La protection des données "sensibles "à l'ère du numérique : Regard sur le droit de l'Union européenne

Sophie Gambardella

Une version a été publiée dans l'ouvrage suivant : Taleb-Karlsson (A.) De David Beauregard-Berthier (0.), *Protection des données personnelles et sécurité nationale. Quelles garanties juridiques dans l'utilisation du numérique ?*, Bruxelles, Bruylant, coll. « A la croisée des droits », 2017, pp. 63-88.

LA PROTECTION DES DONNEES « SENSIBLES » A L'ERE DU NUMERIQUE : REGARD SUR LE DROIT DE L'UNION EUROPEENNE

Sophie GAMBARDELLA
Docteur en droit
CERIC – UMR DICE 7318, Faculté de droit d'Aix-Marseille Université

Dans son rapport de 2014 relatif au numérique et aux droits fondamentaux, le Conseil d'Etat ouvre ses propos de la sorte : « Envisager la manière dont le numérique affecte les droits fondamentaux, c'est déjà postuler son importance et sa spécificité par rapport à d'autres mutations technologiques »[1]. Cette affirmation est porteuse d'une idée forte lorsque nous abordons la question de la protection de la vie privée à l'ère du numérique. Le Conseil d'Etat prend, en effet, le soin de parler de « mutations technologiques » plutôt que d'« avancées technologiques », comme pour nous mettre en garde sur le fait que cette révolution, dans le domaine des droits de l'Homme, peut-être porteuse d'un certain nombre de dangers que nous devons considérer. Par ses mots, le Conseil d'Etat nous renvoie ainsi à cette modernité dans laquelle nous vivons, baptisée par Ulrich Beck de « modernité réflexive »[2], où les risques engendrés par les évolutions techniques doivent nous obliger à repenser ces mutations afin de minimiser les atteintes, notamment aux droits fondamentaux. La question de la protection des données à caractère personnel est aujourd'hui au cœur de ce type de réflexion tant la protection de la vie privée est en tension avec la volonté d'accroître l'accessibilité de tout un chacun à tout type de données, même à caractère personnel.

Au sein de l'Union européenne, la refonte du régime juridique de protection des données à caractère personnel, engagée depuis 2012[3], avait pour objectif de trouver un juste équilibre au cœur de cette tension entre intérêts divergents. La nécessité d'assurer la protection du droit fondamental de tout individu au respect de sa vie privée a conduit très tôt, à l'échelle européenne, à la mise en place d'un régime juridique de protection des données à caractère personnel à travers notamment la directive 95/46/CE[4], qui est encore aujourd'hui la clé de voûte de la législation de l'Union européenne en la matière[5]. La prise de conscience de l'évolution des modes de traitement des données et l'adoption de la Charte des droits fondamentaux de l'Union européenne qui proclame, en son article 8, le droit de toute personne à la protection de ses données à caractère personnel ont impulsé, en 2012, une proposition de la Commission de règlement général sur la protection des données. Le 14 avril 2016, le Parlement européen a adopté, après quatre années de négociations, le nouveau

[1] Etude annuelle 2014 du Conseil d'Etat, *Le numérique et les droits fondamentaux*, La Documentation Française, collection Etudes et documents du Conseil d'Etat, septembre 2014, p. 41.
[2] U. BECK, *La société du risque. Sur la voie d'une autre modernité*, trad. de l'allemand par L. Bernardi, Paris, Aubier, 2001, p. 335.
[3] Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), COM/2012/011 final - 2012/0011 (COD).
[4] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Journal officiel des Communautés européennes n° L 281* du 23 novembre 1995, pp. 0031-0050.
[5] Pour une étude théorique globale de la protection des données à caractère personnel dans l'Union européenne voir : L. COUDRAY, *La protection des données personnelles dans l'Union européenne : Naissance et consécration d'un droit fondamental*, Editions universitaires européennes, 2010, 693 p.

règlement général sur la protection des données[6]. Le règlement sera applicable à partir de mai 2018. A l'heure actuelle, les réflexions doctrinales sur la protection des données à caractère personnel ne peuvent donc pas faire abstraction du nouveau règlement même si la directive de 1995 reste encore, pour deux ans, le texte juridique de référence dans ce domaine[7]. De plus, en parallèle, a été négociée une directive 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[8]. Cette directive a été adoptée en même temps que le règlement général sur la protection des données. Le droit de l'Union européenne en matière de protection des données à caractère personnel est donc, en cette année 2016, un droit en pleine évolution. C'est dans ce contexte mouvant que nous voudrions à travers cette contribution engager une réflexion sur la protection des données sensibles à l'ère du numérique.

La catégorie juridique des données à caractère personnel, apparaît dans les années 80 et englobe, selon les termes de la directive 95/46/CE, « toute information concernant une personne physique identifiée ou identifiable (personne concernée) » de manière directe ou indirecte[9]. Les données qui répondent à cette définition bénéficient alors d'une protection juridique soutenue en ce qui concerne leur collecte, leur traitement et leur échange. Le nouveau règlement général sur le protection des données reprend mot pour mot cette définition. Au sein de la catégorie des données à caractère personnel, l'article 8 de la directive 95/46/CE et l'article 9 du nouveau règlement invitent, de surcroît, à identifier une sous-catégorie de données : les données dites « particulières » ou « sensibles » dont la protection juridique devrait, de fait, être renforcée. L'article 8 de la directive 95/46/CE fait entrer dans la catégorie des données sensibles celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle. Le nouveau règlement ajoute dans cette catégorie les données génétiques et biométriques. Par ailleurs, les données relatives aux condamnations pénales, aux infractions pénales et aux mesures de sûreté connexes font aussi l'objet d'un traitement particulier prévu dans l'article 8 de la directive, dans la mesure où elles ne peuvent être traitées que sous contrôle de l'autorité publique. Elles peuvent ainsi, à ce titre, être considérées comme des données sensibles d'autant plus que la proposition de règlement de 2012 les incluait dans la définition du paragraphe 1 de l'article 9 consacré aux catégories particulières de données personnelles[10]. La protection de ce type de données est

[6] 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), *Journal officiel de l'Union européenne L119* du 4 mai 2016.

[7] Pour une approche plus large de la réforme de la protection des données au sein de L'Europe voir : C. CASTETS-RENARD (Dir.), *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, coll. Europe(s), 2015, 190 p.

[8] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *Journal officiel de l'Union européenne n° L 119* du 4 mai 2016, pp. 89-131.

