déc. n° 451423) confirme l'amende d'un montant de 35 M€ à l'encontre de la société Amazon Europe Core, notamment pour avoir déposé des cookies publicitaires sur les ordinateurs d'utilisateurs du site de vente « Amazon.fr » sans consentement préalable ni information satisfaisante.

Le consentement doit porter sur chacune des finalités poursuivies par le traitement de données et toute nouvelle finalité ultérieure, compatible avec la ou les finalités initiales, assignée au traitement de données est soumise au recueil d'un consentement propre. En cas de recueil effectué de manière globale, il doit être précédé d'une information spécifique à chacune des finalités. Le Conseil d'État (CE, 19 juin 2020, Société Google LLC, déc. n° 430810) ainsi confirmé une sanction de 50 millions d'euros à la charge de Google car l'utilisateur qui souhaite créer un compte Google pour utiliser le système Android est d'abord invité à accepter que ses informations soient traitées conformément à un paramétrage par défaut, incluant un ciblage publicitaire au milieu d'informations relatives à d'autres finalités. L'information fournie est donc insuffisante.

Sauf obligation légale contraire, pour des raisons légitimes, la personne intéressée peut s'opposer au traitement. Il doit s'agir de motifs tenant à une situation particulière l'emportant sur les intérêts du responsable du traitement. Ainsi, des parents ne peuvent pas s'opposer, par principe, sans motif particulier, à un traitement de données de leur enfant scolarisé dans la « base élève 1er degré » de l'éducation nationale (CE, 18 nov. 2015, déc. n° 384869). Seule la personne concernée dispose de ce droit, ce qui n'est pas le cas, selon le Conseil d'État, des ayants droit d'un défunt (qui demandaient à son employeur de leur communiquer les relevés de téléphone pour étayer un contentieux d'ordre médical : CE, 8 juin 2016, déc. n° 386525). Il s'agit le plus souvent de s'opposer à l'utilisation des données à des fins de prospection commerciale. Mais parfois la motivation va plus loin, comme dans le cas d'un homme voulant faire arracher la page du registre paroissial mentionnant son baptême (alors qu'il avait déjà obtenu son annulation). La Cour de cassation considère que cette donnée est « *un fait dont la réalité historique ne pouvait être contestée* » (Cass. 1ère civ., 19 novembre 2014, pourvoi n ° 13-25.156). L'exercice de ce droit suppose également le droit d'interroger et d'accéder à la base de données sans avoir à fournir un motif. L'article 39 de la loi précise que toute personne physique justifiant de son identité a le droit d'interroger le responsable du traitement de données à caractère personnel. L'individu dispose également d'un droit de copie de ses propres données. Toutefois lorsqu'il s'agit d'un traitement intéressant la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans des conditions spécifiques, de manière indirecte, par l'un des membres de la CNIL. Il en est de même des données à caractère médical pour lesquelles le droit d'accès peut s'exercer directement ou par l'intermédiaire d'un médecin désigné par la personne concernée. Le droit de rectification permet à toute personne de corriger les erreurs décelées à l'occasion de la communication des informations. Le responsable doit procéder à la modification sans frais et la justifier auprès des demandeurs.

Une des difficultés rencontrées tient à la question de **l'identité numérique**. Sur internet, l'identité est souvent portée par des pseudonymes qui garantissent l'anonymat et donc la vie privée (même si par ailleurs ils sont aussi source d'impunité pour la commission d'infractions). Or, lorsqu'une demande de droit d'accès aux

données est effectuée (notamment auprès des autorités publiques), il est exigé de présenter son identité nominative, ce qui revient à créer de nouvelles données personnelles et à lever l'anonymat protecteur.

Le règlement européen du 27 avril 2016 ajoute **le droit à la « portabilité des données »,** c'est-à-dire le droit de récupérer les données personnelles recueillies par les prestataires de services numériques auxquels ils ont fait appel (e-mails, listes de contacts, etc.) et de les transférer auprès d'autres prestataires en cas de changement. Il s'agit ici moins d'un droit à la protection de la vie privée que d'un droit du consommateur permettant de faire jouer la concurrence et, collectivement, de fluidifier le marché.

Le règlement ne distingue pas les données sensibles des autres, mais évoque d'une part **le profilage et traite spécifiquement les données liées au corps : génétiques, biométriques, de santé**.

> Le grand danger des *big data* est le « profilage », c'est-à-dire « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* » (règlement européen du 27 avril 2016, art. 4).

