FIDE
XXIX, Congress, The Hague, May 2020

Questionnaire Topic 2 : The New EU Data Protection Regime

Rapport français : Céline Castets-Renard, Mathieu Combet, Olivia Tambou[1]

Question 1 : Identifiez et décrivez les principaux instruments légaux nationaux qui ont été introduits pour transposer le GDPR. En particulier, montrez comment ces instruments ont profité des plus remarquables flexibilités incorporées dans le GDPR (par exemple article 6(1)(c); article 23 et articles 86-90 du GDPR) et quelle autorité nationale de contrôle supervise leur exercice en relation avec ces instruments.

En France, les deux principaux textes adaptant le droit français au RGPD et transposant la Directive Police Justice sont actuellement la nouvelle loi Informatique et Libertés (ci-après LIL) et le décret n°2019-536 du 29 mai 2019 entrés en vigueur le 1er juin 2019. La LIL comporte actuellement 128 articles répartis en cinq titres:

- Titre Ier : Dispositions communes, consacré notamment aux principes, définitions, à l'autorité de contrôle qui est la Commission Informatique et libertés (ci-après CNIL), formalités préalables, voies de recours,
- Titre II : Traitements relevant du RGPD
- Titre III : Dispositions applicables aux traitements de la directive Police Justice
- Titre IV : Dispositions applicables aux traitements intéressant la sûreté de l'Etat et la défense;
- Titre V : Dispositions relatives à l'outre-mer

Cette présentation ainsi que le "choix" d'opérer de nombreux renvois au RGPD en raison de son effet direct rend le texte final parfois peu lisible voire inintelligible pour des non spécialistes. En outre, on constate des phénomènes tantôt de sur-adaptation visant à aller au-delà des règles ayant effet direct du RGPD, tantôt de sous-adaptation visant à maintenir des règles nationales antérieures dont la formulation n'est pas conforme à celle du RGPD. (C'est notamment le cas pour les règles relatives à l'article 80 RGPD cf. notre analyse question 13).

D'une manière générale, le gouvernement a estimé que le RGPD comportait une liste de 56 renvois au droit national. Il a été décidé de faire une utilisation modérée des marges d'appréciation[2] laissées aux Etats membres par le RGPD. Une part importante de l'usage des dérogations et limitations concerne les autorités publiques ou certaines catégories de traitements de données.

[1] Les questions 3,5,6,10, 11 ont été préparées par Céline Castets-Renard, Full Professor à l'Université d'Ottawa, les questions 2,4,7,12 et 14 par Mathieu Combet Maître de Conférences à l'Université de Saint-Etienne, les questions 1,8,9,13, 15 par Olivia Tambou, Maître de Conférences à l'Université Paris-Dauphine.

[2] Pour plus de détails cf. notre article French Adaptation of the GDPR in Mc Cullagh K., Tambou O., Bourton S. (Eds.), National Adaptations of the GDPR, Collection Open Access Book, Blogdroiteuropeen, Luxembourg February 2019, 130 pages Available at: https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf)

Les principales flexibilités au RGPD existant en France sont :

- **Une disposition relative au droit applicable en cas d'usage de clauses ouvertes par les Etats membres**

Cette question n'a pas été abordée dans le RGPD. La France a néanmoins pris l'initiative de préciser que lorsque le RGPD renvoi au droit national le soin de l'adapter le droit français s'applique en principe "*lorsque la personne concernée réside en France y compris lorsque le responsable de traitement n'est pas établi en France*". (art. 3 II LIL). Le critère de résidence est remplacé par le critère de l'établissement lorsque des traitements à des fins journalistiques ou à des fins d'expression universitaire, artistique, ou littéraire sont en cause. Autrement dit, le droit français s'appliquera, dès lors que le responsable du traitement est établi en France.

- **Les données post-mortem** (considérant 27 RGPD, art. 84-86). Exclues du champ d'application du RGPD, les données personnelles des personnes décédées font l'objet de dispositions introduites en France en 2016 par loi n° 2016-1321 dite République numérique. Il s'agit notamment de permettre aux personnes de laisser des directives relatives au traitement de leurs données personnelles après leur mort (testament numérique) et de préciser les droits pouvant être exercés par les héritiers en l'absence de ces directives.

- **L'interdiction des traitements des données sensibles** (art. 9 RGPD, art. 44 de la LIL).
  Six types de traitements de données sensibles sont possibles en France:
  1° Les traitements nécessaires 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 mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel
  2° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels
  3° Les traitements comportant des données concernant la santé justifiée par l'intérêt public
  4° Les traitements conformes aux règlements types mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux agents, aux stagiaires ou aux prestataires ;
  5° Les traitements portant sur la réutilisation des informations publiques sous réserve que ces traitements n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées ;
  6° Les traitements nécessaires à la recherche publique

- **L'âge du consentement du mineur (art.8 RGPD, art. 45 de la LIL).** La France a opté pour une solution inédite qui prévoit :
    - avant 13 ans le consentement du seul titulaire de l'autorité parentale,
    - entre 13 et 15 ans le consentement conjoint du mineur et du titulaire de l'autorité parentale. La conformité du double consentement a été justifiée tant par le gouvernement que par le Conseil constitutionnel français[3] par la lettre 8 RGPD qui distingue le consentement donné, du consentement autorisé. Pour autant, cette interprétation unilatérale du RGPD peut interroger
    - Après 15 ans, le consentement du seul mineur.

.

