Droit à la vie privée

De Terwangne, Cécile

Published in:
Law, norms and freedom in cyberspace = Droit, normes et libertés dans le cybermonde

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 5
Droit à la vie privée : un droit sur l'information et un droit à l'information

Cécile DE TERWANGNE*

Introduction

1. Le droit à la vie privée a été de longue date au cœur des préoccupations scientifiques et académiques d'Yves Poullet[1]. Instrument de l'épa-

* Professeur à la Faculté de droit de l'Université de Namur, directrice de recherche au CRIDS.

[1] Une sélection dans sa bibliographie aura vite démontré l'intérêt marqué par Yves Poullet pour la matière de la vie privée depuis sa première publication en 1977… : Y. POULLET, « Privacy : conditions for its survival in our I.S. », *Data Protection Review*, 2010, http://www.dataprotectionreview.eu/ ; L. COSTA, Y. POULLET, « Privacy and the regulation of 2012 », *Computer Law and Security Review.*, 2012, pp. 254-262; E. DEGRAVE, Y. POULLET, « Le droit au respect de la vie privée face aux nouvelles technologies », *Les droits constitutionnels en Belgique*, Bruxelles, Bruylant, 2011, pp. 1001-1035 ; Y. POULLET, « La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ? », *Legicom*, 2009, n° 4, pp. 47-69 ; Y. POULLET, A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance de la vie privée pour la démocratie », *État de droit et virtualité*, Montréal, Thémis, 2009, pp. 157-222 ; Y. POULLET, « Pour une troisième génération de réglementation de protection des données », *Défis du droit à la protection à la vie privée*, coll. Cahiers du CRID, vol. 31, Bruxelles, Bruylant, 2008, pp. 25-70 ; Y. POULLET, « Internet et vie privée : entre risques et espoirs », *Journal des tribunaux*, 2001, n° 6000, pp. 155-165 ; P. TURNER, C. DE TERWANGNE, Y. POULLET, *Vie privée : nouveaux risques et enjeux – Privacy : new risks and opportunities*, Bruxelles, Stroy-Scientia, 1997 ; Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », *La vie privée : une liberté parmi les autres ?*, coll. Travaux de la Faculté de droit, n° 17, Bruxelles, Larcier, 1992, pp. 231-277 ; M.H. BOULANGER, C. DE TERWANGNE, Y. POULLET, « Protection de la vie privée face à l'informatique "made in Belgium" », *Droit de la consommation*, 1990, pp. 394-416 ; Y. POULLET, « Privacy Protection and Transborder Data Flow : Recent Legal Issues », *Advanced topics of law information technology*, Deventer, Kluwer Law and Taxation Publishers, 1989, pp. 29-41 ; Y. POULLET, J. BERLEUR, « Le droit à la vie privée selon le projet Gol », *J.T.*, 1982, pp. 769-711 ; Y. POULLET, « Informatique et vie privée : le projet de loi H. Vanderpoorten : commentaire du texte et comparaison avec les législations étrangères », *Une banque de données économiques régionale ? : Aspects économique, informatique, juridique et socio-politique*, Namur, Presses universitaires de Namur, 1977, pp. 299-381.

nouissement individuel, ce droit est aussi une condition de la démocratie en ce qu'il permet d'exercer d'autres droits et libertés et d'effectuer librement des choix existentiels. C'est parce qu'il est à l'abri de surveillance et d'intrusion d'autorités publiques que l'individu peut s'informer sans peur, échanger sans arrière-pensée, se mouvoir librement, s'associer avec d'autres, militer dans l'ombre, etc. L'enjeu démocratique qui s'attache à la protection de la vie privée n'a cessé de mobiliser les capacités analytiques, réflexives et créatives d'Yves Poullet qui s'est, dès le début de sa vie professionnelle, attaché avec brio et conviction à défendre cette valeur érigée en droit.

Les pages qui suivent sont consacrées à l'étude de ce droit dans son rapport à l'information. Les évolutions remarquables que la notion a connues et qui ont touché également l'étendue de sa protection ont fait apparaitre deux dimensions : le droit à la vie privée s'apparente aujourd'hui à un droit sur l'information et à un droit à l'information.

La société de l'information, société dans laquelle l'information et les services offerts par les technologies de l'information et de la communication servent de support à toutes les activités humaines, a exacerbé l'importance de ce rapport entre droit à la vie privée et information, et singulièrement vis-à-vis des données à caractère personnel. La phénoménale valeur économique et sociétale que ces données représentent dans le monde d'Internet et des objets connectés aujourd'hui explique qu'elles sont l'objet de convoitises concurrentes et sont au cœur d'intérêts rivaux. Cela étant, le droit à la vie privée s'exerce aussi plus largement, à l'égard d'informations qui ne relèvent pas de la catégorie des données à caractère personnel.

CHAPITRE 1. Droit à la vie privée : un droit sur l'information

SECTION 1. – Protection de la vie privée et divulgation d'informations privées. La vie privée comme rempart contre l'indiscrétion

2. Dans une vision première, traditionnelle, la vie privée est envisagée comme ce pan de l'existence que l'on mène à l'abri des regards, cette vie non pas nécessairement secrète mais réservée aux intimes, la vie privée de publicité en quelque sorte. Montaigne, déjà, voyait la vie privée comme

une arrière-boutique où se retirer : « Il faut se réserver une arrière-boutique toute nôtre, toute franche, en laquelle nous établissons notre vraie liberté et principale retraite et solitude »[2]. Dans cette première acception, le concept de vie privée garantit la solitude de l'individu (« le droit d'être laissé seul »[3]) ainsi que sa « solitude à plusieurs »[4], pour reprendre les termes de François Rigaux qui vise par cette expression la possibilité de nouer, librement et à l'abri de toute ingérence extérieure, des relations humaines.

Dans cette optique, l'individu doit pouvoir choisir l'information qu'il souhaite voir filtrer de l'autre côté du « mur de la vie privée »[5]. Pour Allan Westin, c'est d'ailleurs par cette faculté que se définit la *privacy* : « the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others »[6]. En dehors de ce choix, l'information c'est l'indiscrétion.

3. La protection de la vie privée s'effectue à ce stade par la condamnation des divulgations non consenties. Il s'agit de la protection classique contre les révélations – par le fait de la presse le plus souvent – des liaisons établies par une personne[7], de sa situation familiale, de son état de santé[8], de son passé, de ses convictions religieuses[9], etc. De telles révélations sont aujourd'hui à la portée de tout un chacun et s'effectuent par le truchement d'Internet, principalement au travers des réseaux sociaux, Facebook, Twitter, Instagram ou Youtube pour ne citer que ceux-là, ou par

---

[2] MONTAIGNE, *Essais*, I, 29.

[3] « The right to be let alone » (S. WARREN, L. BRANDEIS, « The Right to Privacy », *Harvard Law Review*, 1890, n° 4, 193).

[4] F. RIGAUX, « Protection de la vie privée : questions d'actualités », *Ann. Dr. Louv.*, 1984, p. 3.

[5] Expression suggérée par Royer-Collard, lors de la discussion de la loi sur la presse du 17 mai 1819, cité par R. LINDON, « La presse et la vie privée », *J.C.P.*, 1965, I, 1887.

[6] A. WESTIN, *Privacy and Freedom,* New York, Atheneum, 1967, p. 7.

[7] Cour eur. D.H., 24 juin 2004, arrêt *von Hannover c. Allemagne*, req. n° 59320/00 ; 25 novembre 2008, arrêt *Biriuk c. Lituanie*, req. n° 23373/03, § 41.

[8] Cour eur. D.H., 25 novembre 2008, arrêts *Armonienė c. Lituanie* et *Biriuk c. Lituanie*, req. n^{os} 36916/02 et 23373/03 (concernant la révélation que les requérants étaient porteurs du virus du SIDA). La divulgation d'informations relatives à la santé ne met pas seulement en jeu la vie privée de la personne concernée mais également la confiance de l'ensemble des patients dans la confidentialité de la prise en charge médicale : « *respecting the confidentiality of health data is crucial not only for the protection of a patient's privacy but also for the maintenance of that person's confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from seeking appropriate treatment, thereby endangering their own health and, in the case of transmissible diseases, that of the community* » (arrêt *Biriuk*, § 42).