Ce profilage ne sera autorisé que si la personne concernée donne son consentement, si la loi le permet ou s'il est nécessaire à la conclusion d'un contrat. Ainsi, le règlement institue le droit de ne pas faire l'objet d'une décision qui se fonderait exclusivement sur un traitement de données automatisées qui affecterait une personne de manière significative. Cela implique qu'on puisse exiger une intervention humaine.

Selon l'article 9 : « *Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.* »
Les exceptions sont nombreuses :

- la personne concernée a donné son consentement explicite ;
- en matière de droit du travail, de la Sécurité sociale et de la protection sociale (sous conditions) ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- le traitement est mis en œuvre par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ;
- les données sont manifestement rendues publiques par la personne concernée ;
- pour l'exercice ou la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;
- pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;
- dans le cadre de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale ;
- si le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ;
- si le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Vient enfin le « Droit à l'oubli ». Cette expression, très galvaudée, peut désigner plusieurs objets, comme l'effacement de pages internet, le déréférencement des moteurs de recherche (voir le chapitre sur la liberté d'expression sur internet), l'interdiction faite aux assureurs ou employeurs de discriminer une personne dont le dossier médical fait apparaître un cancer en rémission, l'effacement des données contenues dans un fichier…

Dans le cas des données personnelles, l'article 17 du règlement européen (« droit à l'effacement – droit à l'oubli ») ne fait au fond que rassembler des hypothèses déjà prévues :
« *La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :*
- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière,
- la personne concernée retire le consentement sur lequel est fondé le traitement,
- la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement,
- les données à caractère personnel ont fait l'objet d'un traitement illicite, les données à caractère personnel doivent être effacées pour respecter une obligation légale, les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information. »

Le Conseil constitutionnel (CC, 27 octobre 2017, M. Mikhail P. déc. n° 2017-670 QPC [Effacement anticipé des données à caractère personnel inscrites dans un fichier de traitement d'antécédents judiciaires]) a eu l'occasion d'appliquer la même philosophie en censurant les dispositions qui restreignaient la liste des personnes pouvant demander l'effacement de leurs données contenues dans le TAJ (fichier de traitement d'antécédents judiciaires). Ce fichier peut contenir les informations recueillies au cours d'une enquête ou d'une instruction concernant une personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait pu participer à la commission de certaines infractions et seules peuvent demander l'effacement les personnes ayant fait l'objet d'un acquittement, d'une relaxe, d'un non-lieu ou d'un classement sans suite. Eu égard à l'ampleur des occasions où se fichier est consulté, le Conseil juge ces restrictions disproportionnées.

La Cour de cassation (Cass. crim., 10 avr. 2018, pourvoi n° 17-84.674) a audacieusement appliqué ce droit dans l'hypothèse d'un fichier judiciaire. Le requérant a demandé l'effacement de ses données dans le fichier automatisé des empreintes digitales (FAED) mais le président de la chambre de l'instruction s'y était opposé au motif que sa demande était irrecevable car ne lui avait pas fourni les éléments objectifs sur les circonstances de la commission de l'infraction et sur sa personnalité, lui permettant d'apprécier la nécessité de la conservation de ses empreintes digitales. Le décret instituant le fichier (du 8 avril 1987), prévoit les hypothèses dans lesquelles le procureur responsable du traitement doit effacer les données. Le juge s'est fondé sur ces dispositions pour demander au demandeur de lui fournir la preuve d'un des éléments. La Cour de cassation casse l'ordonnance car il appartenait au président de la chambre de l'instruction de vérifier lui-même si l'enregistrement des empreintes répondait aux conditions réglementaires, et d'apprécier si leur conservation était ou non nécessaire pour des raisons liées à la finalité du fichier au regard notamment de la nature ou des circonstances de la commission de l'infraction, ou de la personnalité de la personne concernée. La Cour intègre ainsi clairement le changement de paradigme du droit des données : désormais, même le fichage judiciaire ne paraît plus en soi légitime et la puissance publique doit en justifier l'usage.