- **Traitement des données à caractère personnel relatives aux condamnations pénales** (art. 10 RGPD, art. 46 LIL). Six catégories de personnes peuvent traiter ces données particulières. La principale nouveauté est d'avoir introduit "Les réutilisateurs des informations publiques ... sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernée". Il s'agit de répondre à l'engagement politique de la France en matière d'Open Data.

- **Fondement légal pour des décisions administratives individuelles exclusivement automatisées** (art. 22 RGPD §2b), art. 47 de la LIL cf. réponse question 6 pour plus de détails)

- **Quelques limitations de droits** (art. 23 RGPD- art. 48, 49, 52, 58 LIL)
    - **pas de droit à l'information pour les données collectées indirectement** (art. 14 RGPD) pour certains traitements mis en œuvre pour le compte de l'Etat intéressant la sécurité publique, le contrôle et le recouvrement des impôts (art. 48 LIL)
    - **pas de droit d'accès** pour les traitements aux seules finalités d'établissement de statistiques ou de réalisation de recherche scientifique ou historiques et sous certaines conditions (art. 49 alinéa 3 LIL).
    - **droit d'accès, de rectification et d'effacement indirect** par le biais de la CNIL pour certains traitements liés au contrôle et recouvrement des impôts (art. 52 LIL)
    - pas **de communication à la personne concernée de violation de données** (Art. 34 RGPD, art. 58 II LIL) pour une catégorie de traitements dont la communication serait susceptible d'engendrer un risque pour la sécurité nationale, la défense ou la sécurité publique**.** Liste des traitements concernés à l'art. 85 du décret n°2019-536.
    - **Des limitations de droits** découlant de l'article 85 RGPD cf. question 9.

- **Le maintien de quelques formalités préalables** (Chapitre IV de la LIL, art. 31-36) : Une autorisation préalable a été maintenue pour:
    - des traitements de souveraineté, (art. 31-1 LIL),

[3] cf. Point 63 de la décision du Conseil Constitutionnel nº 2018-765 du 12 juin 2018.

    - certains traitements dans le domaine de la santé (art 66 III LIL),
    - certains traitements de données génétiques ou biométriques (art. 32 LIL).
- **Etablissement d'une liste limitative de personnes pouvant traiter le NIR** (numéro d'inscription au répertoire), art. 30 LIL, décret n°2019-341 du 19 avril 2019.
- **Traitement des données dans le cadre des relations de travail (art. 88 du RGPD),** existence de règles en matière de vidéosurveillance, droit d'information du salarié, traitement des fiches de paie, dans le code du travail (notamment art. L1221-9 et L-1222-4)
- **Prise en compte de certains publics : mineurs, TPE, PME, collectivités locales**
    - L'article 48 alinéa 2 de la LIL précise que l'information au titre de l'article 13 du RGPD doit être transmise au mineur de moins de 15 ans "*en langage clair et facilement accessible*".
    - Mission de la CNIL visant en accompagner plus particulièrement ces acteurs.

Question 2 : Est-ce que votre ordre juridique national différencie la vie privée les droits à la vie privée (art. 7 Charte des droits fondamentaux de l'UE) et à la protection des données personnelles (art. 8 de la charte) ? Est-ce que le droit à la protection des données personnelles reconnu par la Charte européenne a influencé l'interprétation de votre droit national ?

En droit français, le droit au respect de la vie privée a été introduit à l'article 9 du Code civil, introduit par la loi du 17 juillet 1970. De son côté, la protection des données personnelles a été introduite par LIL en 1978 modifiée par la loi n°2004-801 du 6 août 2004 pour l'adapter à la directive 95/46 CE et enfin par la loi n°2018-493 du 20 juin 2018 pour l'adapter au RGPD et à la Directive Police Justice.

C'est en raison des risques d'atteintes à la vie privée des personnes que la protection des données personnelles a été intégrée au droit au respect de la vie privée. C'est ce qui ressort de certaines décisions du Conseil Constitutionnel comme la décision n°2012-652 du 22 mars 2012 sur la loi relative à la protection de l'identité sur le fondement de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

La Charte européenne sur les droits fondamentaux (art. 8) a eu une influence sur la protection du droit à la protection des données qui n'était pas reconnue comme un droit fondamental en France. Au demeurant, le contentieux portant sur ces questions ne se fonde pas directement sur les dispositions de la Charte, mais sur des textes nationaux ou de droit dérivé. Il n'en demeure pas moins que la jurisprudence de la Cour de justice de l'Union européenne a eu une certaine influence sur la protection des données personnelles comme avec le droit à l'oubli avec notamment l'arrêt Google Spain de 2014[4] ou bien encore l'arrêt Manni de 2017[5].

[4] CJUE 13 mai 2014, *Google Spain SL, Google Inc. c/ Mario Costeja González* e.a., aff. C-131/12, ECLI:EU:C:2014:317
[5] CJUE 9 mars 2017, *Camera di Commercio c/ S. Manni*, aff. C-398/15, ECLI:EU:C:2017:197

Le Conseil d'Etat français a, dans une décision du 24 février 2017[6], saisi la Cour de justice de l'Union européenne de plusieurs questions préjudicielles portant notamment sur le droit à l'oubli. En outre, et en attendant la réponse de la Cour de justice, la Cour de cassation a décidé de surseoir à statuer dans un arrêt du 5 juin 2019[7].

Question 3 : Comment les responsables de traitement ont-ils interprété et appliqué les principes de traitement "loyal" , principe de finalité et de minimisation des données ? L'autorité nationale de contrôle a-t-elle appliqué ces principes et ont-ils été interprétés par les juridictions nationales ?

Question 4 : Comment les bases légales - "consentement" et "légitime intérêt" - les notions les plus opaques dans l'environnement numérique - ont-elles été interprétées par les juridictions nationales ?