[9] Cour eur. D.H., 6 juin 2013, arrêt *Avilkina c. Russie*, req. n° 1585/09 (concernant des Témoins de Jéhovah).

le dépôt de commentaires sur un portail d'actualités[10], pouvant toucher instantanément des milliers, voire des millions de destinataires.

Certaines divulgations peuvent être légitimées au nom de la liberté d'expression et du droit du public à l'information, lorsqu'un intérêt public s'attache à l'information en cause.

4. La protection de la vie privée ne va pas jusqu'à imposer aux médias ou à quiconque souhaite diffuser des informations d'intérêt public relatives à une personne une obligation de notification préalable, qui conduirait à prévenir cette personne de ce qu'on compte publier sur elle. Cela serait inévitablement susceptible de constituer une forme de censure avant la publication[11].

Par contre, la solution de consulter préalablement la personne concernée, voire même d'obtenir son consentement, avant de communiquer les informations la concernant peut être envisagée dans des circonstances où il ne s'agit pas de communication publique au nom de la liberté d'expression et du droit du public à l'information. La Cour européenne des droits de l'homme a ainsi évoqué cette solution dans le cadre de transmission d'informations médicales confidentielles par un hôpital aux autorités publiques à propos de témoins de Jéhovah[12]. C'est aussi dans cette ligne que s'inscrit la législation de protection des données qui impose un devoir de transparence vis-à-vis des personnes à propos de qui on récolte ou on communique des données, et qui requiert d'obtenir le consentement des individus[13] pour agir en-dehors des finalités poursuivies initialement (comme dans le cas du passage d'un traitement de données dans un contexte médical au traitement dans un contexte administratif ou policier ; voy. *infra*).

SECTION 2. – Protection de la vie privée et interception d'informations privées. La vie privée comme rempart contre une société de surveillance

5. Tout comme les personnes sont en droit de veiller aux informations qu'elles acceptent de divulguer, elles sont protégées contre les interceptions

[10] Comme dans le cas de l'affaire *Delfi*, du nom de l'un des plus grands portails d'actualités sur Internet d'Estonie sur lequel les articles publiés suscitent chaque jour quelque 10.000 commentaires (Cour eur. D.H. [GC], 16 juin 2005, arrêt *Delfi c. Estonie*, req. n° 64569/09, §§ 11 et 12).

[11] Cour eur. D.H., 10 mai 2011, arrêt *Mosley c. Royaume Uni*, req. n° 48009/08.

[12] Cour eur. D.H., arrêt *Avilkina c. Russie*, précité, § 48.

[13] Ou de pouvoir s'appuyer sur une norme légale qui l'autorise (voy. art. 6.4 du Règlement général pour la protection des données).

de leurs informations, que ces interceptions soient le fait des autorités publiques[14] ou d'acteurs du secteur privé, comme un employeur[15].

De longue date, les citoyens ont été protégés contre les interceptions de leur courrier par le principe du « secret des lettres »[16], bientôt modernisé en « respect de la correspondance »[17] pour devenir aujourd'hui le « respect » ou la « confidentialité des communications »[18].

6. C'est dans un premier temps contre les agissements des autorités publiques que l'on veut garantir la confidentialité des échanges entre individus. Les interceptions ne sont admises qu'au prix de strictes conditions protégeant la société contre les dérives de la surveillance étatique.[19]

Tant la jurisprudence[20] que les textes légaux[21] européens ont clarifié que la confidentialité doit porter sur le contenu des messages échangés

[14] Parmi de nombreux arrêts, voy. Cour eur. D.H. [GC], 2 août 1984, arrêt *Malone c. Royaume Uni*, req. n° 86/91/79.

[15] Voy. not. Cour eur. D.H., 3 avril 2007, arrêt *Copland c. Royaume Uni*, req. n° 62617/00.

[16] Voy. not. art. 29 Const.

[17] Not. art. 8 CEDH.

[18] Not. art. 7 de la Charte des Droits fondamentaux de l'Union européenne ; art. 5 de la Directive 2002/58 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), *J.O.U.E.*, L 201 du 31 juillet 2002.

[19] Cour eur. D.H. [GC], 2 août 1984, arrêt *Malone c. Royaume Uni*, req. n° 86/91/79 ; 16 février 2000, arrêt *Amann c. Suisse*, req. n° 27798/95.

[20] Cour eur. D.H., 25 septembre 2001, arrêt *P.G. ET J.H. c. Royaume-Uni*, req. n° 44787/98, § 42 ; C.J.U.E. [GC], 8 avril 2014, *Digital Right Ireland*, aff. jointes C-293/12 et C-594/12. La CJUE a relevé que les données relatives au trafic et à la localisation visées par la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications (*J.O.*, L 105, p. 54) étaient susceptibles de permettre de tirer des conclusions très précises sur la vie privée des personnes dont les données avaient été conservées. Voy. égal. Cour eur. D.H., 20 octobre 2015, arrêt *Sher et autres c. Royaume Uni*, req. n° 5201/11, spécial. § 170 : « Les observations du tiers intervenant, Privacy International, portent essentiellement sur la perquisition d'appareils électroniques, pratique qui implique l'accès aux données personnelles et aux données de communication. Le tiers intervenant explique que les innovations technologiques offrent des possibilités de collecte, de stockage, de partage et d'analyse de données inimaginables auparavant. Selon lui, le contrôle par les forces de l'ordre des appareils électroniques d'un individu leur permet d'accéder à toutes les traces numériques laissées par celui-ci à quelque moment que ce soit, y compris les informations qui ne sont pas stockées sur ces appareils eux-mêmes mais sur des serveurs informatiques distants interconnectés. Le croisement de ces données serait extrêmement révélateur. La perquisition d'appareils électroniques revêtirait un caractère particulièrement intrusif, ce qui commanderait la fixation d'un seuil élevé d'exigence pour l'appréciation de la justification d'une atteinte aux droits protégés par l'article 8 ».

[21] L'article 5.1 de la directive 2002/58, précitée, prescrit la confidentialité des communications ainsi que la confidentialité des données relatives au trafic y afférentes, càd toutes les données traitées en vue de l'acheminement d'une communication ou de sa facturation.

mais également sur les données de communication (nom de l'émetteur, du destinataire, moment de la communication, durée, numéro appelé ou, dans le cadre de communication via Internet, adresse IP, etc.). Cette dernière catégorie de données a toutefois été pendant huit ans la cible d'une obligation de conservation systématique instaurée par la directive européenne 2006/24 du 15 mars 2006 et pesant sur les fournisseurs de services de communications électroniques accessibles au public et les fournisseurs de réseau public de communications[22]. Cette obligation visait à garantir la disponibilité de ces données de communication au bénéfice des autorités publiques afin de leur permettre de mener des investigations en vue de la détection et de la poursuite d'infractions graves. La Cour de Justice de l'Union européenne a estimé que, si l'ingérence répondait bien à un objectif d'intérêt général, à savoir contribuer à la lutte contre les infractions graves et le terrorisme, elle ne satisfaisait cependant pas à l'exigence de proportionnalité. Pour la Cour de Justice, la directive entraînait une ingérence d'une trop vaste ampleur et d'une gravité particulière dans les droits fondamentaux à la vie privée et à la protection des données personnelles consacrés par les articles 7 et 8 de la Charte des droits fondamentaux de l'UE, sans que des garanties encadrent une telle ingérence, assurant que celle-ci demeure limitée au strict nécessaire. La Cour a en conséquence invalidé la directive 2006/24 dans un arrêt retentissant[23]. Elle confirmera sa condamnation de la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation dans son arrêt *Tele2 Sverige* du 21 décembre 2016[24] tout en reconnaissant aux États le droit de prévoir, à titre préventif, une conservation ciblée de ces données pour lutter contre la criminalité grave, à condition qu'une telle conservation soit limitée au strict nécessaire[25].