Le droit de l'Union consacre en partie le Droit au déréférencement des moteurs de recherches. En fonction de la densité des recherches effectuées par les internautes et leurs mots clefs (le nom d'une personne par exemple), certaines pages, même anciennes, apparaissent dans les premières mentions des moteurs de recherche et anéantissent toute possibilité d'oubli de l'information, même quand la justice à lavé la personne de tout soupçon. Sous l'angle du droit des données personnelles cela contrarie le droit à l'effacement. Les moteurs de recherche étant des traitements, les entreprises qui commercialisent ses moteurs doivent accéder à la demande de « déréférencement ». Cette obligation n'est pas prévue par les textes européens et n'existe qu'à la demande de la personne fichée et peut être limité géographiquement au pays concerné (« géoblocage » à partir de l'adresse IP de l'internaute consultant). Cependant cela s'oppose aussi à la liberté de l'information, il ne s'agit donc pas d'effacer la page qui fournit une information exacte et légale mais de ne pas en faciliter l'accès. Pour la Cour européenne, ces moteurs sont un instrument susceptible « *bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée* » (CEDH, 5 mai 2011, Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine, §63/949).

La CJUE a déjà posé les bases de ce droit pour les données personnelles non sensibles et posé le principe selon lequel les droits fondamentaux contenus aux articles 7 et 8 de la Charte « *prévalent, en principe, non*

seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne » (CJUE, Gr. Ch., 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et a, aff. C-131/12). Un intérêt du public prépondérant pour une information peut néanmoins conduire à refuser le déréférencement (CJUE, Gr. Ch., 24 septembre 2019, GC, AF, BH, ED c/ CNIL, n° C-136/17 et CJUE, Gr. Ch., 24 septembre 2019, Google LLC c/ CNIL, n° C-507/17). Pour identifier l'existence d'un intérêt du public prépondérant à obtenir une information particulière en tapant le nom d'une personne, la CNIL doit s'intéresser à la nature des données en cause, leur contenu, leur caractère plus ou moins objectif, leur exactitude, leur source, les conditions et la date de leur mise en ligne et les répercussions que leur référencement est susceptible d'avoir pour la personne concernée d'une part, mais aussi à la notoriété de cette personne, son rôle dans la vie publique et sa fonction dans la société d'autre part, tout en prenant en compte « *la possibilité d'accéder aux mêmes informations à partir d'une recherche portant sur des mots-clés ne mentionnant pas le nom de la personne concernée ainsi que le rôle qu'a, le cas échéant, joué cette dernière dans la publicité conférée aux données la concernant* » (CE, 6 déc. 2019, déc. n° 395335, cons. 11 ; n° 405910, cons. 9 ; n° 409212, cons. 10).

Concernant les données sensibles, la Cour de cassation, à propos d'informations relatives à un procès pénal, a estimé que le juge du fond devait éviter d'ordonner une mesure d'injonction d'ordre général conférant un caractère automatique à la suppression de la liste de résultats et apprécier la portée effective du sacrifice de la vie privée au bénéfice du droit à l'information du public sans autre précision (Cass. 1ère civ., 14 fév. 2018, pourvoi n° 17-10.499, Sté Google Inc. et Cass. 1ère civ., 27 nov. 2019, pourvoi n° 18-14.675).

Le Conseil d'État a été saisi par plusieurs requérants de recours à l'encontre de décisions de la CNIL refusant de mettre en demeure la société Google de procéder à certains déréférencements, en application de l'arrêt Google Spain, vers une vidéo « youtube » et plusieurs liens renvoyant à des articles de journaux, des billets de blogs ou d'autres médias faisant état de la proximité des requérante avec l'ancien Président de l'Algérie ou leur condamnation pour apologie de crimes contre l'humanité (alors que la Cour de cassation avait par ailleurs cassé ces décisions), ou bien encore vers une fiche descriptive d'un livre autobiographique écrit par l'un des requérants et dans lequel il fait état de son homosexualité. Ici il faut resserrer les exigences et ne refuser le déréférencement que si il est strictement nécessaire à l'information du public (CE, 6 déc. 2019, déc. n° 395335, cons. 15) c'est-à-dire si on ne peut y accéder autrement que par la mention du nom. La CNIL devra alors utiliser les mêmes indices que précédemment évoqués, à l'exception de celui relatif au rôle joué par la personne demandant le déréférencement. Néanmoins, le maintien de l'information nominative sera assorti d'une obligation lourde pour le moteur de recherches : il se devra, « *au plus tard à l'occasion de la demande de déréférencement, aménager la liste de résultats de telle sorte que les liens litigieux soient précédés sur cette liste de résultats d'au moins un lien menant vers une ou des pages web comportant des informations à jour* » (CE, 6 déc. 2019, déc. n° 401258, cons. 13). Cela pour s'assurer du respect de la réputation. Enfin, si la personne ayant fait la demande de déréférencement est aussi celle qui est à l'origine de la publication de l'information, le CNIL devra abaisser l'intensité de son contrôle : elle n'aura plus à vérifier s'il existe un intérêt impérieux du public à avoir accès à l'information en tapant le nom de la personne.