Le Conseil d'Etat a eu l'occasion de se prononcer sur la notion **"d'intérêt légitime"** dans un arrêt du 18 mars 2019 dans le cadre d'une procédure d'une personne exerçant son droit d'opposition à l'exploitation des données personnelles de ses enfants[8].
Selon le Conseil d'Etat, le droit de toute personne physique de s'opposer au traitement de ses données personnelles, conformément à l'article 38 de la LIL est subordonné à l'existence de raisons légitimes. Ces dernières doivent tenir de manière prépondérante à la situation particulière du demandeur. C'est-à-dire que le fait de faire état de craintes d'ordre général sans pour autant évoquer des considérations qui sont propres à la situation de ses enfants n'est pas suffisant pour établir l'existence d'un motif légitime.
Si le Conseil d'Etat ne s'est pas prononcé sur le fondement du RGPD en raison du fait qu'il n'était pas applicable aux moments des faits, il est intéressant de noter que l'article 21 relatif au droit d'opposition prévoit, quant à lui, que « la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant ». Partant, la position adoptée par le Conseil d'Etat apparaît particulièrement proche de la notion d'intérêt légitime, telle qu'elle est mentionnée dans le RGPD. On dénombre près d'une vingtaines d'affaires qui ont été jugées par le Conseil d'Etat sur la notion d'intérêt légitime dans le cadre d'une procédure portant sur le droit d'opposition. Il n'en demeure pas moins que la notion d'« intérêts légitimes » mentionnée à l'article 6.1 du RGPD n'a pas encore fait l'objet d'une interprétation des juridictions nationales.

En ce qui concerne le **consentement,** c'est surtout la CNIL qui s'est prononcée sur cette notion. En vertu de l'article 2, point h) de la directive 95/46/CE, le consentement s'entend comme toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. À cet égard, la notion de consentement, reprise dans le RGPD est d'ailleurs plus exigeante dès lors qu'il est prévu que celui-ci doit être donné par un acte positif clair par lequel la personne

[6] n°391000, 393769, 399999 et 401258.
[7] Civ. 1ère, 5 juin 2019, n°18-14.675.
[8] CE, 18 mars 2019, n°406313.

concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant[9].

Il est à noter que le Tribunal de grande instance de Paris s'est prononcé sur 38 clauses des «Conditions d'utilisation » et des « Règles de confidentialité » de Google qu'il a déclaré comme abusives et certaines de ces clauses portaient sur le consentement des utilisateurs. En effet, la rédaction de ces clauses faisait apparaître qu'il y avait une présomption de consentement du consommateur à la collecte de ses données personnelles.
Le consentement a aussi été au cœur de la première condamnation de la CNIL post RGPD qui a été rendue contre Google le 21 janvier 2019[10].

Question 5 : Y a-t-il eu des débats ou décisions au niveau national concernant la validité des données personnelles comme "contrepartie" à la fourniture de contenu numérique ?

Cette question a fait l'objet de débats, spécialement dans le cadre de l'adoption de la directive relative à certains aspects des contrats de fourniture du contenu numérique en avril 2019 (Dir. 2019/770/UE). La proposition initiale de la directive ne considérait le prix à payer pour la fourniture d'un contenu numérique que comme une somme d'argent. Or, l'économie numérique est fondée sur la donnée et la fourniture de données à caractère personnel constitue parfois le seul prix à payer. La fourniture de données à caractère personnel a été réintroduite par le compromis adopté au Conseil et la directive s'appliquera désormais lorsque le consommateur fournit uniquement des données à caractère personnel. Les services de communication interpersonnelle par contournement, les contrats groupés et le traitement des données à caractère personnel sont inclus dans le champ d'application de la directive relative au contenu numérique. À l'issue des négociations, une référence expresse au règlement général sur la protection des données personnelles (RGPD) a été introduite dans la directive (voir notamment le considérant 37 et l'article 3§8).

Ces enjeux ont aussi fait l'objet de discussions au Sénat en France lors de la présentation du rapport d'information n° 326 (2017-2018) de M. André Gattolin et Mme Colette Mélot, fait au nom de la commission des affaires européennes, déposé le 21 février 2018[11].

Notons que la Quadrature du net, association de défense des libertés fondamentales dans l'environnement numérique, a défendu la position de ne pas considérer les données personnelles comme une marchandise et de ne pas les introduire dans la directive sur la fourniture de contenus numériques[12]. Le considérant 24 de la directive précise au contraire que : "tout en reconnaissant pleinement que la protection des données à caractère personnel est un

[9] Délibération CNIL n°2013-4203 du janvier 2014 ; Délibération CNIL n°MED-2018-023 du 25 juin 2018 ; Décision CNIL n°MED-2018-02325 du juin 2018.
[10] Délibération n°SAN-2019-001 du 21 janvier 2019,
[11] Voir : http://www.senat.fr/rap/r17-326/r17-326_mono.html#toc8.
[12] Cette association appelle à la reconnaissance d'un principe fondamental que le droit à la vie privée et à la protection des données, tout comme n'importe quel autre droit fondamental, ne puisse être vendu : https://www.laquadrature.net/2017/11/21/contenu_num_pe.

droit fondamental et que, par conséquent, les données à caractère personnel ne peuvent être considérées comme des marchandises, la présente directive devrait garantir aux consommateurs, dans le cadre de ces modèles commerciaux, le droit à des recours contractuels". L'article 3§1 porte sur le champ d'application et pose ainsi que la directive s'applique lorsque le professionnel fournit ou s'engage à fournir un contenu numérique ou un service numérique au consommateur et le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel, sauf lorsque les données à caractère personnel fournies par le consommateur sont exclusivement traitées par le professionnel pour fournir le contenu numérique ou le service numérique ou pour permettre au professionnel de remplir les obligations légales qui lui incombent.