7. Il y a un certain paradoxe à confronter cette analyse de la Cour qui relève très justement le caractère disproportionné de l'obligation de conservation systématique et massive des données de trafic et de localisation[26], soit les données encadrant les communications et non le contenu des communications lui-même, avec la pratique actuelle des acteurs privés

[22] Art. 3 de la directive 2006/24/CE, précitée.

[23] C.J.U.E. [GC], 8 avril 2014, *Digital Right Ireland*, aff. jointes C-293/12 et C-594/12, pts 69 et 71.

[24] C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsenet Secretary of State for the Home Department/Tom Watson e.a*, aff. jointes C-698/15 et C-203/15.

[25] Ce qui fera dire à E. Wery : « Le moins que l'on puisse dire, c'est que la Cour a de la suite dans les idées. Elle a placé la protection des données personnelles au panthéon des valeurs défendues par le droit de l'Union, et elle ne semble pas prête à modifier ce hit-parade » (https://www.droit-technologie.org/actualites/etats-ne-peuvent-imposer-obligation-generale-de-conservation-de-donnees/).

[26] Voy. égal. dans le même sens Cour eur. D.H., 12 janvier 2016, arrêt *Szabo et Vissy c. Hongrie*.

de messagerie tels Messenger, Instagram, WhatsApp, Wechat ou Skype. Ces derniers conservent les messages échangés – tant les données de communication que le contenu[27] – et les traces de toute activité recourant à leurs services[28]. Les informations recueillies par ces acteurs leur servent à réaliser et alimenter le profilage de leurs clients et des personnes en lien avec ceux-ci. L'exploitation commerciale des profils très fins obtenus et sans cesse actualisés est la base de la rentabilité économique des services offerts gratuitement.

Il est à noter que le profilage, qui servait surtout initialement à orienter les opérations de marketing et réduisait les personnes concernées à leur dimension de consommateurs, a désormais également un impact politique et porte atteinte au droit à l'information. La pratique a montré que le profilage peut conduire à sélectionner les informations véhiculées jusqu'aux personnes concernées et avoir une influence manifeste et préoccupante sur des campagnes électorales et lors de référendums.

8. Enfin, la protection contre la surveillance des individus à travers leurs communications s'étend au lieu du travail[29]. C'est principalement la protection contre les agissements de l'employeur qui est ici en cause. Il est désormais loin le temps où l'on disait que la vie privée s'arrêtait à la porte de l'entreprise ou du bureau. Considéré avec sa casquette d'employé ou de salarié, l'individu jouit de la même protection que contre les opérations de surveillance réalisées par les autorités publiques. Ce droit à la protection de la vie privée dans les relations de travail et sur le lieu de travail a été énoncé à plusieurs reprises par la Cour européenne des droits

[27] WhatsApp signale toutefois que s'ils conservent bien une série de données entourant l'utilisation de leurs services, ils ne conservent normalement pas les messages échangés. Ceux-ci sont stockés sur les terminaux des utilisateurs : « Nous ne conservons pas vos messages durant la prestation de nos Services en temps normal. Une fois que vos messages (y compris vos discussions, photos, vidéos, messages vocaux, fichiers et informations de partage de la position) sont transmis, ils sont supprimés de nos serveurs. Vos messages sont stockés dans votre propre appareil. Si un message ne peut pas être transmis immédiatement (par exemple si vous êtes hors ligne), nous le conservons sur nos serveurs pendant 30 jours au maximum pour essayer de le transmettre. Si un message n'est toujours pas transmis après 30 jours, nous le supprimons » (https://www.whatsapp.com/legal/#privacy-policy-information-we-collect).

[28] Voy. par exemple la « Politique d'utilisation des données » de Facebook, à l'adresse https://www.facebook.com/policy.php et la « Politique de confidentialité » d'Instagram à l'adresse https://help.instagram.com/155833707900388.

[29] On n'évoquera pas ici la protection contre la prise d'images et de sons par les caméras de surveillance. Voy. parmi une jurisprudence abondante le tout récent arrêt de la Cour européenne des droits de l'homme : 9 janvier 2018, arrêt *Lopez-Ribalda c. Espagne*, req. n° 1874/13.

de l'homme[30]. Le récent arrêt *Barbulescu* prononcé en Grande Chambre[31] l'a mis remarquablement en lumière, en en dessinant précisément les contours. Ainsi, la Cour a établi les critères à appliquer pour apprécier la légalité ou non d'une mesure de surveillance par l'employeur de la correspondance électronique des salariés. Ces critères portent sur l'information préalable des travailleurs quant à l'existence et à la nature de la surveillance, sur l'étendue de la surveillance effectuée (accès aux contenus ou aux seules données de communication), sur la justification des mesures de surveillance, sur la possibilité de mesures alternatives moins attentatoires, sur les conséquences de la surveillance pour l'employé et si ce dernier a bénéficié de garanties adéquates.

SECTION 3. – La maîtrise des données à caractère personnel. La vie privée comme régulateur d'une société de l'information

9. Avec l'expansion des technologies de l'information et de la communication, de nouveaux défis ne cessent de naitre pour la vie privée. Les ordinateurs, et par la suite les puces, les réseaux et les objets connectés, ont donné une amplitude inquiétante à une pratique qui leur est bien antérieure : le traitement des données sur les individus. Données recueillies à l'insu des personnes, données réutilisées pour des finalités inavouées, données conservées des mois voire des années, données transmises à des tiers, données confidentielles diffusées : la réalité concernant le sort des données à caractère personnel dans l'environnement numérique d'aujourd'hui a bien des faces noires. Les individus faisant usage du réseau et de toute la variété de services en ligne existant désormais, que ce soit par le biais d'un ordinateur, d'un téléphone portable (*smartphone*) d'une tablette ou d'une montre, perdent dans une grande mesure la maîtrise de leurs données. Ils ne savent pas ce qui est fait de leurs données, ils ne peuvent contrôler à distance qui y accède. Une série d'acteurs de l'internet et des nouveaux médias, par contre, connaissent leurs goûts, leurs centres d'intérêt, leurs mouvements, les endroits et les personnes qu'ils fréquentent,…

[30] Voy. par exemple Cour eur. D.H., 28 novembre 2017, arrêt *Antovic et Mirkovic c. Montenegro.*

[31] Cour eur. D.H. [GC], 5 septembre 2017, arrêt *Barbulescu c. Roumanie*, req. n° 61496/08.

C'est dans ce contexte que la notion de vie privée a été amenée à évoluer pour intégrer désormais la maîtrise par chacun des informations qui le concernent en propre[32]. C'est donc la vie privée comme faculté d'autonomie[33] qui est mise en exergue, et plus précisément d'autodétermination informationnelle[34], c'est-à-dire le droit pour l'individu de « savoir ce qui se sait sur lui », de connaître les données le concernant qui sont détenues par d'autres, d'en maîtriser les circuits de communication, d'en contrecarrer les utilisations abusives. La vie privée ne se réduit donc pas à une quête de confidentialité, c'est la maîtrise par chacun de son image informationnelle. La maîtrise ne s'exerce pas seulement sur les informations « porteuses de vie privée », informations qui s'identifient elles-mêmes à la vie privée[35] ; elle s'étend à toute donnée se rapportant à un individu identifié ou identifiable. Par ailleurs, « maîtriser » ne signifie pas nécessairement choisir et déterminer ce qui est communiqué à autrui. Il s'agit surtout d'avoir accès aux données conservées et/ou utilisées par d'autres et d'avoir connaissance du sort réservé à ces données.