§3. Le contrôle

Le RGPD a conduit a supprimé les procédures préalables, autorisations ou déclarations. Seuls certains fichiers doivent encore être déclarés en raison de la sensibilité des données, en particulier dans le domaine de la santé, pour la collecte en ligne et pour les fichiers administratifs régaliens.

Seules perdurent les autorisations pour les traitements de données personnelles du secteur de la santé présentant une finalité d'intérêt public (hors recherche qui suivent un autre régime d'autorisation).

D'autres obligations entrent en vigueur, notamment l'obligation pour les organismes de **remplir un ou plusieurs registres internes** :

- le registre des traitements (article 30.1) ;
- le registre des activités de sous-traitance (article 30.2) ;
- le registre des violations de données à caractère personnel (article 33).

La CNIL contrôle ces obligations. Elle est composée de 17 membres: quatre parlementaires, deux membres du conseil économique et social, deux conseillers d'État, deux conseillers de la Cour de cassation, deux conseillers à la Cour des comptes, cinq personnalités qualifiées pour leurs connaissances en informatique ou des questions touchant aux libertés individuelles. Le président est élu en son sein. Le mandat est de cinq ans renouvelables une fois sans qu'il puisse être mis fin à ce mandat de façon anticipée, sauf empêchement constaté par la commission.

La CNIL se charge de nombreuses missions, particulièrement d'information auprès de toute personne concernée, mais aussi une mission de publication et d'élaboration des normes destinées aux procédures d'autorisations et de déclarations. Elle répond aux demandes d'avis des pouvoirs publics et assure le suivi des réclamations et plaintes relatives au traitement de données à caractère personnel. Pour ce faire la CNIL peut procéder à un certain nombre de vérifications et accéder ainsi au traitement qui entre dans son champ de compétence. Elle dispose également d'un pouvoir de proposition en faveur de l'évolution de la loi. En cas d'autorisation, la CNIL se prononce dans les deux mois à compter de la réception de la demande, son silence signifiant rejet. Si les dispositifs relatifs au traitement des données personnelles font l'objet de sanctions pénales, le plus souvent il est possible de saisir la CNIL qui opérera une médiation dans le cadre de ses missions de contrôle. Ensuite, le président de la CNIL peut saisir en référé le juge compétent pour faire cesser une atteinte grave et immédiate aux droits fondamentaux et saisir le parquet des infractions dont la Commission a connaissance. De son propre chef, en cas d'urgence, la CNIL peut décider l'interruption du traitement pour trois mois maximum, décider le verrouillage de certaines données, informer le Premier ministre pour qu'il prenne les décisions concernant les services de l'État. Des sanctions pécuniaires pouvant aller jusqu'à 300 000 euros d'amende ou 5 % du chiffre d'affaires permettent de dissuader les responsables.

La Cour de Justice de l'Union Européenne (CJUE, 6 octobre 2015, aff. C-362/14, Maximillian Schrems c/ Data Protection Commissioner) a eu l'occasion de renforcer le rôle des instances telles que la CNIL en insistant sur le fait qu'elles peuvent contrôler elles-mêmes la condition d'équivalence des protections nécessaire à des transferts de données transfrontières hors de l'Union européenne. Ainsi, même en présence d'une décision de la Commission, les autorités nationales de contrôle, saisies d'une demande, doivent pouvoir examiner en toute indépendance si le transfert des données d'une personne vers un pays tiers respecte les exigences posées par la directive. La Cour se fonde alors sur l'autorité de la Charte des droits fondamentaux de l'Union qui reconnaît un droit autonome à la protection des données. Ainsi, la Cour annihile les effets d'un accord (« *Safe Harbour* ») conclu entre l'UE et les Etats-Unis qui permettait aux américains d'assurer eux-mêmes que leur protection est équivalente à celle de l'Europe, alors même que les données européennes, collectées par des grands collecteurs américains, étaient transmises sans garanties aux agences de renseignement du gouvernement américain.

En revanche, **le Conseil d'Etat a dû rappeler que la CNIL ne dispose pas d'un pouvoir réglementaire au-delà de ce que la loi lui accorde.** Le droit souple qu'elle édicte ne peut donc pas servir de base à une répression portant sur des normes nouvelles qu'elle aurait ainsi édicté. Ce fût le cas des lignes directrices souples spécifiques aux cookies. Elle en a la compétence, à condition de ne pas leur accorder de valeur contraignante (CE, 19 juin 2020, Association des agences-conseils en communication et autres, déc. n° 434684). Sur cette base, elle a tout de même considéré que la pratique qui consiste à bloquer l'accès à un site web ou à une application mobile si l'utilisateur ne consent pas à être suivi (« *cookie walls* ») n'est pas conforme au RGPD, ce que le Conseil d'Etat a censuré.