Dans le cadre du débat autour de monétisation des données, la France a adopté le 11 juillet 2019[13], sa propre taxe sur les services numériques, taxe dite GAFA à défaut de pouvoir le faire à l'échelle de l'UE. Un accord a été trouvé au récent G7 de Biarritz fin août 2019 avec le Président Trump sur la mise en œuvre de cette taxe française qui devrait être supprimée dès qu'une taxe similaire aura été mise en place à l'échelle de l'OCDE.

Question 6 : L'article 22 accorde le droit de ne pas faire l'objet d'une décision automatisée, y compris le profilage. L'article 22(2)(b) permet aux Etats membres d'introduire des mesures législatives pour permettre que ce droit ne s'applique pas à certaines situations. De telles mesures législatives ont-elles été introduites dans votre droit et, si oui, quelles mesures de sauvegarde des droits, libertés et légitimes intérêts des personnes concernées ont-elles été incorporées ?

L'article 10 de la nouvelle LIL pose que "aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception : 1° des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, sous les réserves mentionnées au 3 du même article 22".

- **Exceptions prévues par le RGPD**

Si cette partie de la LIL reprend le RGPD, il faut toutefois noter une formulation différente entre le RGPD et la version française. Alors que le RGPD accorde clairement un droit au profit de la personne concernée, "de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire", la LIL affirme qu'aucune décision ne peut être prise, ce qui semble être une obligation s'adressant au responsable de traitement, sans pour autant qu'il en soit explicitement débiteur. La reconnaissance d'un droit subjectif qui peut être mis en œuvre par un créancier de l'obligation a sans doute plus de vigueur qu'une

[13] Loi n° 2019-759 du 24 juillet 2019 portant création d'une taxe sur les services numériques et modification de la trajectoire de baisse de l'impôt sur les sociétés

formulation générale impersonnelle de nature à créer une obligation non explicitée à l'égard du responsable de traitement. Cette remarque doit toutefois être nuancée par le fait que cette disposition de la LIL s'intègre au chapitre V de la loi n° 2018-493 du 20 juin 2018 relatif aux "Dispositions particulières relatives aux droits des personnes concernées". L'intention du législateur français n'est certainement pas de remettre en cause ce droit consacré par le RGPD mais on pourra regretter qu'il n'ait pas repris la même formulation. La forme de la LIL s'explique cependant par la conservation de l'expression précédente prévue par la loi de 1978. Au demeurant, le CEPD a bien précisé que l'article 22 consacre une interdiction.[14]

- **Garanties supplémentaires**

Parmi les différences, il faut également relever que la LIL ajoute une condition tenant au fait que "les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre" doivent être "communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande". Cette disposition renforce la protection de la personne concernée, ce qui est compatible avec un des objectifs du RGPD. On peut donc dire que le législateur français a adopté des mesures supplémentaires de sauvegarde des droits, libertés et légitimes intérêts des personnes concernées, y compris dans le cadre des exceptions prévues par le RGPD.

Une telle disposition traduit la volonté de reconnaître explicitement un droit à la transparence et à l'explication qui est sous-entendu dans le RGPD et a fait l'objet de débats, surtout parmi la doctrine aux États-Unis et en Europe sur le fait de savoir s'il existe ou non un droit à explication à l'article 22 du RGPD[15], complété par les articles 13-15[16]. Il semble qu'il faille distinguer le droit à l'information, clairement consacré dans le RGPD, et le droit individuel à explication qui n'est pas visé dans le RGPD lui-même mais uniquement au considérant 71. Ce débat a peu été repris en France pour des raisons expliquées ci-après.

[14] CEPD, Lignes directrices sur la prise de décision individuelle automatisée et le profilage, WP 251, 6 févr. 2018, p. 21.

[15] B. Goodman and S. Flaxman, EU Regulations on Algorithmic Decision-Making and A « right to Explanation » (2016) : https://arxiv.org/abs/1606.08813; B. Goodman: A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection, 29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain; M. Hildebrandt, « The New Imbroglio – Living with Machine Algorithms », in The Art of Ethics in the Information Society (2016). S. Wachter, B. Mittelstadt, L. Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation?, *International Data Privacy Law*, à paraître. Andrew D. Selbst and Julia Powles, Meaningful Information and the Right to Explanation (Nov. 27, 2017). International Data Privacy Law, vol. 7(4), 233-242 (2017). Available at SSRN: https://ssrn.com/abstract=3039125. Voir aussi : L. Edwards et M. Veale, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, Duke Law & Technology Review, Forthcoming, ssrn : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855.

[16] Rappelons que l'article 15h) du règlement consacre le droit d'obtenir du responsable de traitement des informations sur l'existence d'une prise de décision automatisée, y compris un profilage, mais aussi « au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ».

- **Dispositions spécifiques à la France non directement liées au RGPD**

La loi précitée n° 2016-1321 *Pour une République numérique* (ci-après LRN) posait déjà des règles relatives à la transparence des décisions automatisées prises par l'administration[17].Elle contenait deux catégories de règles à l'égard des plateformes numériques, d'une part, et des administrations, d'autre part. La loi du 20 juin 2018 est venue modifier les secondes. La LRN a créé un nouvel article L. 311-3-1 du Code des relations entre le public et l'administration (CRPA), selon lequel : "*une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande*". Ce droit à l'information a été précisé par décret[18].