---

[32] Voy. F. Rigaux, « Protection de la vie privée : questions d'actualités », *op. cit*., pp. 588-589, n° 532 : « (…) La juridiction constitutionnelle a déduit du droit de la personnalité l'un de ses attributs, à savoir : « le pouvoir reconnu à l'individu et résultant de la notion d'autodétermination, de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués (…) Cet attribut du droit de la personnalité est appelé « droit à la maîtrise des données personnelles » (…) Il n'est toutefois pas sans limite. (…) ». Voy. égal. Cour eur. D. H., 26 mars 1987, arrêt *Leander c. Suède*, *Publ. Cour,* série A, n° 116 ; Cour eur. D.H. [GC], 4 décembre 2008, arrêt S. et *Marper c. Royaume Uni,* req. n° 30562/04 et 30566/04.

[33] Pour la reconnaissance explicite d'un droit à l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'article 8 CEDH, voy. Cour eur. D.H., 7 mars 2006, *Evans c. Royaume-Uni*, req. n° 6339/05 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007) ; 20 mars 2007, *Tysiac c. Pologne*, req. n° 5410/03 ; 1er juillet 2008, *Daroczy c. Hongrie*, req. n° 44378/05.

[34] Voy. H. Burkert, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *Droit de l'Informatique et des Télécoms*, 1985, 8-16 ; E. Degrave et A. Lachapelle, « Le droit d'accès du contribuable à ses données à caractère personnel et la lutte contre la fraude fiscale », note sous C. const., 27 mars 2014, *R.G.C.F.*, 2014, p. 325 ; C. de Terwangne, « La difficile application de la législation de protection des données à caractère personnel », *J.T.*, 2017, p. 752 ; A. Rouvroy et Y. Poullet, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie », in *État de droit et virtualité* (K. Benyekhlef, P. Trudel (eds)), Montréal, Thémis, 2009, pp. 157-222, disponible à l'adresse http://www.crid.be/pdf/public/6050.pdf.

[35] …Même si la maîtrise s'exerce bien sûr également sur de telles informations : voy. l'arrêt de la Cour européenne des droits de l'homme rendu dans l'affaire *Gaskin* mettant en cause un orphelin britannique souhaitant avoir accès au dossier conservé par l'administration sur ses années d'enfance et d'adolescence passées sous la tutelle de l'Assistance publique (Cour eur. D. H., 7 juillet 1989, arrêt *Gaskin c. Royaume-Uni*, *R.U.D.H.*, 1989, pp. 230 et s. ; *Rev. trim. D.H.*, 1990/4, pp. 353 et s., note P. Lambert).

C'est en ce sens que l'Assemblée parlementaire du Conseil de l'Europe a veillé à compléter sa Résolution 428 (1970). En effet, le droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des Droits de l'Homme avait été défini par l'Assemblée en janvier 1970 dans sa « Déclaration sur les moyens de communication de masse et les droits de l'homme » contenue dans cette Résolution comme « le droit de mener sa vie comme on l'entend avec un minimum d'ingérence ». Près de trente ans après l'adoption initiale de ce texte, l'Assemblée parlementaire a précisé que « Pour tenir compte de l'apparition des nouvelles technologies de la communication permettant de stocker et d'utiliser des données personnelles, il convient d'ajouter à cette définition *le droit de contrôler ses propres données* »[36].

Le droit à la protection des données tient compte, d'une part, des déséquilibres de pouvoirs entre la personne concernée et celui qui traite les données, déséquilibres engendrés par les capacités de traitement des données à disposition de ce dernier et dramatiquement exacerbés aujourd'hui du fait des développements techniques, et, d'autre part, de l'impact que les traitements de données peuvent avoir sur les divers droits et libertés des individus. D'autres droits et libertés entrent en effet en ligne de compte, tels la liberté de se déplacer (traitement de données de géolocalisation), la liberté d'association (fichiers des membres de groupes et d'associations), la liberté de s'informer et de s'exprimer en toute transparence (ne pas voir les informations filtrées en fonction de profils préétablis), le droit de pétition, de se loger, de trouver un emploi, le droit à la non-discrimination, etc. « Ainsi, pour parler de la liberté d'expression et de la liberté d'association, comment imaginer que celles-ci puissent survivre si la personne se sait surveillée dans ses communications et ne peut à certains moments s'exprimer anonymement si la technologie garde systématiquement trace de ses messages ? La liberté de s'informer suppose que l'information ne soit pas filtrée, que l'on ne soit pas conduit, profilage aidant, à son insu ou malgré soi, vers l'information qu'autrui souhaite nous voir consommer. Pire, la même technique de profilage peut amener l'auteur du profilage à priver de certains services ou informations un consommateur pour lequel il estime qu'il est peu rentable de l'autoriser à y avoir accès »[37].

10. La jurisprudence et le législateur se sont conjugués pour donner forme à la protection de la maitrise par les individus de leurs données

[36] Rés. 1165(1998) de l'Assemblée parlementaire du Conseil de l'Europe sur le droit au respect de la vie privée, adoptée le 26 juin 1998 (c'est nous qui soulignons).

[37] Y. Poullet, J.-M. Dinant, C. de Terwangne et M.-V. Perez-Asinari, *L'autodétermination informationnelle à l'ère de l'Internet*, Rapport pour le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

à caractère personnel. Ainsi, le Conseil de l'Europe a élaboré, dès 1981, la Convention n° 108[38], tandis que l'Union européenne s'est dotée de l'article 8 de la Charte des droits fondamentaux[39], précédé d'une consécration de la protection des données dans la directive européenne 95/46/CE[40], texte remplacé par le règlement général sur la protection des données (RGPD)[41]. En ce qui concerne la Belgique c'est par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel, revue en 1998[42], que la protection est assurée jusqu'à l'entrée en application dudit règlement.[43]

---

[38] Convention n° 108 du Conseil de l'Europe du 28 janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Cette Convention a fait l'objet d'un travail de modernisation ayant abouti en 2016 à un texte renouvelé, encore en attente d'adoption officielle par le Comité des Ministres du Conseil de l'Europe : texte consolidé des propositions de modernisation de la Convention 108 finalisées par le CAHDATA (réunion des 15-16 juin 2016), https://rm.coe.int/16806b6f7b. Sur ce texte, voy. C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, pp. 81-120.

[39] La Charte des droits fondamentaux de l'UE distingue explicitement la protection de la vie privée (article 7) et des données à caractère personnel (article 8) : art. 7 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications » ; art. 8 : « 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 de protection des données ».

[40] Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des données à caractère personnel et à la libre circulation de ces données.

[41] 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). Sur ce texte, voy. C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *Journal de droit européen*, 2017, pp. 302-316 ; Y. POULLET, « Le nouveau règlement général européen de la protection des données (en abrégé RGPD) est arrivé », *Tax, Audit and Accountancy*, décembre 2017, n° 57, pp. 6-24, disponible à l'adresse https://www.ibr-ire.be/nl/DocumetsMailings/TAA-57.pdf.

[42] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, modifiée par la loi du 11 décembre 1998. Pour un commentaire de cette loi, voy. Th. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution : la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, pp. 377 et s.

[43] Deux lois sont destinées à apporter des compléments au RGPD : la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018 et une loi encore à l'état d'avant-projet (Avant-projet de loi relatif à la protection des personnes

Cette protection de la maitrise des données se décline en un catalogue de principes et de droits garantissant aux personnes concernées leur information et dès lors leur pouvoir de décision, d'action et de surveillance quant au sort réservé à leurs données. Les principes en question, qui sont développés dans les paragraphes qui suivent, sont : le principe de loyauté, le principe de finalité qui impose de s'en tenir aux finalités annoncées pour traiter les données recueillies, le principe de proportionnalité au nom duquel seules les données nécessaires pour atteindre les objectifs fixés peuvent faire l'objet d'un traitement et le principe de qualité des données[44].

11. L'exigence de loyauté induit que le traitement des données soit réalisé dans la transparence pour les personnes concernées, et sans tromperie. Les traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données[45]. La loyauté du traitement de données ne se limite pas à la collecte, mais doit être garantie à toutes les étapes du traitement. Le Groupe de l'article 29 (groupe des autorités européennes de contrôle de la protection des données)[46] a insisté sur le fait que « l'obligation de traiter les données à caractère personnel conformément au principe de loyauté doit être interprétée strictement lorsqu'un enfant est concerné. Dans la mesure où un enfant n'est pas encore complètement mûr, les responsables du traitement doivent en avoir conscience et agir en toute bonne foi lors du traitement de ses données »[47].