[9] Selon la directive « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

[10] Dans le compromis de 2015, les Etats ont préféré séparer de nouveau ces données des autres données dîtes sensibles en créant un article 9 bis). Finalement, le règlement de 2016 leur consacre un article à part entière : l'article 10.

alors renforcée. Les Etats doivent, en principe, interdire leur traitement. Toutefois ce principe connaît des exceptions très encadrées qui permettent de rendre licite, dans des cas particuliers, la protection des données sensibles. Depuis l'adoption de la directive 95/46/CE, d'un côté le contexte géopolitique a changé, de l'autre la révolution numérique s'est accélérée et ces deux facteurs ont affaibli considérablement la protection juridique spécifique accordée aux données sensibles, ce qui explique d'ailleurs en partie la refonte du droit de l'Union européenne sur ces questions.

Avec l'utilisation des nouvelles technologies, les données à caractère personnel dites « sensibles » peuvent être collectées par l'individu lui-même et sont au même titre que les autres données personnelles, traitées de manière numérique et versées dans le *big data*. Dans ce contexte où un simple « clic » vaut accord, la recherche du consentement de la personne concernée ne peut, par exemple, plus suffire à protéger ces données dites « sensibles ». Le contrôle du traitement des données semble, en effet, échapper aussi bien aux autorités publiques qu'à l'utilisateur lui-même. Pourtant, le consentement de la personne concernée est un rempart solide contre les atteintes portées au droit au respect de la vie privée dans la mesure où il responsabilise la personne concernée et lui offre un moyen de contrôler le traitement qui est fait de ses données. Par ailleurs, les autorités étatiques peuvent, de manière justifiée, se livrer à un tel traitement des données sensibles si un intérêt public important légitime un tel traitement. En d'autres termes, si cela s'avère nécessaire. Les textes européens ont toujours laissé une grande marge de manœuvre aux Etats dès que les questions touchaient à la sécurité nationale. Dans ce contexte, les Etats sont à la fois les responsables du traitement des données et les garants de leur traitement licite. Or, la montée en puissance de la menace terroriste conduit les Etats à invoquer de plus en plus fréquemment ce motif afin de collecter des données sensibles sans parfois que la personne concernée n'en soit informée. La question sous-jacente et plus globale qui sous-tend cette réflexion est certes plus alarmiste mais résolument réaliste. Comment ne pas se demander aujourd'hui si nous pouvons encore protéger les données sensibles alors que d'un côté, leur traitement dépasse très largement les frontières étatiques et que d'un autre côté, à l'intérieur même des frontières étatiques, les autorités tendent à affaiblir la protection de ces données, en raison de leur nature même et au nom de la sécurité nationale. Dans ce contexte, le consentement de la personne concernée, expression de la volonté de cette dernière de voir utiliser des informations sur sa vie privée, a-t-il, par exemple, encore un rôle à jouer dans la protection des données à caractère personnel et plus particulièrement dans le cadre de la protection des données sensibles ? Afin d'apprécier la mesure dans laquelle d'un côté le numérique et de l'autre le contexte géopolitique altèrent la protection des données dites sensibles et conduisent à une réévaluation de l'équilibre entre liberté et sécurité, il convient de comprendre les spécificités du régime juridique de protection des données sensibles par rapport au régime juridique général de protection des données à caractère personnel. Il faudra se demander si ses spécificités du régime juridique des données sensibles suffisent encore aujourd'hui à maintenir une protection renforcée de ces données face non seulement à la révolution numérique mais face aussi aux impératifs de sécurité nationale de plus en plus prégnants aux vues des derniers attentats terroristes qui ont été perpétrés à Paris le 13 novembre 2015 et à Bruxelles le 22 mars 2016.

Section 1 – Vers un effacement de la spécificité de la protection juridique accordée aux données à caractère personnel sensibles

Une version a été publiée dans l'ouvrage suivant : Taleb-Karlsson (A.) De David Beauregard-Berthier (0.), *Protection des données personnelles et sécurité nationale. Quelles garanties juridiques dans l'utilisation du numérique ?*, Bruxelles, Bruylant, coll. « A la croisée des droits », 2017, pp. 63-88.

Le groupe de travail « article 29 » sur la protection des données[11] tout en reconnaissant que « le consentement de la personne concernée a toujours été une notion clé en matière de protection des données »[12] s'efforce, tout au long de son rapport de rappeler que le consentement de la personne concernée n'est qu'une des cinq conditions de licéité du traitement des données à caractère personnel, selon la directive 95/46/CE et le nouveau règlement (UE) 2016/679[13]. Le règlement (UE) 2016/679 tend même à noyer le consentement de la personne concernée au sein d'une multitude d'exceptions au principe d'interdiction de traitement des données sensibles. Pourtant, le fait même que la Commission européenne ait demandé une contribution de ce groupe de travail, dans le cadre de la révision de la directive 95/46/CE, sur cette notion de consentement atteste d'un côté, du rôle particulier de ce dernier dans la protection des données à caractère personnel de manière générale mais plus particulièrement dans la protection des données sensibles et d'un autre côté, de la nécessité de réfléchir la notion à l'aune de ses transformations à l'ère du numérique.

§1. La multiplication des exceptions au principe d'interdiction du traitement des données sensibles

L'article 8 de la directive 95/46/CE ainsi que l'article 9 du règlement (UE) 2016/679 consacrés aux données à caractère personnel dites sensibles posent, en leurs paragraphes 1, le principe de l'interdiction du traitement de ce type de données. Ces données, de par leur particularité, nécessitent une protection juridique renforcée par rapport au régime juridique général de protection des données à caractère personnel. Toutefois, le paragraphe 2 de ces articles vient tempérer l'interdiction en prévoyant des conditions de licéité du traitement de ce type de données, pour lesquelles le critère de nécessité préside largement à leur mise en œuvre[14]. Il est important de noter, dès à présent, que l'article 8§2 et suivants de la directive et

[11] Le Groupe de travail « article 29 » est un organe consultatif institué par la directive 95/46/CE.

[12] Groupe de travail « article 29 » sur la protection des données, *Avis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011 (WP 187), 01197/11/FR, p. 3.

[13] L'article 7 de la directive 95/46/CE et l'article 6 du règlement (UE) 2016/679 prévoient en effet qu'outre le consentement de la personne concernée, il existe cinq autres conditions de licéité du traitement des données à caractère personnel.

« Article 7 - Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :

a) la personne concernée a indubitablement donné son consentement ou

b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ou

c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou

d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou

e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ou

f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1 ».

[14] Hormis le consentement de la personne concernée, les autres conditions générales de licéité du traitement des données sensibles requièrent que ce traitement soit nécessaire. Ainsi, le traitement des données sensibles peut être licite s'il est « nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates », ou encore s'il est « nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ». De la même manière, le traitement des données sensibles est considéré comme licite s'il est effectué par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, dans le cadre de leurs activités légitimes et avec des garanties appropriées. En d'autres termes, si ce traitement est nécessaire pour la réalisation de leurs activités. Le

l'article 9§2 du règlement ne font qu'énoncer les conditions de licéité du traitement des données sensibles, ce qui n'exonère en aucun cas le responsable du traitement de ce type de données de ses obligations générales dans ce cadre, telles qu'un traitement loyal, transparent et équitable des données. Par ailleurs, la personne concernée dispose des mêmes droits que le traitement porte sur des données à caractère sensible ou non : droit d'information, d'accès aux données, de rectification de ces dernières, de recours en cas de traitement illicite des données. Le règlement (UE) 2016/679 prévoit, par ailleurs, de conférer à la personne concernée un droit à l'oubli et à l'effacement numérique[15] et un droit de portabilité des données.