Section 3 : Données, renseignements et surveillance de masse

§1. En droit de l'Union

L'article 5.1 de la directive 2002/58/CE de 2002 protège le principe de confidentialité des communications effectuées au moyen d'un réseau public de communication (internet) ainsi que la confidentialité des données relatives au trafic de ce réseau. Il est donc interdit à toute autre personne que les utilisateurs d'écouter, d'intercepter ou de stocker les communications et les données. Il impose également l'effacement ou l'anonymisation des données relatives au trafic par le fournisseur du réseau public de communication. À l'inverse, les opérateurs ont une obligation de conservation et de mise à disposition de l'autorité judiciaire des données techniques qui pourraient être utiles dans le cadre de la constatation de la poursuite des infractions pénales. Ils doivent conserver ces informations pendant un an (loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme). Il en est de même des fournisseurs de services de connexion. La loi sur l'économie numérique prévoit qu'ils détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu des services dont ils sont prestataires. La directive européenne du 15 mars 2006 a indiqué que les données relatives au trafic et à la localisation, générées par l'utilisation de services de communications électroniques, doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication. D'une manière générale il doit être mis fin aux traitements informatiques lorsque la durée nécessaire aux finalités poursuivies est achevée.

La directive 2002/58/CE du 12 juillet 2002, impose que « *les systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires* ». L'article 15 de la directive permet pourtant d'y déroger : « *lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques* ». L'avis 1/15 admet le principe du transfert de données (passagers aériens) dans le cadre de la lutte contre le terrorisme (CJUE, Gr. Ch., 26 juill. 2017, Avis 1/15, Projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers).
Selon la directive 2006/24/CE du 15 mars 2006, dite directive *e-Privacy,* pour lutter contre le terrorisme, la conservation de toutes les données relatives au trafic en matière de téléphonie fixe et mobile, d'accès à internet, de courrier électronique et de téléphonie via internet alors même que l'article 7 de la Charte des droits fondamentaux et l'article 8 prévoient la protection des données personnelles et leur effacement. Par deux arrêts du 8 avril 2014, la Cour de justice de l'Union européenne a invalidé ces dispositions au motif que le législateur européen avait dépassé les limites appropriées et nécessaires aux objectifs de recherche, de détention et de poursuite d'infractions graves, en imposant à ces fournisseurs une trop large obligation de conservation des données, sans encadrement strict : « *la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ou exception soient opérées en fonction de l'objectif de lutte contre les infractions graves* ». Et elle conclut que « *force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* ». La Cour considère que la directive aurait dû prévoir des règles claires et précises régissant la portée et l'application de cette mesure et imposer un minimum d'exigences pour que les personnes disposent de garanties suffisantes comme la conservation des données sur le territoire de l'Union (CJUE, Gr. Ch., 8 avr. 2014, Digital Rights Ireland Ltd et autres et Kärntner Landesregierung et autres, aff. jtes C-293 et 594/12).

En 2017, dans l'affaire *Tele2 Sverige AB.* (CJUE, Gr. Ch., 21 déc. 2016, aff. jtes C-203/15 et C-698/15, Tele2 Sverige AB c/Post-ochtelestyrelsen et Secretary of State for the Home Department c/Tom Watson), la CJUE a été amenée à compléter sa jurisprudence quant à l'obligation générale de conservation des données : est-elle, *en soi*, excessive indépendamment d'éventuelles garanties ? Appliquant la directive 2002/58/CE au domaine de la sécurité et de la répression pénale, la Cour s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique. Elle refuse de laisser aux États le soin d'apprécier des nécessités particulières accompagnées de garanties propres comme elle refuse que la conservation et l'accès aux données soient traités différemment l'un de l'autre : l'accès des autorités nationales aux données conservées doit être limité au cadre de la lutte contre la criminalité grave, sous le contrôle préalable d'une juridiction ou d'une autorité administrative indépendante. Les données en cause doivent en outre être conservées sur le territoire de l'Union. La règle devient la non-conservation des données, l'interdiction de la surveillance généralisée mais la possibilité d'une surveillance ciblée, adéquate et proportionnée (ce que la Cour accepte à l'égard des fichiers de police, voir *infra*). L'arrêt *Tele2 Sverige AB*, exige en outre une information à destination des personnes concernées, cette information étant, de fait, « *nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours* ».