En outre, l'article 6 de la LRN prévoit que "*Sous réserve des secrets protégés, les administrations (...) publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles*".

La possibilité ainsi laissée de se prévaloir des secrets risque de vider de sa substance le principe de la diffusion de l'information. Dans son avis sur le projet de loi[19], le Conseil d'Etat avait d'ailleurs mis en garde contre une trop grande précision des informations données dans ce cadre à même de "*permettre à des usagers de se constituer un profil permettant de contourner les prescriptions qui seraient applicables aux opérateurs* ". Rappelons, en outre, que le considérant 63 encadre cette exception qui ne doit pas faire obstacle à la transparence[20].

- **Intégration de ces dispositions spécifiques dans le cadre de l'exception permise par le RGPD (art. 22§2b)**

Le législateur français a profité de la flexibilité offerte par l'article 22§2 b) du RGPD pour modifier ces dispositions et renforcer l'exception en droit national au droit de ne pas faire l'objet d'une décision automatisée. Le nouvel article 10 de la LIL précise que : "*2° Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du*

[17] J.-M. Pastor, Accès aux traitements algorithmiques utilisés par l'administration, *AJDA* 2017. 604.

[18] Un décret n° 2017-330 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique a été pris le 14 mars 2017 pour préciser l'obligation de communication. Il indique désormais à l'article R. 311-3-1-2 du code des relations entre le public et l'administration (CRPA) que **:** « l'administration communique à la personne faisant l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, à la demande de celle-ci, sous une forme intelligible et sous réserve de ne pas porter atteinte à des secrets protégés par la loi, les informations suivantes : le degré et le mode de contribution du traitement algorithmique à la prise de décision ; les données traitées et leurs sources ; les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ; les opérations effectuées par le traitement ». Ce droit d'accès peut s'exercer auprès de toute administration, y compris des collectivités territoriales, « *sous réserve de ne pas porter atteinte à des secrets protégés par la loi* » mais aussi dans les limites des restrictions et secrets énumérés au 2° de l'article L. 311-5 du CRPA. Enfin, le silence gardé par l'administration au terme du délai d'un mois vaut décision de rejet (CRPA, art. R. 311-12 et R. 311-13). du CRPA).

[19] Avis du 3 déc. 2015, n° 390741.

[20] Le considérant 63 du RGPD indique que le droit d'accès accordé à l'article 15 du RGPD « *ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Cependant, ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée* ».

chapitre Ier du titre Ier du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 8 de la présente loi. Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration". Par dérogation, "*aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel*".

Garanties pour les personnes concernées

S'agissant des mesures de sauvegarde des droits, libertés et légitimes intérêts des personnes concernées, la nouvelle LIL a prévu que « *pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard* ». À l'évidence, un droit individuel à explication est ici explicitement consacré en droit national, ce qui témoigne d'une sur-adaptation du RGPD par le législateur français.

- **Interprétation et garanties précisées par le Conseil constitutionnel**

Le Conseil constitutionnel a précisé que "c*es dispositions se bornent à autoriser l'administration à procéder à l'appréciation individuelle de la situation de l'administré, par le seul truchement d'un algorithme, en fonction des règles et critères définis à l'avance par le responsable du traitement. Elles n'ont ni pour objet ni pour effet d'autoriser l'administration à adopter des décisions sans base légale, ni à appliquer d'autres règles que celles du droit en vigueur. Il n'en résulte dès lors aucun abandon de compétence du pouvoir réglementaire*". [21]

En outre, le seul recours à un algorithme pour fonder une décision administrative individuelle est subordonné au respect de trois conditions :

1) d'une part, conformément à l'article L. 311-3-1 du CRPA, la décision administrative individuelle doit mentionner explicitement qu'elle a été adoptée sur le fondement d'un algorithme et les principales caractéristiques de mise en œuvre de ce dernier doivent être communiquées à la personne intéressée, à sa demande. Il en résulte que, lorsque les principes de fonctionnement d'un algorithme ne peuvent être communiqués sans porter atteinte à l'un des secrets ou intérêts énoncés au 2° de l'article L. 311-5 du code des relations entre le public et l'administration, aucune décision individuelle ne peut être prise sur le fondement exclusif de cet algorithme.

2) D'autre part, la décision administrative individuelle doit pouvoir faire l'objet de recours administratifs, conformément au chapitre premier du titre premier du livre quatrième du CRPA. L'administration sollicitée à l'occasion de ces recours est alors tenue de se prononcer sans pouvoir se fonder exclusivement sur l'algorithme. La décision administrative est, en outre, en cas de recours contentieux, placée sous le contrôle du

[21] CC décision n° 2018-765 DC du 12 juin 2018 (pts 69-72).

juge, qui est susceptible d'exiger de l'administration la communication des caractéristiques de l'algorithme.

3) Enfin, le recours exclusif à un algorithme est exclu si ce traitement porte sur l'une des données sensibles mentionnées au paragraphe I de l'article 8 de la LIL qui reprend l'article 9 du RGPD).

Par ailleurs, le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard. Il en résulte que ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement. Au vu de tous ces éléments, le Conseil constitutionnel a estimé que le législateur a défini des garanties appropriées pour la sauvegarde des droits et libertés des personnes soumises aux décisions administratives individuelles prises sur le fondement exclusif d'un algorithme.