Le principe de loyauté est donc lié au devoir de transparence qui sera exposé dans des développements ultérieurs (voy. *infra* Chapitre 2, Section 1).

---

physiques à l'égard des traitements de données à caractère personnel). Cette dernière réalisera aussi la transposition de la directive 2016/680/UE 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.

[44] Pour une liste complète des principes gouvernant la protection des données sous tous ses aspects, *cf.* art. 5 RGPD.

[45] Cour eur. D.H., 3 avril 2007, arrêt *Copland c. Royaume Uni.*

[46] Groupe de l'article 29, avis 2/2009 du 11 février 2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), *WP* 160 ; document de travail 1/2008 du 18 février 2008 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), *WP* 147.

[47] V. Verbruggen, *Les Codes commentés. La protection des données*, Bruxelles, Larcier, 2011, p. 56.

12. Principe clé de la protection, le **principe de finalité** exige que tout traitement poursuive une ou des finalité(s) déterminée(s), explicite(s) et légitime(s), que l'on ne fasse que ce qui est compatible avec cette (ces) finalité(s)[48], que l'on ne traite que les données pertinentes et non excessives au vu de la (des) finalité(s)[49] et que l'on ne conserve ces données qu'aussi longtemps que cela est nécessaire pour atteindre la finalité du traitement[50]. La spécification de la finalité est fondamentale, car c'est elle qui va déterminer le traitement de données à caractère personnel et permettre à la personne concernée de contrôler le sort réservé aux données la concernant. La finalité doit être précise afin de permettre à la personne concernée d'effectuer cette analyse et d'exercer les droits qui lui sont conférés par la loi.

13. Au nom du **principe de qualité des données**, ces dernières doivent être exactes et, si nécessaire, mises à jour[51].

14. La maitrise des données personnelles implique de pouvoir vérifier le respect de ces principes de protection. L'individu concerné par les données se voit reconnaitre un **droit de rectification** des données incorrectes et un **droit de faire effacer** les données non pertinentes, celles portant excessivement atteinte à ses droits et intérêts, et celles conservées au-delà de la période autorisée. Ce droit à l'effacement est présenté, dans le RGPD[52], comme assimilé au « **droit à l'oubli** », notion qui a fait couler beaucoup d'encre et suscité de nombreux débats[53]. La personne concer-

[48] Pour un cas d'utilisation non compatible des données condamnée par la Cour européenne des droits de l'homme, voy. Cour eur. D.H., arrêt *M.S.c. Suède*,

[49] Cour eur. D.H. [GC], 4 décembre 2008, arrêt S. et *Marper c. Royaume Uni*, req. n° 30562/04 et 30566/04.

[50] Cour eur. D.H., 18 septembre 2014, arrêt *Brunet c. France*.

[51] Pour un cas de jurisprudence, voy. Cour eur. D.H. [GC], arrêt *Rotaru c. Roumanie*, 4 mai 2000. Sur une limitation légitime de ce droit, voy. Cour eur. D.H., 5 décembre 2017, déc. *Anchev c. Bulgarie*, req. nos 38334/08 et 68242/16.

[52] Art. 17 RGPD.

[53] Voy. le retentissant arrêt C.J.U.E. [GC], 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* C-131/12. Égal. Cour eur. D.H., 13 novembre 2012, arrêt *M.M. c. Royaume-Uni*, req. n° 24029/07. En doctrine : J. Ausloos, B. Van Alsenoy, « Bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens », *A.&M.*, 2014/5, p. 398 ; C. Bernard-Glanz, « Les arrêts Digital Rights Ireland et Google Spain, ou le printemps européen de la protection des données », *C.D.E.*, 2014/3, pp. 685 à 717 ; A. Cassart, J. Henrotte, « Arrêt Google Spain : la révélation d'un droit à l'effacement plutôt que la création d'un droit à l'oubli », *J.L.M.B.*, 2014 ; E. Cruysmans, A. Strowel, « Un droit à l'oubli face aux moteurs de recherche : droit applicable et responsabilité pour le référencement de données "inadéquates, non pertinentes ou excessives" », *J.T.*, 2014, p. 451 ; E. Defreyne, R. Robert, « L'arrêt "Google Spain" : une clarification

née dispose également le **droit de s'opposer** aux utilisations non compatibles avec la finalité annoncée et aux communications et aux accès non autorisés. Pour pouvoir effectuer ces vérifications, il s'impose de conserver pendant un certain temps des traces des opérations réalisées sur les données[54].

CHAPITRE 2. Droit à la vie privée : un droit à l'information

15. Droit au secret et droit à la maitrise des données, le droit à la vie privée est également un droit à l'information. Ce droit à recevoir l'information prend la forme d'un droit à être informé spontanément des traitements de ses données à caractère personnel et d'avoir accès à ces données (Section 1), d'un droit à recevoir les informations ayant un impact sur la vie privée (Section 2) et d'un droit à l'information dans un contexte procédural (Section 3).

SECTION 1. – Droit d'être informé des traitements de données à caractère personnel et droit d'accès à ces données

16. Les droits liés à l'information de la personne concernée à propos de ses données à caractère personnel lui sont octroyés afin de lui permettre d'exercer pleinement son autodétermination informationnelle. Ils visent à assurer la transparence des traitements de données. Cette transparence,

---

de la responsabilité des moteurs de recherche … aux conséquences encore floues », *R.D.T.I.*, 2014/3, pp. 73 à 114 ; C. DE TERWANGNE, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *Les enjeux européens et mondiaux de la protection des données personnelles,* Bruxelles, Larcier, 2015, pp. 237 à 268 ; D. LINDSAY, « The "Right to be Forgotten" by search Engines under Data Privacy Law : A Legal Analysis of the Costeja Ruling », *Journal of Media Law*, 2014/6, pp. 159 à 179.

[54] Sur le devoir de conserver des traces pour vérifier les accès accordés aux données, voy. Cour eur. D.H., 17 juillet 2008, arrêt *I. c. Finlande,* req. n° 20511/03 ; C.J.U.E., 7 mai 2009, arrêt *Rijkeboer*, C-553-07.

d'initiative ou sur demande, doit permettre à l'individu non seulement d'avoir connaissance, mais aussi de contrôler ce qui est fait avec ses données, de vérifier le respect des règles, de traquer les abus ou les illégalités, de corriger les erreurs.

§ 1. Le droit d'être informé

17. Si ce n'est pas prévu dans les premiers instruments de protection des données comme la Convention 108 du Conseil de l'Europe, un devoir d'information active est mis, dans les textes ultérieurs, à charge des personnes qui traitent des données. Il s'agit d'éclairer les sujets des données de ce qui est fait avec leurs données et par qui. Un premier devoir d'information apparait dans la directive 95/46[55], fortement renforcé dans le RGPD[56]. Ce dernier texte veille par ailleurs à présenter cette exigence d'information sous la forme d'un droit de la personne concernée et non plus d'une obligation du responsable du traitement.

Dans un premier temps, tout responsable de traitement est tenu de fournir des informations sur lui-même et sur son délégué à la protection des données s'il en a un, ainsi que sur la finalité qu'il poursuit en traitant les données, sur les catégories de données traitées, sur la base juridique du traitement et, le cas échéant, les intérêts légitimes liés à ce traitement des données, sur les catégories de destinataires des données et enfin, sur les intentions de transfert des données vers des pays tiers[57]. D'autres informations doivent ensuite être fournies lorsque cela est nécessaire pour garantir un traitement équitable et transparent : la durée de conservation des données, l'existence d'un droit d'accès, de rectification et des autres droits, notamment le droit de retirer son consentement, le caractère obligatoire ou non des réponses ainsi que les conséquences d'un défaut éventuel de réponse et enfin, l'existence d'une décision automatisée ou d'un profilage, accompagnée d'informations concernant la logique sous-jacente.