La Cour admet, au demeurant, l'obligation légale pour les opérateurs de téléphonie mobile de recueillir des données personnelles des utilisateurs de cartes SIM prépayées, y compris en dehors de toute nécessité liée à la facturation ou au contrat, et de les tenir à la disposition d'autorités sans avoir à disposer d'une décision de justice ou à en notifier les personnes concernées si cela est nécessaire « *à la poursuite des infractions pénales et administratives, à la prévention d'un danger et à l'accomplissement de tâches liées au renseignement* » (CEDH, 30 janv. 2020, Breyer c. Allemagne, req. n° 50001/12). En l'absence de consensus européen quant à la collecte et à la conservation d'informations sur les détenteurs de cartes SIM prépayées, les États membres du Conseil de l'Europe jouissent d'une certaine marge d'appréciation. En outre, l'enregistrement ne portait pas sur des informations hautement personnelles ou permettant de créer des profils de personnes ou de retracer les déplacements des abonnés. De plus, aucune donnée concernant des communications particulières n'était conservée. Sans être insignifiante, l'ingérence a donc été de nature relativement limitée, comme la durée de la conservation (un an).

En France, l'article L. 851-2 du Code de la sécurité intérieure, depuis la loi « renseignement » n° 2015-912 du 24 juillet 2015, permet (pour deux mois renouvelables et après avis de la Commission nationale de contrôle des techniques de renseignement), pour les seuls besoins de la prévention du terrorisme, dans le cas d'une personne préalablement identifiée susceptible d'être en lien avec une menace terroriste, le recueil en temps réel, sur les réseaux des opérateurs à l'égard de tous les services de communication au public en ligne, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion, à la localisation des équipements terminaux utilisés, ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. Depuis la loi n° 2016-987 du 21 juillet 2016, la mesure s'étend à l'entourage de la personne lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation, sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation ; celle-ci peut être également accordée individuellement pour chacune de ces personnes.

À propos de ces données de trafic, le Conseil d'État a tenté de demander à la CJUE d'assouplir sa position (CE, 26 juill. 2018, Ass. Quadrature du Net et autres, Igwan.net., déc. n° 394922 ; CE, 26 juill. 2018, French Data Network, déc. n° 393099). Mais en même temps (CJUE, 2 oct. 2018, Ministerio Fiscal, aff. C-207/16), la Cour a admis que toutes les infractions pénales, sans atteindre une particulière gravité peuvent néanmoins justifier un accès du juge national aux données à caractère personnel conservées par des fournisseurs de services de communications électroniques dès lors que cet accès ne porte pas une atteinte grave à la vie privée. Dans le cadre de l'enquête sur un vol avec violences d'un portefeuille et d'un téléphone mobile, la police judiciaire espagnole a demandé au juge d'instruction responsable de l'affaire de lui accorder l'accès aux données d'identification des utilisateurs des numéros de téléphone activés depuis le téléphone volé. La loi espagnole s'y oppose, prévoyant que seules les infractions punies d'une peine de prison supérieure à

cinq ans le permettent. Mais la directive *Vie privée et communications électroniques* ne prévoit rien de tel. Cette nouvelle précision n'est pas contradictoire dans la mesure où l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne. En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée dans ce domaine que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave ».