Selon le paragraphe 2 de l'article 8 de la directive 95/46/CE, les données sensibles ne peuvent faire l'objet d'un traitement que si la personne concernée a donné son consentement à un tel traitement ou si ce traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail ; à la défense des intérêts vitaux de la personne concernée ou d'une autre personne ; aux activités d'une fondation, d'une association ou de tout autre organisme à but non lucratif ou encore aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé. Enfin, un tel traitement peut être licite si les données de la personne concernée ont été rendues publiques par cette dernière, en somme, si elle a elle-même consenti à les rendre publique. L'Etat, peut, de surcroît, prévoir par voie législative et pour des motifs d'intérêt public, d'autres exceptions que celles du paragraphe 2 de l'article 8 à condition que ces exceptions soient entourées de garanties appropriées. La sécurité peut, par exemple, être un motif permettant de rendre licite le traitement des données sensibles. Il peut sembler que le champ d'application du principe même d'interdiction du traitement des données se réduit comme une peau de chagrin au fur et à mesure que l'on avance dans la lecture de l'article 8 de la directive. Néanmoins, le critère de nécessité vient encadrer la plupart de ces exceptions et limite le traitement de ces données à des situations particulières à apprécier au cas par cas.

Le règlement (UE) 2016/679 reprend l'ensemble des exceptions de la directive de 1995 et y ajoute deux nouvelles exceptions permettant de rendre licite le traitement des données sensibles. En premier lieu, le traitement des données sensibles sera licite s'il est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice et chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle. Ce dernier aspect a été ajouté par le Conseil dans le compromis de 2015. En second lieu, le traitement des données sensibles sera licite s'il est nécessaire à des fins d'archivage dans l'intérêt public ou à des fins historiques, statistiques ou scientifiques. Là encore le Conseil, dans le compromis de 2015, a

---

critère de nécessité vient ainsi limiter le champ d'application de ces exceptions à l'interdiction générale de traitement des données sensibles.

[15] La doctrine juridique a été prolifique sur la question du droit à l'oubli numérique suite à l'arrêt *Google Spain* rendu par la Cour de justice de l'Union européenne. Voir notamment : D. DECHENAUD (Dir.), Le droit à l'oubli numérique : Données nominatives – Approche comparée, Bruxelles, Larcier, 2015, 452 p. ; M. BOIZARD, « La tentation de nouveaux droits fondamentaux face à internet : vers une souveraineté individuelle ? Illustration à travers le droit à l'oubli numérique », *in* A. BLANDIN-OBERNESSER (Dir.), *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, coll. Rencontres européennes, 2016, pp. 31-55. ; C. CASTETS-RENARD, « Google et l'obligation de déférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », *RLDI*, dossier spécial, n°106, 2014, pp. 68-75. ; V-L. BENABOU et J. ROCHFELD, « Les moteurs de recherche, maître ou esclaves du droit à l'oubli numérique ? Acte 2 : Le droit à l'oubli numérique, l'éléphant et la vie privée », *Dalloz* 2014, pp. 1481-1485. ; M. Clément-Fontaine et R. Amaro, « Séance 9 : Le droit à l'oubli numérique », in N. Martial-Braz (Dir.), La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau trans Europe experts, Paris, Société de législation comparée, coll. Trans Europe Experts, 2014, pp. 422-453.

ajouté une exception supplémentaire qui permet de rendre licite le traitement des données sensibles et qui a été conservé dans le règlement final. Un tel traitement est ainsi licite s'il est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontières graves pesant sur la santé. Si le critère de nécessité préside toujours à la recevabilité de ces conditions de licéité du traitement des données sensibles, la largesse des champs couverts par ces dernières interroge sur la substance même du principe d'interdiction. Quelle différence existe-t-il, en pratique, entre la licéité du traitement d'une donnée sensible et la licéité du traitement d'une donnée à caractère personnel non sensible ? Une différence fondamentale persiste. Alors que le traitement des données à caractère personnel peut-être licite s'il est nécessaire aux fins des intérêts légitimes poursuivis par un responsable du traitement, dans le cas des données sensibles, ces intérêts légitimes sont strictement définis – intérêts vitaux de la personne concernées, diagnostic médical, défense d'un droit en justice… – de sorte que le régime de protection s'en voit renforcé puisque seuls les traitements de données sensibles réalisés à ces fins seront licites. Le critère de nécessité joue le rôle de repère dans la recherche d'équilibre entre liberté du responsable du traitement et sécurité des données.

Par ailleurs, le consentement de la personne concernée, qui est une condition générale de licéité du traitement des données à caractère personnel devient dans le cadre du traitement des données sensibles une condition spécifique. Parmi les conditions de licéité du traitement des données sensibles, le consentement occupe une place particulière dans la mesure où il demeure la seule exception qui offre à la personne concernée, la liberté de choix. Même si le consentement de la personne concernée est la première des conditions de licéité du traitement des données sensibles listées par l'article 8§2 de la directive, il reste qu'il n'est pas présenté comme une condition plus importante ou plus primordiale que les autres. Dès lors, si le consentement de la personne concernée est le « véritable marqueur du degré de subjectivisation du droit de chacun sur ses données »[16], force est de constater que ce degré est faible dans le régime juridique de la directive 95/46/CE. Le consentement de la personne concernée peut, d'ailleurs, ne pas suffire pour rendre licite le traitement des données sensibles puisque l'article 8§2 a) précise que la législation nationale peut prévoir que le consentement de la personne concernée ne permette pas, dans certains cas, de lever l'interdiction de traitement prévue au paragraphe 1. De plus, alors que la proposition de règlement de la commission de 2012 offrait, en son article 4, une définition propre de la notion de « personne concernée » c'est-à-dire distincte de la définition de « donnée à caractère personnel », le nouveau règlement fusionne de nouveaux les deux définitions, reprenant par là même la proposition d'amendement 712 de la Commission LIBE[17]. Si certains auteurs estiment que cet amendement n'atteste pas d'un choix idéologique dans la conception de la protection des données à caractère personnel[18], il nous semble qu'une lecture, peut-être plus critique, peut en être faite.