Pour que ce droit à être informé ne soit pas un leurre, le RGPD exige que les informations à fournir le soient de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant[58]. Il est vrai que sous la directive 95/46, le responsable du traitement devait déjà communiquer aux personnes concernées toute une série

[55] Art. 10 et 11 de la directive 95/46.
[56] Art. 12 à 14 RGPD.
[57] Art. 13, § 1, et 14, § 1, RGPD.
[58] Art. 12, § 1, RGPD.

d'informations mais celles-ci étaient rarement lues en raison notamment de la longueur et de la complexité des documents dans lesquels elles étaient insérées. Le législateur européen tente dès lors dans le RGPD de remédier à ce problème en mettant l'accent sur la transparence et la clarté avec lesquelles les informations doivent être mises à disposition. L'utilisation d'icônes[59], par exemple, devrait permettre de donner d'emblée aux individus une bonne visibilité sur le traitement.

Cette formalité d'information doit être accomplie soit au moment de l'obtention des données, soit au plus tard au moment de la première communication des données, si les données ont été obtenues de manière indirecte.

Le droit à l'information n'est bien sûr pas absolu et une série d'exceptions peuvent intervenir au nom d'intérêts supérieurs comme la poursuite des infractions ou la protection du secret professionnel.

§ 2. Le droit d'accès : Un accès « riche »

18. Le droit d'accès offre à la personne concernée une autre voie pour obtenir des informations sur les traitements effectués sur ses données. À l'inverse du droit d'être informé, cette voie exige une démarche de sa part. Entre la première formulation du droit d'accès dans la Convention 108 et celle contenue dans le RGPD, une remarquable extension de ce droit est apparue. L'accès aujourd'hui ne se réduit plus à la seule connaissance de l'existence d'un fichier, de l'identité de son responsable et des données qu'il contient. L'accès s'exerce à l'égard de ces informations mais est une prérogative bien plus riche désormais.

19. Le droit à la curiosité. Chacun a le droit d'interroger un responsable de traitement pour savoir s'il détient ou non des données sur lui[60]. Le responsable interrogé doit confirmer ou non s'il détient des données à propos de l'individu qui s'est adressé à lui et, si c'est le cas, il doit accorder l'accès auxdites données et fournir les mêmes indications que celles qui doivent être communiquées au titre du droit d'être informé (voy. ci-dessus). Une indication supplémentaire doit être fournie à propos de la source des données, dans les cas où les données n'ont pas été obtenues directement auprès de la personne concernée[61].

[59] Art. 12, § 7, RGPD.
[60] Art. 15 RGPD.
[61] Art. 15, § 1, g), RGPD.

20. L'accès à l'information sur l'origine des données. Cette obligation d'information sur l'origine des données, qui est logiquement d'application lorsque les données n'ont pas été recueillies directement auprès de la personne concernée, est d'un grand intérêt étant donné que c'est souvent la question de la source des informations qui préoccupe les personnes concernées (comment se fait-il que mes informations se retrouvent dans les mains de cet organisme, qui les lui a fournies ?). Avoir connaissance de l'origine des données détenues sur son compte permet à la personne concernée de se rendre compte des filières de communication des données et, le cas échéant, de contester de telles communications (eu égard, par exemple, au caractère incompatible de la communication par rapport à la finalité de collecte des données[62]). Enfin, en cas de problèmes liés à la qualité des données et de nécessité de correction, il devient possible de faire effectuer ces corrections à la source, ce qui évite la propagation ultérieure d'erreurs.

21. Le droit d'être informé des destinataires ou des catégories de destinataires à qui les données sont communiquées soulève la question de la portée dans le temps de ce type d'information. En effet, c'est souvent parce que l'on s'est rendu compte de quelque chose de douteux ou parce que l'on souhaite savoir à quelle source des personnes ont obtenu des informations, que l'on exerce son droit d'accès pour découvrir les personnes à qui les données ont été transmises. L'accès aux données sur les destinataires est aujourd'hui, dans un monde numérisé, lié à la question de l'accès aux *log files* ou journaux d'événements. Ces derniers sont des fichiers qui relèvent un certain nombre de renseignements sur toutes les transactions gérées par le serveur. C'est donc à partir de ces journaux et des traces digitales qu'ils conservent que l'on peut identifier les accès qui se sont produits. L'information sur les destinataires se heurte toutefois directement aux pratiques d'effacement de telles données au terme d'un certain délai.

La Cour de justice de l'Union européenne[63] a affirmé que le sens même du droit d'accès dans toutes ses composantes est de permettre aux individus de prendre connaissance du sort réservé à leurs données et de procéder à des vérifications des opérations effectuées sur elles, afin d'être à même d'exercer leurs autres droits prévus par la directive. En conséquence, pour

[62] Voy. *infra*, l'exigence de respect du principe de finalité.

[63] C.J.C.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, C-553/07. Voy. C. GAYREL, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de Justice de l'Union européenne, Tribunal de Première Instance et Tribunal de la Fonction publique européenne », *R.D.T.I.*, nos 48 et 49, 2012, pp. 95 et 96.

la Cour, il est impératif que l'accès ne soit pas réduit au présent, mais couvre également le passé. Il ne s'agit pas pour autant de permettre de remonter sans limites dans le temps. La fixation d'un délai de conservation légitime varie en fonction de paramètres identifiés par la Cour et doit être tempérée par l'intervention du critère de proportionnalité[64]. L'arrêt *Rijkeboer* présente un enseignement concret pour les responsables de traitement. Ils savent à l'avenir que pèse sur eux l'obligation de veiller à la conservation des traces des communications et accès aux données accordés à des tiers pendant à tout le moins une durée raisonnable, afin de permettre aux personnes concernées d'être informées, à leur demande, de ces transmissions de leurs données et de pouvoir en contrôler la licéité.

22. L'accès à la logique qui sous-tend le traitement des données. Lorsqu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité (attribution d'une prime ou désignation comme bénéficiaire d'un régime particulier de la sécurité sociale, par exemple), cette personne doit pouvoir obtenir du responsable du traitement la connaissance de la logique qui sous-tend le traitement automatisé en question[65]. Le but de ce droit d'accéder à la logique d'un traitement (càd au raisonnement, aux critères appliqués) consiste à permettre aux personnes concernées de contrôler les fondements de décisions automatisées prises à leur encontre, impliquant le traitement de leurs données. Ce droit présente un grand intérêt face au déploiement exponentiel du phénomène de profilage.

23. L'accès aux données traitées elles-mêmes. La personne concernée qui apporte la preuve de son identité a le droit d'obtenir du responsable du traitement la communication, sous une forme claire et intelligible, des données faisant l'objet du traitement[66]. Le responsable du traitement doit fournir gratuitement[67] une copie des données[68]. La Cour européenne des

[64] Voy. les paragraphes 58 et 59 et 63 de l'arrêt et leur commentaire dans C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E, 7 mai 2009, *R.D.T.I.*, 2011, n° 43, pp. 65 à 81.

[65] Art. 15, § 1, h), RGPD.

[66] Art. 15 RGPD.

[67] Art. 12, § 5, RGPD.

[68] Art. 15, § 3, RGPD ; voy. pour l'accès à des copies d'examen : C.J.U.E., 20 décembre 2017, *Novak c. Data protection Commissioner*, aff. C-434/16 ; concernant l'obtention de photocopies de dossiers médicaux, voy. Cour eur. D.H., 27 avril 2009, arrêt *K.H et autres c. Slovaquie*, req. n° 32881/04, § 47 : « Gardant à l'esprit que l'exercice du droit au respect de la vie privée et familiale, consacré par l'article 8, doit être concret et effectif, la Cour

droits de l'homme a précisé que « l'intéressé ne doit pas être contraint de justifier spécifiquement la demande qu'il forme pour recevoir une copie de ces dossiers. C'est plutôt aux autorités qu'il revient de démontrer l'existence de raisons impérieuses de refuser un tel service »[69]. La Cour a aussi relevé l'intérêt que représente le fait d'obtenir une copie des données : « La Cour observe également que les intéressées ont considéré qu'il leur fallait disposer de tous les documents sous forme de photocopies afin qu'un expert indépendant, le cas échéant à l'étranger, puisse les examiner et aussi afin qu'elles puissent se prémunir contre une éventuelle destruction par mégarde des originaux »[70].