Le droit de l'UE s'oppose à une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques, même pour lutter contre les infractions graves. En particulier, les obligations pour les fournisseurs de services de communications électroniques, de transmettre ou de conserver des données de connexion de leurs utilisateurs, de manière généralisée et indifférenciée, même limitées aux fins de lutte contre les infractions ou en cas d'atteinte à la sécurité nationale (CJUE, 6 oct. 2020, Privacy International, aff. C-623/17). L'objectif de lutte contre la criminalité ne saurait à lui seul justifier qu'une mesure de conservation généralisée et indifférenciée des données relatives au trafic et à la localisation soit considérée comme nécessaire. Par trois décisions rendues le 6 octobre 2020 (CJUE, 6 octobre 2020, Privacy International, aff. C-623/17 ; La Quadrature du Net e.a., French Data Network e.a., aff. C-511/18 et C-512/18 ; Ordre des barreaux francophones et germanophone e.a., aff. C-520/18), la CJUE a précisé que la conservation généralisée et indifférenciée des données de connexion (autres que les données d'identité) ne peut être imposée aux opérateurs que pour les besoins de la sécurité nationale en cas de menace grave et sous le contrôle préalable d'une autorité indépendante et d'un juge en aval, lors de l'exploitation des données conservées. Toutefois, pour la lutte contre la criminalité grave, les États peuvent imposer la conservation ciblée de données, dans certaines zones ou pour certaines catégories de personnes pré-identifiées comme présentant des risques particuliers. La Cour censure d'ailleurs, des formes de détournement de procédure tel le fait d'admettre comme éléments de preuve des données relatives au trafic et des données de localisation afférentes à des appels téléphoniques dans une procédure pour homicide (CJUE, GC, 5 avr. 2022, Commissioner of the Garda Síochána e.a., aff. C-140/20). Le Conseil d'État, pour concilier le respect du droit européen et les exigences du gouvernement français dans sa lutte contre le terrorisme et la criminalité grave, avait admis le maintien de la conservation et d'accès des autorités publiques aux données, et jugeait que la conservation généralisée des données était justifiée par l'existence d'une menace pour la sécurité nationale (CE, 21 avr. 2021, La Quadrature du Net e.a., déc. n° 393099). Mais la CJUE rappelle que la menace grave pour la sécurité nationale doit être réelle et actuelle ou prévisible (CJUE, 6 oct. 2020, La Quadrature du Net e.a., aff. jointes C-511/18). En outre, ce type de décision doit pouvoir faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante (donc pas un fonctionnaire de police), dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations, ainsi que le respect des conditions et des garanties devant être prévues.

La Cour admet néanmoins comme proportionnées (à condition d'être posées par des règles claires et précises, et de poser des garanties effectives contre les risques d'abus) :

- une conservation ciblée des données relatives au trafic et à la localisation en fonction de catégories de personnes concernées ou au moyen d'un critère géographique (comme le taux moyen de criminalité dans une zone, les infrastructures stratégiques ou très fréquentées comme aéroports, gares, ports maritimes, zones de péage) pour obtenir des informations de fréquentation ;
- une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques (carte SIM prépayée par exemple, pour laquelle le vendeur vérifiera et enregistrera les documents d'identité officiels), pour une période temporellement limitée au strict nécessaire ;
- une conservation rapide (*quick freeze*) des données relatives au trafic et à la localisation, dont disposent les fournisseurs de services dès le premier stade de l'enquête portant sur une menace grave pour la sécurité publique, ou sur un éventuel acte de criminalité grave, sur la base d'éléments objectifs et non discriminatoires.

La chambre criminelle a également tiré les conséquences de ces positions européennes concernant les données de trafic (qui établissent les contacts qu'une personne a eus par téléphone ou SMS, la date et l'heure de ces contacts, la durée de l'échange) et les données de localisation (qui permettent de connaître les zones d'émission et de réception d'une communication passée avec un téléphone mobile identifié, et d'obtenir la liste des appels ayant borné à la même antenne relais). Elle juge que la réglementation française (avant la loi n ° 2021-998 du 30 juillet 2021), en ce qu'elle prévoyait la conservation générale des données de connexion

pour la protection des intérêts fondamentaux de la Nation et la lutte contre le terrorisme, était conforme au droit de l'Union, sous réserve d'un réexamen périodique de l'existence d'une menace grave pour la sécurité nationale. Il faut donc qu'un juge d'instruction (et non seulement le parquet) puisse vérifier que les faits en cause relèvent de la criminalité grave et que la conservation « rapide » des données de connexion et l'accès à celles-ci respectent les limites du strict nécessaire. La loi en ce qu'elle permet au procureur de la République, ou à un enquêteur, d'accéder aux données est donc contraire au droit de l'Union, car elle ne prévoit pas un contrôle préalable par une juridiction ou une entité administrative indépendante. Cependant, l'acte ayant permis d'accéder aux données ne peut être annulé par le juge que s'il a été porté atteinte à la vie privée de la personne mise en examen et si celle-ci a subi un préjudice. La personne mise en examen peut contester efficacement la pertinence des preuves tirées de ses données, mais elle ne peut invoquer la violation des exigences en matière de contrôle de l'accès aux données que si elle prétend être titulaire ou utilisatrice d'une ligne identifiée, ou si elle démontre qu'à l'occasion de ces investigations, il a été porté atteinte à sa vie privée (par exemple que les données n'étaient pas limitées à ce qui était strictement nécessaire au bon déroulement de l'enquête en cause). Ce qui n'était pas le cas dans les affaires jugées (Cass. crim., 12 juill. 2022, pourvois n^{os} 21-83.710, 21-83.820, 21-84.096 et 20-86.652).