Le Conseil constitutionnel a ainsi réduit les risques liés à l'utilisation d'un algorithme protégé par un secret ou un droit de propriété intellectuelle, lesquels secret et droit ne pourraient faire obstacle à la transparence. Il a également précisé les conditions d'un recours contre une décision prise sur le fondement d'un algorithme et le fait que l'explication doit être apportée par un humain et non par un algorithme et sous contrôle judiciaire. Cela suppose donc que le type d'algorithme utilisé soit maîtrisable et explicable, ce qui exclut les outils auto-apprenants dits *machine learning* qui "apprennent" et évoluent sans contrôle humain. Enfin, l'exclusion des données sensibles doit permettre d'éviter le risque d'une discrimination algorithmique fondée sur des données biaisées concernant par exemple les origines ethniques. Si ces dispositions vont dans le bon sens pour limiter les risques de discrimination amplement relevés par la doctrine, notamment aux États-Unis[22], de tels risques ne peuvent être totalement éliminés puisque d'autres facteurs en apparence objectifs peuvent conduire à des résultats biaisés et discriminants. Ces facteurs dits "proxies" peuvent être indirectement porteurs d'informations sensibles, comme par exemple le code postal qui révèle souvent un niveau social voire une origine ethnique.

- **Décisions de justice**

Par ailleurs, il faut remarquer que le début de l'article 10 de la LIL précise que "aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne". Cette disposition n'est pas nouvelle et était déjà consacrée par la loi n° 78-27 du 6 janvier 1978[23]. Une évaluation automatisée des

[22] Voir par exemple S. Barocas et A. Selbst, Big Data's Disparate Impact, 104 Cal. L. Rev. 3, 671-732 (2016); A. Chander, The Racist Algorithm?, 115 Mich. L. Rev. 6, 1023-1045 (2017).

[23] L'article 10 de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 prévoyait ainsi que : « *Aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ».

caractéristiques d'une personne conduisant à une décision ne peut être réalisée sur la seule base de cette évaluation. Cela suppose donc que d'autres critères soient pris en compte ou encore que d'autres moyens soient utilisés *a minima* en complément pour aider la prise de décision et non pour la prendre.

Question 7 : Comment le droit à l'effacement (art. 17) ou son prédécesseur dans la directive (art. 12, dir. 95/46/CE) a-t-il été appliqué au niveau national par les moteurs de recherche, les autorités nationales de contrôle et les juridictions ?

L'exercice du droit à l'effacement, tel qu'il ressort de l'article 17 du RGPD et 12 de la directive 95/46/CE, a connu une application renforcée depuis l'arrêt Google Spain de 2014 rendu par la Cour de justice de l'Union européenne.

En ce qui concerne le droit au déréférencement, il est possible de constater que le contentieux qui s'y rapporte met en évidence, à la fois, un renforcement de la protection des droits des personnes physiques et le détermination d'un équilibre entre les droits des personnes physiques et le droit à l'information.

Dans une délibération de 2016[24], la CNIL a infligé une sanction à Google de 100.000 euros pour avoir refusé de mettre en œuvre des demandes bien fondées de déréférencement de personnes physique sur l'ensemble des extensions de noms de domaine de son moteur de recherche. Les juridictions administratives ont adopté une position similaire sur le « droit au déréférencement» en imposant à des sociétés de répondre favorablement à des demandes de particuliers[25]. Au demeurant, plusieurs questions préjudicielles du Conseil d'Etat[26] sont pendantes devant la Cour de justice de l'Union européenne portant sur le champ du « droit au déréférencement»[27].

Les juridictions judiciaires connaissent des problématiques similaires. Elles tentent de trouver un juste équilibre entre la protection des droits des personnes et le droit à l'information. Ainsi, dans une ordonnance de référé du 19 décembre 2014 le TGI de Paris considère que la demanderesse « justifie de raisons prépondérantes et légitimes prévalant sur le droit à l'information »[28]. Or, dans une ordonnance de référé du 23 mars 2015, le TGI de Paris a cherché le juste équilibre entre les libertés d'expression et d'information, et la protection de la vie privée et des données personnelles[29]. Le 5 juin 2019, la Cour de cassation a décidé de surseoir à statuer dans une affaire portant sur le « droit au déréférencement », en attendant que le Cour de justice rende sa décision[30].

[24] Délibération n°2016-054 du 10 mars 2016 de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X.
[25] Conseil d'État, 10ème - 9ème chambres réunies, 19 juillet 2017, n° 399922.
[26] CE, 24 février 2017, Assemblée, n°s 391000, 393769, 399999, 401258, à publier au Lebon.
[27] CJUE, aff. C-507/17.
[28] TGI Paris, Ord., 24 novembre 2014, Marie-France M. / Google France et Google Inc.
[29] TGI Paris, Ord., 23 mars 2015, M. P ./ 20 Minutes France.
[30] Cass., Civ. 1ère, 5 juin 2019, n°18-14.675.

En ce qui concerne le droit à l'effacement, il existe également un contentieux portant sur cette question. Dans une ordonnance de 2018, le TGI de Grenoble a ordonné à la Banque Rhône-Alpes l'effacement total de toutes les données personnelles d'un client figurant par erreur dans un traitement dans le cadre de la loi américaine Foreign Account Tax Compliance Act (FACTA)[31]. Dans un arrêt du 12 mars 2019, la Cour d'appel de Grenoble a confirmé le jugement du TGI de Grenoble[32]. Pour la juridiction d'appel *: « la Banque Rhône Alpes ne peut se limiter à une rectification de l'erreur à compter de 2018, M. X. ayant un droit fondamental à ce que toutes les données le concernant soient définitivement effacées du ficher FATCA* ».