C'est l'ensemble des données traitées qui doivent être communiquées, tant les données objectives que les données subjectives (p. ex., un avis, l'évaluation de la solvabilité d'une personne, l'évaluation et les remarques émises par un examinateur[71]).

L'exigence que les données soient communiquées « de façon compréhensible, en des termes clairs et simples »[72] implique que la forme des données doit permettre à un individu ordinaire de saisir la portée de l'information transmise. Ainsi, si un code ou un profil particulier est attribué à la personne concernée (par une banque qui évalue sa valeur de crédit, par exemple, ou à l'issue de tests d'embauche), celle-ci doit être mise en mesure de comprendre la signification du code ou du profil.

SECTION 2. – Droit de recevoir les informations ayant un impact sur la vie privée

24. La jurisprudence a fait émerger une autre dimension du droit à l'information basé sur la protection de la vie privée. L'information dont il s'agit ne consiste plus en données relatives à un individu identifié ou identifiable. Il s'agit d'informations qui, en soi, n'ont aucun *rapport direct* avec la vie privée, mais qui ont un *impact* sur la vie privée. La vie privée est entendue, à ce stade, comme la capacité d'autonomie dans le sens

considère que pareilles obligations positives doivent s'étendre – en particulier dans les affaires qui comme l'espèce portent sur des données à caractère personnel – à la mise à disposition, en faveur de la personne concernée, de copies des dossiers dont elle est l'objet ».

[69] *Ibid.*, § 48.

[70] *Ibid.*, § 51.

[71] C.J.U.E., 20 décembre 2017, *Novak c. Data protection Commissioner*, aff. C-434/16, pts 42 et s.

[72] Art. 12, § 1, RGPD.

de la capacité de déterminer le cours de son existence, autrement dit comme la liberté d'effectuer en toute connaissance de cause des choix de vie (choix du domicile, décisions quant à des mesures de protection,…). Elle implique nécessairement dès lors le droit d'être informé sur les facteurs extérieurs ayant une incidence sur le bien-être et sur la jouissance du domicile ainsi que sur la santé.

L'importance pour une personne de connaitre les circonstances extérieures ayant une influence sur sa santé est particulièrement soulignée par la jurisprudence. Ainsi, la Cour européenne des droits de l'homme a proclamé à plusieurs reprises, et notamment en formation de grande chambre, que la question de l'accès à des informations susceptibles d'apaiser les craintes d'un individu ou de lui permettre d'évaluer le danger auquel il a été exposé, « présente un lien suffisamment étroit avec la vie privée au sens de l'article 8 pour soulever une question sur le terrain de cette disposition »[73].

La Cour a donc établi, à travers plusieurs arrêts basés sur l'article 8 CEDH[74], l'existence d'un véritable droit à l'information, impliquant un devoir corollaire de communication d'informations pour l'État[75].

---

[73] Cour eur. D.H., 9 juin 1998, arrêt *McGinley et Egan c. Royaume-Uni*, *Recueil*, 1998-III, § 97 ; Cour eur. D.H. [GC], 19 octobre 2005, arrêt Roche *c. Royaume-Uni*, req. n° 32555/96, § 162.

[74] Et également de l'article 2 CEDH protégeant le droit à la vie, qui ne fait toutefois pas l'objet de la présente analyse. À l'occasion de l'affaire *Öneryildiz c. Turquie* tranchée le 30 novembre 2004, la Cour affirma : « L'obligation positive de prendre toutes les mesures nécessaires à la protection de la vie au sens de l'article 2 implique avant tout pour les États le devoir primordial de mettre en place un cadre législatif et administratif visant une prévention efficace et dissuadant de mettre en péril le droit à la vie. […] Parmi ces mesures préventives, il convient de souligner l'importance du droit du public à l'information, tel que consacré par la jurisprudence de la Convention. En effet, avec la chambre, la Grande Chambre convient que ce droit, qui a déjà été consacré sur le terrain de l'article 8 (*Guerra et autres*, § 60), peut également en principe être revendiqué aux fins de la protection du droit à la vie ».

[75] Après avoir refusé de rattacher un tel devoir d'information à l'article 10 CEDH, garantissant pourtant le « droit de recevoir des informations » (voy. C. DE TERWANGNE, « La Convention européenne des droits de l'homme et le droit de recevoir des informations de la part des autorités publiques », *Amén.*, 1998/4, pp. 265-270 ; J.-P. MARGUENAUD, « L'incidence de la Convention européenne des droits de l'homme sur le droit de l'environnement », *J.T. dr. eur.*, 1998, pp. 220 et s.), la Cour a fait évoluer sa jurisprudence. Dans ses arrêts *Társaság a Szabadságjogokért c. Hongrie* et *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes c. Autriche*, la Cour a relevé qu'elle s'orientait vers une interprétation plus large de la notion de « liberté de recevoir des informations », englobant la reconnaissance d'un droit d'accès à l'information (14 avril 2009, arrêt *Társaság a Szabadságjogokért c. Hongrie,* req. n° 37374/05, § 35 ; 28 novembre 2013, arrêt *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes c. Autriche,* req. n° 39534/07, § 41).

C'est à l'occasion de l'affaire *Guerra*[76], que la Cour a, de façon novatrice et hardie, proclamé l'obligation pour les autorités (italiennes en l'occurrence) de porter à la connaissance des personnes concernées les informations essentielles sur ce qui pourrait affecter le droit au respect de leur vie privée et familiale. Elle en a déduit en l'occurrence un devoir de communication d'informations sur les risques d'atteinte à l'environnement. La position de la Cour est remarquable car non seulement elle a raisonné en amont d'une atteinte réelle (elle évoque le *risque* d'atteinte), mais les mesures de protection qu'elle envisage ne correspondent pas vraiment à ce que l'on aurait classiquement imaginé pour protéger la population. Ainsi, l'État n'est pas appelé en l'espèce à minimiser les risques encourus par la population voisine de l'usine en agissant sur l'origine de ces risques. La Cour se place sur un autre plan et érige la transparence en instrument de protection de la vie privée des personnes. Veiller à la protection de la vie privée revient donc, notamment, à informer de façon adéquate les personnes concernées sur ce qui *pourrait* avoir, et, *a fortiori*, ce qui a, un impact grave sur leur vie privée et familiale.[77] La Cour est en outre allée très loin dans sa définition des obligations positives pesant sur l'État puisqu'elle a condamné l'État italien pour n'avoir pas collecté les informations nécessaires et diffusé spontanément celles-ci auprès de la population en cause.

Quelques mois plus tard, dans son arrêt *McGinley et Egan*[78], la Cour a confirmé cette position jurisprudentielle en déclarant que l'article 8 impose à l'État de mettre en place une procédure effective et accessible permettant d'obtenir communication de l'ensemble des informations pertinentes et appropriées concernant les risques pour la santé engendrés par une activité de l'État. Les informations au centre des débats étaient de deux ordres : des informations d'ordre personnel (informations sur l'état de santé des deux requérants et leur suivi médical) et des informations techniques et scientifiques (notamment les mesures des retombées radioactives sur le sol de l'île, l'air et l'eau de mer). La Cour n'a pas scindé son argumentation en fonction de la nature personnelle ou non des informations mais a considéré l'effet réducteur d'angoisse, voire éclairant sur l'étendue des risques encourus, que les informations visées, dans leur ensemble, pouvaient avoir

[76] Cour eur. D.H., 19 février 1998, arrêt *Guerra et autres c. Italie*, § 60.