§2. En droit de la CEDH

La Cour européenne a été saisie de ce type de mesures dans son arrêt *Big Brother Watch et autres c. Royaume-Uni* (CEDH, 13 sept. 2018, Big Brother Watch et autres c. Royaume-Uni, req. n^{os} 58170/13, 62322/14 et 24960/15) qui censure en partie des systèmes britanniques de surveillance sur des plaintes de journalistes et d'organisations de défense des droits : il s'agit d'abord, d'interception massive de communications, qui certes n'emporte pas en lui-même violation de la Convention, mais pour laquelle l'exploitation doit toutefois répondre, pour respecter l'article 8, à six exigences fondamentales, énoncées dans l'arrêt *Weber et Saravia c. Allemagne* (CEDH, 29 juin 2006, Weber et Saravia c. Allemagne (déc.), req. n° 54934/00) : les buts pour lesquels l'interception peut être autorisée ne doivent pas être trop vagues (« *l'intérêt de la sécurité nationale* », « *la prospérité économique du Royaume-Uni* ») pour pouvoir constituer une limite claire aux activités des services de renseignement ; le champ d'application doit être clair (par. ex. la notion de communication « intérieure » est floue) ; la durée doit être délimitée et non renouvelable à l'infini ; le filtrage, le stockage et l'analyse des éléments interceptés doivent présenter des garanties contre l'ingérence arbitraire et disproportionnée ; la divulgation des éléments interceptés doit être limitée au « *minimum nécessaire dans les buts autorisés* » ; enfin il faut des garanties efficaces ou contraignantes contre la conservation disproportionnée des données interceptées. Il s'agit ensuite de l'obtention de données de communication auprès de fournisseurs de services de communication, qui doit tenir compte de la spécificité des informations journalistiques confidentielles pour respecter l'article 10. Enfin, la Cour dit que le dispositif de partage de renseignements avec des États étrangers n'emporte violation ni de l'article 8 ni de l'article 10.

La Cour européenne (CEDH, Gr. Ch., 25 mai 2021, Big Brother Watch et autres c. Royaume-Uni, req. n^{os} 58170/13, 62322/14 et 24960/15) a dû toute de même sanctionner le système de renseignements britannique (*Regulation of Investigatory Powers Act 2000*) impliquant l'interception en masse de communications, la réception d'éléments interceptés obtenus auprès de gouvernements et de services de renseignement étrangers et l'obtention de données de communication auprès des fournisseurs de services de communication. Compte tenu des multiples menaces auxquelles les États doivent faire face dans les sociétés modernes, le recours à un régime d'interception en masse n'est pas en soi contraire à la Convention. Toutefois, pareil régime doit être encadré par des « garanties de bout en bout », c'est-à-dire qu'au niveau national la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ (dès la définition de l'objet et de l'étendue de l'opération) et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori*. Ainsi, le système de renseignement de la Suède présente des carences en l'absence de règle claire concernant la destruction des éléments interceptés, la décision de partage de renseignements avec des partenaires étrangers, et l'absence de contrôle *a posteriori* effectif (CEDH, Gr. Ch., 25 mai 2021, Centrum för rättvisa c. Suède, req. n° 35252/08).

N’est pas suffisante pour fonder des poursuites judiciaires (par le recueil de données relatives au trafic et des données de localisation) une législation qui n’autorise la conservation des données de télécommunication qu’à des fins de facturation et à des fins commerciales et de manière généralisée et indifférenciée pendant 14 mois (CEDH, 15 février 2024, Škoberne c. Slovénie, req. n° 19920/20).

La Cour a aussi sanctionné le système polonais de « surveillance secrète » d’une loi anti-terrorisme. L’absence de recours internes effectifs au moyen desquels les personnes qui se croient surveillées pourraient contester les mesures de surveillance est sanctionnée *in abstracto*, comme l’absence de contrôle indépendant, n’empêchant pas le recours excessif à la surveillance. Enfin, les prestataires de services TIC2 sont tenus de conserver de manière généralisée et indifférenciée les données de communication aux fins d’un accès éventuel par les autorités nationales compétentes, s’avère insuffisante à limiter à ce qui est « nécessaire dans une société démocratique » (CEDH, 28 mai 2024, Pietrzak et Bychawska-Siniarska et autres c. Pologne, n^{os} 72038/17 et 25237/18).