La définition de la « personne concernée » occupait une place de choix dans le proposition de règlement de 2012 puisqu'elle ouvrait l'article 4 consacré aux définitions des termes clés. Ainsi, de la définition de la personne concernée découlait celle des données à caractère personnel comme si les données à caractère personnel appartenait à l'individu, était un

[16] N. MARTIAL-BRAZ, J. ROCHFELD, E. GATTONE, « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement 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 », *Recueil Dalloz*, 2013, pp. 2788 et ss.
[17] Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen.
[18] *Ibid*.

élément de son être. D'ailleurs, alors que dans la proposition de règlement de la Commission de 2012, les données à caractère personnel étaient définies comme « toute information *se rapportant* à une personne concernée » ; dans le compromis de 2015, le Conseil les définissait comme « toute information *concernant* une personne physique identifiée ou indentifiable ». Le verbe pronominal, qui marquait un lien fort entre l'individu et ses données avait été remplacé par une préposition qui se contentait de réunir deux mots. Même si la Commission LIBE avait justifié l'amendement 712 comme un simple déplacement de la définition de « personne concernée », tel n'était pas réellement le cas puisque ce déplacement avait entraîné une modification sémantique. Le règlement a finalement repris la définition de la proposition initiale réintroduisant par là-même le verbe pronominal. Fallait-il alors voir dans ce débat sémantique une volonté de ne pas basculer vers une personnalisation trop grande des données qui aurait pu ouvrir une brèche pour un débat sur la patrimonialisation des données ? Le rapport d'information, rédigé en 2014 pour le Sénat français par Mme Catherine Morin-Desailly, sur la gouvernance mondiale de l'internet peut le laisser penser lorsqu'il est affirmé que les propositions relatives à la patrimonialisation des données et « l'idée de monétisation des données personnelles qui les sous-tend vont à l'encontre de la conception européenne de la vie privée qui place sa protection sur le terrain des droits et libertés fondamentaux »[19]. La cession de ses données par l'individu lui ferait, en effet, perdre le contrôle sur le traitement de celles-ci alors que, par le biais du consentement, celui-ci dispose d'une garantie de traitement licite, loyal et transparent des données. La protection par ricochet des données à caractère personnel, qui découle du droit au respect de la vie privée et familiale, permet ainsi à la fois de protéger la personne concernée vis-à-vis de l'Etat et des entités privées mais aussi vis-à-vis d'elle même. La protection offerte par le biais des droits et libertés fondamentaux serait donc bien plus efficace que celle dont l'individu disposerait dans le cadre d'une patrimonialisation des données[20] et l'Union européenne, notamment par le biais de l'article 8 de la Charte sociale européenne, a ancré la protection des données personnelles dans le champ des droits de l'Homme et des libertés fondamentales. Le consentement de la personne concernée a donc un rôle particulier à jouer dans la protection des données et d'autant plus lorsque ces données sont dites sensibles. Toutefois, parmi les exceptions au principe d'interdiction du traitement des données sensibles, le consentement de la personne concernée est incontestablement celle qui se voit le plus grandement affaiblie par l'avènement du numérique.

§2. L'altération des formes d'expression du consentement au traitement des données sensibles à l'ère du numérique

Selon la lettre de l'article 8 de la directive 95/46/CE consacré aux données à caractère personnel dites sensibles, le traitement de ces données peut être licite si la « personne concernée a donné son consentement explicite à un tel traitement ». Le consentement de la personne concernée doit donc non seulement être libre, spécifique et informé – conditions générales de validité du consentement énoncées à l'article 2 h) de la directive – mais il doit être de surcroît, pour le traitement des données personnelles dites sensibles, explicite. Le projet de règlement de la Commission de 2012 proposait d'étendre cette condition

[19] Rapport d'information n° 696 (2013-2014) de Mme Catherine MORIN-DESAILLY, fait au nom de la MCI sur *la gouvernance mondiale de l'Internet*, déposé le 8 juillet 2014.

[20] L'affaire *Google Spain* illustre bien nos propos. Dans un contexte de patrimonialisation des données, il est difficilement envisageable que la personne concernée, une fois qu'elle a cédé à titre onéreux ses données, puisse faire effacer le lien de référencement de ces dernières. En revanche, en se plaçant sur le terrain des droits de l'Homme, la Cour se demande si l'ingérence dans la vie privée de l'individu est justifiée et elle considère qu'une telle ingérence ne saurait être justifiée par le seul intérêt économique de l'exploitant du moteur de recherche. Voy. CJUE, grande chambre : affaire C-131/12 – *Google v Costeja González*, arrêt du 13 mai 2014.

supplémentaire de validité du consentement à l'ensemble des situations où le consentement de la personne concernée était requis[21]. Toutefois, le texte de compromis de juin 2015[22] puis le règlement de 2016 n'ont pas repris cette solution confinant, de nouveau, cette condition supplémentaire au cas particulier du traitement des données personnelles dites sensibles[23]. Le consentement explicite de la personne concernée est ainsi la première des conditions de licéité du traitement des données sensibles. Or, la révolution numérique a, sans conteste, modifié nos habitudes nous faisant oublier les notions d'attente, de patience. Le numérique nous offre la possibilité d'obtenir, avec immédiateté, en un « clic », l'ensemble des informations dont nous avons besoin. Dans ce contexte, l'utilisateur, à la recherche de toujours plus de rapidité dans l'obtention de réponses et d'accessibilité toujours plus grande des services, accepte sans parfois sans rendre réellement compte, que ses données personnelles soient traitées[24]. Pourtant, selon la directive 95/46/CE et le nouveau règlement de 2016, le consentement valable pour le traitement de données sensibles doit être un consentement de la personne concernée à la fois libre, spécifique, informé et explicite. Si dans l'environnement hors ligne ces conditions ne sont pas toujours évidentes à réunir, dans l'environnement en ligne le changement des formes du consentement rend cette tâche encore plus délicate[25].

Les trois premiers critères de validité du consentement de la personne concernée sont communs à l'ensemble des catégories de données à caractère personnel. Le premier critère pour que le consentement de la personne concernée puisse être considéré comme valable est que ce consentement soit libre c'est à dire qu'il n'y ait pas « de risque de tromperie, d'intimidation ou de conséquences négatives importantes pour la personne concernée si elle ne donne pas son consentement »[26]. Traditionnellement, étaient particulièrement surveillées les relations de travail dans lesquelles le lien hiérarchique entre l'employé et l'employeur pouvait être une source de consentement non libre de la personne concernée. De la même manière, les relations avec l'autorité publique peuvent être appréciées comme des relations déséquilibrées. De manière plus globale, l'existence d'un rapport de subordination entraîne le risque que le consentement de la personne concernée ne soit pas donné librement. La proposition de règlement de 2012 prévoyait en ce sens que « le consentement ne constitue pas un fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif

[21] Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), Bruxelles, le 25.1.2012, COM(2012) 11 final, 2012/0011 (COD)

[22] Préparation d'une orientation générale sur la Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), Bruxelles, le 11 juin 2015, Dossier interinstitutionnel : 2012/0011 (COD).