Question 8 : le RGPD permet aux Etats membres de légiférer pour concilier le droit à la protection des données avec la liberté d'expression (art. 85). Votre Etat a-t-il introduit une loi sur la base de l'article 85(2) du RGPD et, si oui, comment a-t-elle été interprétée et appliquée à cette date ?

Dès son origine en 1978 la LIL comportait une dérogation pour les traitements relatifs à la liberté d'expression qui a été modifié pour l'adapter à l'article 85 RGPD. L'article 80 de la LIL actuelle pose néanmoins trois séries de questionnements relatifs à sa conformité au RGPD:

- l'article 80 LIL reste assez vague en ce sens qu'il ne saurait à lui seul permettre véritablement de concilier le droit à la protection des données avec la liberté d'expression. Le parti pris de l'adaptation française a donc été de considérer que l'article 85§1 ne posait pas d'obligation spécifique d'adopter une loi sur ce sujet. L'article 80 se contente de dresser la liste des droits qui peuvent faire l'objet d'une dérogation pour les quatre finalités prévues par l'article 85§2 RGPD.
- l'adaptation continue comme précédemment à se concentrer essentiellement sur les traitements à des fins journalistiques et n'apporte aucune explication, définition relative aux autres finalités de traitement visés par l'article 85 RGPD (traitement à des fins d'expression universitaire, artistique ou littéraire).
- l'article 80 LIL n'est pas conforme à la lettre du RGPD dans la mesure où il maintient comme auparavant que les restrictions ne concerne que les traitements mis en œuvre "aux fins d'exercice *à titre professionnel* [mis en italique par nous], dans le respect des règles déontologiques de cette profession" alors que cette la référence au caractère professionnel n'existe pas à l'article 85 §2 du RGPD. Autrement dit, le droit français ne permet pas l'application de ces dérogations aux journalistes blogueurs ne disposant pas de carte professionnelle, voire les robots-journalistes. Pourtant, la CJUE a une approche large de la notion d'activité de journalisme incluant "*la divulgation au public, sous quelque moyen de transmission que ce soit, d'informations, d'opinions ou d'idées*."[33] L'approche française est bien plus centrée sur le journalisme et les médias classiques.

[31] TGI Grenoble, ordonnance de référé, 4 juillet 2018, M. X. / Banque Rhône-Alpes.

[32] CA Grenoble, 12 mars 2019, M. X. / Banque Rhône-Alpes.

[33] CJUE 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, aff. C-73/07, EU:C:2008:727, point 61 CJUE, ou encore CJUE, 14 février 2019, *Sergejs Buivids*, aff. C-345/17, ECLI:EU:C:2019:122, point 59.

Les dérogations permises pour les traitements relevant des quatre finalités de l'article 85 RGPD sont:

- des dérogations à l'interdiction de traitement de données sensibles (art. 9 RGPD) ou des traitements de condamnation (art. 10 RGPD)
- des dérogations au droit à l'information, au droit d'accès, mais aussi au droit de rectification et de limitation. En revanche, aucune limitation au droit d'opposition, ni au droit de portabilité, ni à l'article 22 RGPD n'ont été prévues.

L'article 80 de la LIL rappelle, par ailleurs, que la mise en œuvre d'une telle dérogation ne remet pas en cause les règles de droit interne relatives à la possibilité d'exercer un droit de réponse ou de se voir dédommager en cas d'atteinte à la vie privée ou à la réputation des personnes.

Au-delà de l'article 80 de la LIL:

- l'article 19 de LIL rappelle que la CNIL doit exercer ses pouvoirs notamment de contrôles en respectant « *le secret des sources des traitements journalistiques* ».
- En dehors de la LIL, la France a adopté plusieurs lois récemment visant à encadrer la liberté d'expression sur internet, telles que deux lois sur les *fake news*[34].La proposition de loi contre les discours de haine sur Internet actuellement en cours de discussions est au cœur d'un vif débat politique sur l'interdiction ou le maintien de l'anonymat sur Internet[35].

Question 9 : Identifiez l'autorité publique pertinente (ou les autorités) dans votre Etat membre. Précisez sa composition, le processus de nomination des membres et du personnel, ainsi que tout pouvoir additionnel ou des obligations que les autorités nationales de contrôle doivent respecter suivant leur loi nationale. Fournissez les détails pertinents concernant les données de mise en oeuvre ("enforcement record") sous le GDPR.

En France, l'autorité de contrôle est la Commission Nationale Informatique et Libertés (ci-après CNIL). Il s'agit d'une autorité administrative indépendante au sens de la loi n°2017-55 qui ne dispose pas de la personnalité juridique. La CNIL est composée d'un collège pluridisciplinaire de 18 membres dont 9 membres sont désignés par des organes politiques (Parlement, gouvernement). Le Président de la CNIL est nommé par le Président de la République, après validation de son candidat par les deux chambres du parlement. Mme Marie-Laure Denis est la présidente actuelle de la CNIL depuis janvier 2019. Le mandat des commissaires est de 5 ans ou, pour les parlementaires, d'une durée égale à leur mandat électif. Il n'existe aucune restriction d'âge, ni de renouvellement.

La CNIL est actuellement composée de:

- **4 parlementaires** (2 députés, 2 sénateurs)

[34] Loi organique n°2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, Loi n° 2018-120 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.
[35] cf. Voir dossier législatif http://www.assemblee-nationale.fr/dyn/15/dossiers/lutte_contre_haine_internet

- **2 membres du Conseil économique, social et environnemental**, élus par cette assemblée
- **6 représentants des hautes juridictions** (2 conseillers d'État, 2 conseillers à la Cour de cassation, 2 conseillers à la Cour des comptes) élus par leur assemblée générale respectives
- **5 personnalités qualifiées** désignées par le Président de l'Assemblée nationale (1 personnalité), le Président du Sénat (1 personnalité), en Conseil des ministres (3 personnalités). Ces personnes sont choisies pour leur connaissance du numérique et des questions touchant aux libertés individuelles.
- **Le Président de la CADA** (Commission d'accès aux documents administratifs),

En outre, le défenseur des droits y participe avec une voix consultative.