[77] La Convention d'Aarhus du 25 juin 1998 sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement prévoit en son article premier une disposition allant dans le même sens que l'affirmation de la Cour européenne. Cet article stipule : « Afin de contribuer à protéger le droit de chacun […] de vivre dans un environnement propre à assurer sa santé et son bien-être, chaque Partie garantir le[s] droit[s] d'accès à l'information sur l'environnement, […] ».

[78] Cour eur. D.H., 9 juin 1998, arrêt *McGinley et Egan c. Royaume-Uni*, *Recueil*, 1998-III, p. 1362, § 97 et p. 1363, § 101.

pour les requérants. Ce n'est donc pas parce que l'information touchait à un élément de la vie privée que la Cour estima qu'elle devait être communiquée. La Cour fut d'avis que l'article 8 entrait en jeu parce que livrer des individus au doute quant à leur exposition à des niveaux nocifs de rayonnement, et dès lors générer chez ces personnes une anxiété, est attentatoire à leur droit au respect de la vie privée.

En s'appuyant sur ces deux affaires, la Cour soulignera encore, en se prononçant toujours dans le cadre de l'article 8, l'importance de l'accès du public aux informations relatives aux effets des activités qui peuvent porter atteinte à l'environnement et aux droits des individus, ainsi que de l'accès aux informations permettant d'évaluer le danger auquel le public est exposé[79].

Enfin, c'est en composition de grande chambre que la Cour a réitéré sa position, confirmant encore, dans son arrêt *Roche*[80], l'exigence de la mise en place par l'État d'une procédure effective et accessible qui permette aux citoyens d'avoir accès à l'ensemble des informations pertinentes et appropriées leur permettant d'évaluer tout risque auquel ils ont pu être exposés. La Cour a précisé à cette occasion que l'obligation positive de communiquer des informations à un individu ne saurait être satisfaite par le renvoi vers une action en justice à laquelle est associée la divulgation d'informations. L'obligation positive de communication en question n'exige pas de l'intéressé que pour obtenir satisfaction il engage une procédure[81].

En conclusion, de la jurisprudence développée par la Cour se dégage l'obligation de mise à disposition des informations dont la connaissance concourt à assurer la jouissance du droit à la vie privée. En filigrane des arrêts de la Cour, un devoir d'information est mis à charge des États en matière de sécurité, de santé et d'environnement.

SECTION 3. – Exigence procédurale inhérente à la protection de la vie privée et communication d'informations

25. La Cour européenne des droits de l'homme a également, dans un contexte tout autre, tiré des conclusions en termes de devoir de communication d'informations sur la base de l'article 8 de la Convention.

---

[79] Cour eur. D.H., 10 novembre 2004, arrêt *Taskin et autres c. Turquie*, § 119.
[80] Cour eur. D.H. [GC], 19 octobre 2005, arrêt Roche *c. Royaume-Uni*, req. n° 32555/96, § 162.
[81] *Ibid.*, § 165.

Elle a affirmé[82] que, si l'article 8 ne renferme aucune condition explicite de procédure, un processus décisionnel débouchant sur des mesures d'ingérence doit toutefois respecter les intérêts protégés par l'article 8.

À l'occasion de l'affaire *McMichael* dans laquelle une instance devait décider de l'adoptabilité d'un enfant placé en foyer d'accueil, la Cour estima que ne pas permettre aux requérants-parents de consulter certains documents examinés par l'instance de décision (quand bien même celle-ci leur aurait révélé oralement la teneur de ces documents), revient à méconnaître l'article 8.

À côté de l'exigence contenue à l'article 6, § 1er, de la Convention qui garantit le droit à un procès équitable, la Cour a reconnu, sur la base de l'article 8, une condition de procédure autonome car directement liée à la vie privée et familiale. Afin d'accorder aux intérêts des personnes la protection voulue par l'article 8, il s'impose donc, dans un processus décisionnel ayant des répercussions sur la vie privée ou familiale, de communiquer à ces personnes les documents confiés à l'instance de décision, sans se contenter de révéler oralement la teneur des documents en question.

26. Cette décision pourrait avoir des répercussions sur les conditions dans lesquelles, dans les ordres juridiques internes des États signataires de la Convention, sont prises certaines décisions mettant en cause la vie privée et familiale. Par exemple, les autorités prenant des décisions concernant l'octroi du statut de réfugié, les demandes de regroupement familial, l'expulsion hors du territoire, devraient, pour se conformer à l'article 8 de la Convention, communiquer aux personnes requérantes les documents sur lesquels elles s'appuient pour rendre leurs décisions. Des exceptions pourraient sans doute être admises, mais seulement dans la mesure où elles répondraient aux conditions énoncées au paragraphe 2 de l'article 8 de la Convention.

Conclusion

27. Le rapport de la vie privée à l'information se présente sous diverses facettes.

28. Le droit à la vie privée correspond tout d'abord à un droit sur l'information – droit au secret et droit à la maitrise de ses données.

---

[82] Cour eur. D.H., 16 février 2016, arrêt *Soares de Melo c. Portugal*, req. n° 72850/14, § 65 ; 24 février 1995, arrêt *McMichael c. Royaume-Uni, Publ. Cour,* série A, n° 307-B, §§ 85 à 93 ; 26 février 2002, arrêt *Kutzner c. Germany*, req. n° 46544/99.

Traditionnellement, la protection du droit à la vie privée est le moyen de se prémunir contre la curiosité et l'indiscrétion d'autrui. L'information qui est en cause dans cette hypothèse est intrinsèquement liée à la vie privée et la divulgation de cette information réalise l'atteinte à la vie privée. Le droit au secret permet à l'individu d'exercer son droit sur l'information, de choisir ce qu'il accepte de divulguer et de faire sanctionner les révélations non consenties.

Dans une société de surveillance telle la nôtre, où les interceptions des échanges entre individus sont facilitées par les technologies et sont le fait tant des autorités publiques que des acteurs privés, le droit à la vie privée s'élève comme un rempart contre les dérives. Il garantit la confidentialité des communications sous toutes leurs formes.

Dans la société de l'information qui est en place depuis plusieurs décennies maintenant, le droit à la vie privée a induit la protection de la maîtrise des données à caractère personnel. La vie privée, dans son aspect de protection des données, est l'élément-clef de l'équilibre d'une telle société de l'information. Le droit à la maitrise des données personnelles s'érige comme correctif à la disproportion des pouvoirs dérivés de la mainmise sur les informations.

29. Droit *sur* l'information, le droit à la vie privée correspond également à un droit *à* l'information. Désormais, la communication d'informations est un élément du respect de la vie privée. Un véritable droit à l'information est reconnu aux individus.

Ce droit s'exerce dans un premier temps à l'égard des données relatives à la personne concernée. Il prend la forme d'un droit à recevoir des informations concernant le sort réservé à ses données sans avoir à effectuer de démarche. C'est l'instrument de la lutte contre l'opacité des traitements de données. Ce droit à l'information implique aussi le droit d'accès par chacun aux données à caractère personnel le concernant traitées par autrui. Tel qu'il est consacré par les textes européens, la directive 95/46 mais surtout le règlement général sur la protection des données, ce droit d'accès est particulièrement riche et permet de se voir communiquer la copie des données elles-mêmes mais également une série d'informations accessoires singulièrement éclairantes.

Par ailleurs, la protection de la vie privée peut également s'effectuer par la mise à disposition d'informations qui n'ont pas trait à la vie privée mais qui ont une incidence sur elle. La jurisprudence a mis en exergue une obligation d'informer les individus sur les facteurs extérieurs ayant une incidence sur leur bien-être et sur la jouissance de leur domicile ainsi que sur leur santé. Elle en a déduit un devoir de communication d'informations

sur les risques pour la sécurité et la santé des personnes et sur les risques d'atteinte à l'environnement.

Enfin, le respect de la vie privée exige aussi la communication des informations intervenant dans un processus décisionnel ayant des répercussions sur la vie privée.