[23] Le groupe de travail de l'article 29 avait recommandé d'ôter l'adjectif qualificatif « indubitable » dans le nouveau règlement car sa portée était ambiguë. Dans la proposition de règlement, la Commission a suivi l'avis du groupe de travail puisque l'article 4§8 remplace ce qualificatif par une exigence de « déclaration ou d'acte positif univoque ».

[24] Article 2 b) de la directive 95/46/CE : On entend par « Traitement de données à caractère personnel» (traitement): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

[25] Voir notamment sur la question du consentement et de la e-santé : P. DESMARAIS, « L'impact de la santé numérique sur le consentement du patient » (pp. 291-302) et M. SEREZAT, M. CAVALIER, « Le consentement à l'obscurité de la télémédecine » (pp. 303-306), *in* A. LAUDE (Dir.), *Consentement et santé*, Paris, Dalloz, 2014.

[26] Groupe de travail « article 29 » sur la protection des données, *Avis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011 (WP 187), 01197/11/FR, p. 39.

entre la personne concernée et le responsable du traitement ». La généralité de la formule permettait d'englober toute une série de situations connues ou qui pourront être à l'avenir générées par l'utilisation du numérique. Par exemple, en matière de données de santé, la mise en place des dossiers médicaux personnalisés a pu nous interroger. Si la licéité du traitement de ce type de données repose sur le consentement du patient, en cas de refus de celui-ci de consentir à un tel dispositif, ce dernier peut-il se voir refuser certains traitements ou doit-il supporter une charge financière plus lourde[27], ce qui de fait créerait une situation de déséquilibre. Avec le numérique, ce type d'exemples se multiplie dans la mesure où bien souvent si la personne ne consent pas à un traitement de ses données personnelles, elle ne peut simplement pas accéder au service proposé. Pourtant, le Conseil dans sa proposition d'orientation générale a décidé de supprimer cet ajout que l'on ne retrouve donc pas dans le texte du règlement de 2016. Le Conseil a suivi le raisonnement de la Commission LIBE, qui considérait que ce paragraphe 4 était source d'interprétation en pratique, notamment la notion d'équilibre, et donc de complexification dans la mise en œuvre du régime juridique général de protection des données. La notion de consentement libre doit ainsi s'apprécier au cas par cas et la question de l'équilibre de la relation pourra, lors de cette appréciation, entrer dans le faisceau d'indices permettant de déterminer si le consentement a été donné ou non librement.

Le consentement de la personne concernée doit ensuite être spécifique, il doit porter non seulement sur le type de données traitées mais aussi sur la finalité exacte du traitement. Là encore, l'environnement numérique vient complexifier l'appréciation du caractère spécifique du consentement concerné dans la mesure où il arrive, lorsque la personne désire utiliser un service numérique ou une application, qu'elle consente à ce que ses données soient traitées pour l'utilisation de ce service. Consent-elle alors pour autant à ce que ces mêmes données soient utilisées pour lui envoyer, par exemple, des publicités ciblées à partir de cette application ou pour la géo-localiser ? Enfin, le consentement de la personne concernée doit être informé, ce que la directive 95/46/CE détaille dans ses articles 10 et 11 en précisant les informations – par exemple l'identité du responsable du traitement, la finalité du traitement, l'existence d'un droit d'accès aux données et de modifications de celles-ci, ou encore le nom des destinataires des données – dont doit disposer la personne concernée lors d'un traitement de ses données à caractère personnel. Le nouveau règlement vient renforcer cet aspect du consentement en exigeant du responsable du traitement qu'il fournisse des informations à la personne concernée sous une forme intelligible et en des termes clairs et simples. En ce qui concerne ces conditions générales de validité du consentement, le nouveau règlement ne modifie pas substantiellement les notions, il se contente de reprendre dans les grandes lignes les principes de la directive 95/46/CE et d'en renforcer certains aspects. Il précise néanmoins que la personne concernée peut retirer son consentement à tout moment, le consentement n'est donc pas définitif. Toutefois, les traitements réalisés avant le retrait du consentement demeurent licites. La possibilité de retrait de son consentement par la personne concernée n'était qu'implicite dans la directive de 1995. Le nouveau règlement affirme ce droit de manière explicite – « il est aussi simple de retirer que de donner son consentement »[28] –

[27] La licéité du traitement des données de santé dans le cadre du dossier médical personnalisé a bien souvent un tout autre fondement juridique que le consentement de la personne concernée tel que l'intérêt public ou encore le §3 de l'article 8 de la directive 95/46/CE qui dispose : « Le paragraphe 1 ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente ».

[28] Article 7§3 du Règlement (UE) 2016/679.

comme l'avait fait au préalable la directive 2002/58/CE relative aux communications électroniques[29]. La personne concernée peut, par ailleurs, selon l'article 17 du règlement, demander l'effacement de ses données lorsqu'elle a retiré son consentement à leur traitement, que ce consentement constituait la base de licéité du traitement et qu'il n'en existait aucun autre.

Le dernier critère de validité du consentement de la personne concernée est propre aux données sensibles, il s'agit du caractère explicite du consentement. L'ajout de ce critère marque la volonté de protéger plus strictement les données sensibles mais le traitement numérique des données sensibles complexifie l'appréciation du caractère explicite du consentement. Tout d'abord, la dématérialisation du consentement peut, en effet, prendre plusieurs formes allant de la signature électronique sécurisée[30] à la simple case à cocher. Selon la directive 2002/58/CE, « le consentement peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site Internet »[31]. Le groupe de travail de « l'article 29 » a particulièrement attiré l'attention de la Commission sur la pratique des paramètres par défaut. En effet, dans ce dernier cas, l'utilisateur doit décocher une case ou changer les paramètres pour que son consentement ne soit pas enregistré. Or, une telle procédure ne peut raisonnablement pas être assimilée à un consentement explicite de la personne concernée. Le règlement de 2016 ne définit pas la notion de consentement explicite, de sorte que nous pouvons nous demander dans quelle mesure les mutations des formes du consentement impulsées par l'utilisation du numérique ont été prises en compte dans ce nouveau régime juridique. L'article 7§1 du règlement semble nous apporter une réponse dans la mesure où il précise que la charge de prouver que la personne concernée a consenti au traitement de ses données à caractère personnel à des fins déterminées incombe au responsable du traitement. Ainsi, le choix a été fait de renforcer les responsabilités du responsable du traitement en lui faisant porter la charge de la preuve du caractère explicite du consentement. Une telle approche avait été préconisée par le groupe de travail de « l'article 29 » qui espérait qu'une telle obligation conduise les responsable du traitement des données à mettre en place des procédures adéquates mieux formalisées et peut-être plus sécurisées pour recueillir le consentement des personne concernée. Si l'ère du numérique a indubitablement modifié les formes de consentement au traitement des données personnelles, il semble que les Etats de l'Union européenne n'ont, quant à eux, pas souhaité répondre à ces transformations par des critères plus strictes de validité du consentement de la personne concernée. D'un côté, une certaine souplesse dans l'obtention du consentement des personnes concernées est laissée aux responsables des traitements de données à caractère personnel et de l'autre, la responsabilité de ces derniers est renforcée en matière d'obligations d'information et de charge de la preuve du consentement.

[29] Article 6§3 et article 9 §3 et 4 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

[30] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques ; La Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) renvoie à la définition du consentement donnée par la directive 95/46/CE.

[31] Considérant 39 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

Dans les conclusions de son rapport de 2011[32], le groupe de travail « article 29 » sur la protection des données « considère » que le cadre actuel de la protection des données, porté par la directive 95/46/CE, comporte un ensemble bien pensé de règles fixant les conditions d'un consentement valable pour légitimer un traitement des données et que ces conditions s'appliquent aussi bien à l'environnement hors ligne qu'à l'environnement en ligne. Pourtant, les modifications de l'expression du consentement engendrées par l'utilisation du numérique modifient la place du consentement de la personne concernée dans la protection des données sensibles. L'ère du numérique a écorné le rôle du consentement dans le régime juridique général de protection des données en transformant son expression de sorte que celui-ci n'apparaît plus comme un rempart spécifique aux atteintes portées à la vie privée par le traitement des données sensibles. Le régime juridique général de protection des données à caractère personnel tend, par son évolution, à gommer les différences de protection entre les données à caractère personnel et les données à caractère personnel particulières. En effet, d'un côté, la protection des données à caractère personnel est renforcée et de l'autre, les spécificités du régime de protection des données personnelles particulières sont atténuées. Le renforcement général de la protection des données semble suffire à protéger tout type de données à caractère personnel même si les données sensibles bénéficient encore du principe d'interdiction de leur traitement et de l'exigence d'un consentement explicite de la personne concernée. Dans la cadre du domaine de la coopération policière et judiciaire, domaine exclu de l'application du régime général de protection des données, le consentement de la personne concernée est, en matière de protection des données dites sensibles, complètement occulté alors même que les risques d'atteintes à la vie privée ne sont que plus renforcés. Un glissement s'opère alors d'une conception personnifiée de la donnée pour sa protection vers une conception réifiée de la donnée pour sa finalité.

Section 2 – Vers une disparition de la catégorie juridique des données à caractère personnel sensibles dans le domaine pénal ?

L'analyse de la protection des données sensibles, à travers le cadre juridique général européen de protection des données à caractère personnel, nous a conduit à conclure à un appauvrissement de la spécificité du régime juridique de protection de ces données particulières en raison non seulement de la multiplication des exceptions à l'interdiction de traitement mais aussi du rôle mineur joué par la personne concerné dans la protection de ses données. Dans le domaine de la coopération policière et judiciaire, le consentement de la personne concernée tend à complètement s'effacer au profit d'un contrôle de la licéité du traitement des données quasi exclusif de l'autorité publique. La conception subjectiviste de la donnée est alors mise de côté, mais au delà, le doute plane sur le maintien même, dans ce domaine, d'une catégorie de données personnelles dont la protection serait renforcée.

§1. La licéité du traitement des données sensibles au delà du consentement de la personne concernée en matière pénale

La protection des données personnelles en droit de l'Union européenne est marquée par un éclatement du régime juridique dû, en majeur partie, à l'évolution non seulement technologique mais aussi des domaines de compétences de l'Union européenne. Lors de l'adoption de la directive 95/46/CE, le champ d'application de cette dernière excluait le traitement des données liées à la souveraineté de l'Etat et notamment le domaine de la

[32] Groupe de travail « article 29 » sur la protection des données, *Avis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011 (WP 187), 01197/11/FR, p. 40.

coopération policière et judiciaire, soit le Titre VI du TUE. L'article 13 de la directive autorise, de plus, les Etats membres à limiter, par voie législative, l'application de la directive lorsque cela est nécessaire pour sauvegarder la sûreté de l'État, la défense, ou encore la sécurité publique. De la même manière, le règlement général sur la protection des données de 2016 exclut de son champ d'application le traitement des données « 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, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces ». Toutefois, la montée en puissance du terrorisme, à son paroxysme lors des attentats américains du 11 septembre 2001 et des attentats européens de 2004 et 2005, et la mise en place effective d'un espace européen de liberté, de sécurité et de justice (ESLJ) ont nécessité que l'Union européenne encadre le traitement des données en matière de coopération policière et judiciaire. Une décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale a alors été adoptée[33]. Néanmoins, les restrictions de son champ d'application ne permettent pas d'assurer une protection efficace des données personnelles puisque la décision-cadre ne s'applique qu'aux traitements transfrontières des données, de sorte que les données traitées par les Etats de manière interne sont exclues de son champ d'application. La décision-cadre de 2008 consacre, toutefois, un de ses articles à la catégorie des données sensibles. Selon cet article, le traitement de ce type de données n'est pas, par principe, interdit mais il doit, en revanche, faire l'objet d'une autorisation dans une loi nationale qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée. Ainsi si une telle loi existe, le traitement et la mise à disposition des données sensibles devient licite sans même que le consentement de la personne concernée ne soit requis, quelque soit la qualité de cette dernière. L'Etat fait ainsi écran entre l'individu et ses données. Alors que ce dernier perd une part de son autonomie dans le contrôle du traitement de ses données personnelles, ses données, dans le même temps, deviennent la « chose de l'Etat », que ce dernier doit protéger pour garantir, par ricochet, le respect de la vie privée de l'individu. Le texte de 2008 ne recourt d'ailleurs à la notion de consentement que dans une situation précise. Le consentement est, en effet, une des conditions de licéité du traitement ultérieur des données à caractère personnel par un Etat membre pour des finalités autres que celles pour lesquelles elles ont été transmises. En d'autres termes, le consentement ne retrouve un droit de séance que lorsque le traitement des données est réalisé en dehors du domaine de la coopération policière ou judiciaire. Dans le cas contraire, la coopération policière et judiciaire justifie que le consentement de la personne concernée soit écarté des conditions de licéité du traitement des données à caractère personnel et que seul l'Etat garantisse la licéité du traitement de ces dernières et donc le respect des droits des individus. La décision-cadre prévoit d'ailleurs que son application « est sans préjudice des intérêts essentiels en matière de sécurité nationale et des activités de renseignement spécifiques dans le domaine de la sécurité nationale », c'est donc la protection juridique même de ce type de données qui est ébranlée pour ces motifs.

Le champ d'application très restrictif de cette décision a incité la Commission, en parallèle de la négociation de la proposition de règlement de 2012, a proposé une directive sur la protection des données en matière pénale afin de renforcer le corpus juridique de protection des données[34]. La directive a été adoptée en même temps que le règlement en avril 2016[35]. La

[33] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

[34] Commission européenne, Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes

directive (UE) 2016/680 a toutefois encore un champ d'application restreint. Elle ne s'applique, en effet, pas au traitement des données personnelles effectué dans le cadre d'une activité n'entrant pas dans le champ d'application du droit de l'Union, en ce qui concerne notamment la sécurité nationale. Cette référence à la sécurité nationale a fait s'élever des voix au sein du parlement européen dans la mesure où cette notion est floue et non définie en droit de l'Union européenne, alors même qu'elle permet d'exclure tout un régime juridique de protection des droits fondamentaux. Ce débat se justifie d'autant plus qu'alors que la sécurité nationale ne relève que de la compétence exclusive de l'Etat, la sécurité commune serait une compétence partagée avec l'Union européenne. Or, il reste que les actions menées au nom de la sécurité commune ont forcément des implications sur la sécurité nationale. En première lecture, le parlement européen a ainsi fait supprimer la référence à la sécurité nationale, de sorte que la directive s'appliquera dans tous les domaines couverts par le droit de l'Union, incluant ainsi les questions de sécurité commune.

La proposition de directive consacre, tout comme la décision-cadre, un article au traitement des données sensibles. Deux remarques peuvent être faites à ce stade sur ce texte. En premier lieu, la notion de données sensibles est élargie par rapport à la décision cadre de 2008. Les données génétiques entendues comme « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question » sont incluses dans la définition des données sensibles. Le Parlement européen avait, en première lecture, remplacé l'expression « données génétiques » par une référence aux « données biométriques » entendues comme « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ». Cette modification était justifiée par la volonté du Parlement de protéger plus strictement du point de vue des règles de conservation des données, les données génétiques en leur consacrant un article supplémentaire[36]. Dans le texte final de la directive, les données génétiques et les données biométriques sont incluses dans la catégorie particulière des données sensible, sans qu'un régime juridique particulier soit prévu pour les données génétiques. La seconde

---

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, 2012/0010 (COD).

[35] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *Journal officiel de l'Union européenne n° L 119* du 4 mai 2016, pp. 89-131.

[36] Article 8 bis : « Traitement de données génétiques aux fins d'une enquête criminelle ou d'une procédure judiciaire :

1. Les États membres veillent à ce que les données génétiques ne puissent être utilisées qu'afin d'établir un lien génétique dans le cadre de la fourniture de preuves, de la prévention d'une menace pour la sécurité publique ou de la commission d'une infraction pénale spécifique. Les données génétiques ne peuvent être utilisées pour déterminer d'autres caractéristiques susceptibles d'être génétiquement liées.
2. Les États membres prévoient que les données génétiques ou les informations découlant de leur analyse ne peuvent être conservées au-delà de ce qui est nécessaire aux fins pour lesquelles les données ont été traitées et lorsque la personne concernée a été reconnue coupable d'atteintes graves à la vie, l'intégrité ou la sécurité de personnes, sous réserve de durées de conservation strictes fixées par la législation des États membres.
3. Les États membres s'assurent que les données génétiques ou les informations découlant de leur analyse ne sont conservées pour des durées plus longues que si les données génétiques ne peuvent être attribuées à une personne, en particulier lorsqu'elles ont été trouvées sur une scène de crime ».

remarque concerne les conditions de licéité du traitement des données sensibles dans le domaine de la coopération policière et judiciaire. Là encore, le consentement de la personne concernée est écarté des conditions de licéité du traitement des données sensibles et le principe d'interdiction du traitement des données sensibles qui était de nouveau affirmé dans la proposition de directive a disparu de l'article 10 de la directive de 2016. Dans l'ensemble du texte de la directive (UE) 2016/680, la notion de consentement a d'ailleurs été bannie, le paragraphe (35) précisant même « (…) que le consentement de la personne concernée au sens du règlement (UE) 2016/679 ne devrait pas constituer une base juridique pour le traitement des données à caractère personnel par les autorités compétentes. Lorsqu'elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix ». La personne concernée perd donc sa liberté dans le choix du traitement ou non de ses données sensibles et le traitement des données sensibles est licite uniquement en cas de nécessité absolue où alors dans trois autres cas de figure : s'il est autorisé par une législation prévoyant des garanties appropriées ; ou s'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ; ou encore si ce traitement porte sur des données manifestement rendues publiques par la personne concernée. Dans ce dernier cas, on pourrait avoir une lecture large de cette condition de licéité et estimer que si la personne a rendu publiques ses informations, elle consent, par ricochet, à leur traitement. Toutefois, nous sommes là très loin de l'exigence de consentement explicite prévue dans le cadre général de protection des données. Par ailleurs, la première condition de licéité du traitement des données sensibles rend presque caduque l'existence de cette catégorie de données puisque, dès lors que l'Etat adopte une loi dans le domaine large de la coopération policière ou judiciaire dotée de garanties appropriées, le traitement de ces données est possible.

En sus de ces deux textes, l'Union européenne a développé un droit spécifique en matière de coopération policière et judiciaire afin de renforcer la sécurité commune. D'une part, il existe des régimes juridiques spéciaux propres à certains organes communautaires tels qu'Europol et Eurojust et se développent aussi des régimes juridiques spéciaux pour les systèmes d'informations crées au niveau de l'Union européenne comme le système d'information sur les visas ou encore Eurodac. D'autre part, il existe une prolifération d'actes concernant le renforcement de la coopération policière et judiciaire qui chacun consacre un chapitre à la protection des données en rappelant simplement les standards minimums de protection[37]. L'exemple le plus récent, en la matière est la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière[38], qui en son article 13 consacré à la protection des données, rappelle les droits de la personne concernée en matière d'accès, de vérification, d'effacement, de verrouillage de ses données et en matière de recours. Il faut toutefois noter que le paragraphe 4 de l'article 13 pose le principe d'interdiction de traitement des données sensibles tout en n'incluant pas dans cette

[37] Par exemple, la Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres ou encore la Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (Décision Prüm) ou encore Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne.

[38] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *JOUE*, L119 du 4 mai 2016, p. 132.

catégories les données génétiques ni biométriques. En matière de coopération policière et judiciaire, le traitement des données sensibles devient aisément licite en raison des motifs particuliers qui conduisent au traitement de ces données. L'exclusion du consentement de la personne concernée des conditions de licéité des données sensibles leur ôte de leur spécificité et enlève à la personne concernée une part de sa liberté dans la protection de sa vie privée, d'autant plus qu'aucune distinction n'est faite entre l'autorisation de traitement des données sensibles d'une personne victime, suspecte ou coupable. Ainsi, les données sensibles ne semblent plus faire l'objet d'une protection particulière, dès lors qu'elles sont traitées dans le domaine de la coopération policière et judiciaire. Il est de ce fait possible de s'interroger sur l'existence ou non de garanties spécifiques dans le traitement de ces données en matière de coopération policière et judiciaire.

§2. L'affaiblissement des garanties spécifiques appliquées au traitement des données sensibles dans le domaine pénal

La décision-cadre de 2008 tout comme la directive de 2016 ne posent pas comme nous l'avons vu le principe de l'interdiction du traitement des données sensibles. De surcroît, la personne concernée perd sa liberté de choix du traitement ou non de ses données sensibles. Dans ce contexte, les données sensibles constituent-elles toujours, une catégorie particulière de données à caractère personnel dont la protection serait renforcée ? En d'autres termes, ces régimes juridiques prévoient-ils des garanties spécifiques au traitement des données sensibles ?

L'article 23 de la décision cadre de 2008 met en place une garantie particulière dans le cas d'un traitement particulier des données sensibles : la mise en place d'un nouveau fichier. En effet, si un Etat membre désire créer un nouveau fichier contenant des données à caractère personnel dites sensibles, il devra au préalable consulter l'autorité nationale de contrôle de la protection des données comme, par exemple, la CNIL pour la France. A cette occasion, l'autorité nationale appréciera si le traitement des données sensibles s'accompagne de garanties appropriées pour la protection des intérêts légitimes de la personne concernée notamment la durée de conservation des données, les voies de recours possibles pour la personne concernée…. Cette exigence de consultation préalable de l'autorité nationale de contrôle ne s'impose à l'Etat que dans la mesure où le nouveau fichier traite des données sensibles ou utilise pour fonctionner des nouvelles technologies. Il s'agit donc d'une garantie supplémentaire de protection des données sensibles. La directive de 2016 ajoute une seconde garantie des données sensibles en matière de profilage. L'article 11§2 de la directive pose, en effet, le principe selon lequel les décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative ne sont pas fondées sur les catégories particulières de données à caractère personnel à moins que des mesures de sauvegarde des droits de la personne ne soient mises en place. L'article précise d'ailleurs que les discriminations opérées sur la base de tel profilage restent contraires au droit de l'Union européenne. La directive prévoit ensuite un droit d'effacement des données traitées de manière illicite. Initialement, la proposition de directive prévoyait des garanties somme toute très minimales dans le cadre du traitement des données sensibles au point que l'existence de cette catégorie particulière de donnée perdait son sens. Le parlement européen, en première lecture du texte, avait dès lors voulu renforcer la protection des données sensibles afin de redonner à cette catégorie juridique toute son importance.

Le parlement européen avait, en premier lieu, proposé un amendement visant à l'introduction d'un article 25 bis relatif à la mise en place d'une étude d'impact. Ainsi, le responsable du traitement des données ou son sous-traitant aurait dû, dès lors qu'il aurait été question de traiter des données sensibles, procéder à une analyse de l'impact des procédures et systèmes de traitement envisagés sur la protection des données à caractère personnel, et ce avant l'introduction des nouveaux traitements ou dans les meilleurs délais si les traitements existaient déjà. Les éléments de l'analyse d'impact étaient ainsi détaillés par le Parlement. Ils devaient notamment permettre d'apprécier la proportionnalité du traitement eu égard à sa finalité, l'impact du traitement sur les droits et libertés de la personne concernée et inclure une consultation du public. L'individu était ainsi remis au centre de la procédure concernant ses données. La directive de 2016 a effectivement mis en place une procédure d'étude d'impact en son article 27 mais celle-ci est bien moins précise que ce que le Parlement avait prévu dans la mesure où la consultation du public n'est plus mentionnée ni même la référence aux données sensibles. La marge d'appréciation est laissée aux Etats pour déterminer les traitements de données qui nécessitent une analyse d'impact préalable. Par ailleurs, en matière de traitement automatisé des données sensibles, le Parlement européen demandait que soient mises en place des mesures de sécurité supplémentaires afin non seulement d'assurer la prise de conscience pleine et entière des risques mais aussi afin d'avoir la capacité de prendre des mesures de prévention, de correction et d'atténuation, presque en temps réel, contre les faiblesses et les incidents décelés qui pourraient présenter un risque pour les données. L'article 29 de la directive de 2016, consacré à la sécurité du traitement des données à caractère personnel, insiste, en effet, sur la nécessité de prendre toutes les mesures de sécurité possibles lors du traitement des données sensibles. Le Parlement européen s'est ainsi attaché à renforcer la protection des données sensibles en matière de coopération policière et judiciaire et a, en conséquence, cherché pour ce type de données à mettre en place des gardes fous pour que la sécurité ne soit pas un motif pour réduire les droit fondamentaux de la personne en matière de protection des données. Toutefois, le texte final n'est pas allé aussi loin que ce que le Parlement préconisait. A l'heure actuelle, force est de constater, qu'aussi bien dans le régime général de protection des données qu'en matière pénale, les données dites sensibles voient leur régime juridique spécifique s'appauvrir au point qu'elles semblent versées sans distinction dans la catégorie plus globale des données à caractère personnel.

******

Au sein de l'Union européenne, l'année 2016 aura été marqué par une refonte de l'ensemble du cadre juridique européen de protection des données à caractère personnel. L'évolution technologique rapide obligeait à repenser le cadre juridique de 1995. Or, la démarche de l'Union européenne dans le règlement général nous semble davantage être celle d'une volonté d'asseoir des droits existants plutôt que d'en créer des nouveaux repoussant par là même l'idée que l'environnement numérique rendrait désuet notre conception des droits de l'Homme. Dans le cadre répressif, en revanche, l'équation est différente. Le climat anxiogène engendré par les séries d'attentats qui ont touché l'Europe ces deux dernières années ont fait craindre que la liberté soit sacrifiée au profit de la sécurité. Or, aussi bien les retours en arrière opérés par la directive (UE) 2016/680 par rapport à la proposition de 2012 et aux amendements du Parlement que l'adoption rapide de la directive PNR pourtant jusque là bloquée par des négociations difficiles doivent nous alerter et nous conduire à garder un œil vigilant sur les atteintes à nos droits et libertés quelque soit le contexte qui entoure l'adoption de nouveaux textes.

Une version a été publiée dans l'ouvrage suivant : Taleb-Karlsson (A.) De David Beauregard-Berthier (0.), *Protection des données personnelles et sécurité nationale. Quelles garanties juridiques dans l'utilisation du numérique ?*, Bruxelles, Bruylant, coll. « A la croisée des droits », 2017, pp. 63-88.