La CNIL est structurée de manière à assurer une séparation fonctionnelle entre sa mission de régulation et de contrôle. Elle comporte:

- **une formation plénière** dont la compétence principale est d'établir la doctrine de la CNIL (avis, lignes directrices, autorisation, certification, agrément, référentiel, code de conduite, clauses contractuelles, règlement intérieur etc.). Les décisions sont prises à la majorité absolue des membres présents. Un Commissaire du gouvernement assiste à la réunion plénière.
- **un bureau:** composé de la présidente et de deux Vice-Présidents. Le bureau peut, à la demande du président de la CNIL **rendre publique une mise en demeure** prise à l'encontre d'un responsable de traitement ne respectant pas les obligations issues de la LIL, il habilite les agents de la CNIL pouvant exercer des contrôles, etc.
- une **formation restreinte** à laquelle aucun membre du bureau ne participe. Cette formation restreinte est composée de 6 membres élus au sein du collège de la CNIL. La formation restreinte dispose de son propre président. Elle assure la fonction de contrôle de la CNIL (prise de mesures et sanctions).

En ce qui concerne ses missions, la CNIL assume des missions d'information, de recommandation et de contrôle. Quelques spécificités:

- La CNIL peut certifier "*des personnes et des produits, des systèmes de données ou de procédures aux fins de reconnaître qu'ils sont conformes au RGPD*", soit directement, soit par l'intermédiaire d'un organisme accrédité. Le champ de la certification va delà de ce qui a été accepté par le CEPD dans ses lignes directrices. Ce dernier refuse d'appliquer la certification aux personnes et notamment aux DPO. Pourtant, la CNIL vient de procéder à l'agrément de l'AFNOR pour certifier les DPO sur la base de référentiels[36].

[36] CNIL, délibération n° 2018-317 du 20 septembre 2018 *portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO)* et CNIL, délibération n° 2018-318 du 20 septembre 2018 *portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données* (DPO) et CNIL, délibération n° 2018-317 du 20 septembre 2018 *portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO*), *JORF* n°235 du 11 octobre 2018

- Doit sensibiliser les médiateurs de la consommation et les médiateurs publics
- Promouvoir l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement

Le budget de la CNIL en 2019 est de 18,5 millions €, nombre d'employés 215. La majorité des membres et du personnel de la CNIL ont un profil de juriste. Malgré une hausse de son budget, la CNIL considère qu'elle n'a pas suffisamment de moyens pour répondre à l'ensemble de ses missions.

Question 10 : Quelle stratégie pour le traitement des plaintes est prise par votre autorité nationale de contrôle et quelles contraintes, s'il y en a, la loi nationale prévoit-elle ?

La nouvelle LIL ne prévoit pas de dispositions particulières relatives au traitement des plaintes. En revanche, le chapitre VI du règlement intérieur de la CNIL prévoit des dispositions en la matière (art. 47 à 51).
Est considérée comme une plainte toute demande formée par une personne physique ou morale identifiée relative à des faits susceptibles d'être contraires aux textes dont l'application est confiée à la Commission. Les plaintes sont instruites par les services de la Commission (art. 47).
La Commission peut être saisie par voie postale ou électronique. Le plaignant indique son nom et ses coordonnées sur la plainte (art. 48).
Si la demande concerne l'exercice des droits d'accès, de rectification ou d'opposition prévus par la loi du 6 janvier 1978 modifiée, et que le plaignant n'a pas cherché à exercer ses droits directement auprès du responsable du traitement, les services de la Commission lui adressent un courrier l'informant des démarches qu'il lui appartient d'engager préalablement à toute saisine de la Commission (art. 49).
L'objet de la plainte est communiqué au responsable du traitement mis en cause, ou, le cas échéant, au correspondant, afin que celui-ci fournisse toutes les explications utiles. Ces échanges peuvent avoir lieu par tout moyen.
Par dérogation à l'alinéa précédent, l'objet de la plainte peut ne pas être communiqué au responsable de traitement si la Commission estime nécessaire de procéder à un contrôle sur place pour constater directement les faits rapportés.
Le prénom, le nom, la qualité et l'adresse administratives de l'agent chargé d'instruire la plainte sont indiqués au responsable de traitement, à moins que des motifs intéressant sa sécurité s'y opposent.
L'identité du plaignant n'est pas communiquée au responsable de traitement, à moins qu'elle soit indispensable au traitement de la plainte.
Tout courrier adressé au responsable de traitement mentionne le délai dans lequel le responsable de traitement est appelé à y répondre (art. 50).
Les plaignants sont informés de la clôture de leurs plaintes (art. 51).

et Délibération n°2019-092 du 4 juillet 2019 portant agrément d'AFNOR CERTIFICATION pour la certification des compétences du délégué à la protection des données (DPO).

Selon le rapport annuel de la CNIL, 11077 plaintes ont été déposées devant la CNIL en 2018, soit une augmentation de 32% liée à l'entrée en application du RGPD et à la sensibilisation qui l'a accompagnée. Ces plaintes ont fait l'objet de 6609 vérifications indirectes et 4264 demandes de droit d'accès indirect.

Question 11 : Comment les sanctions ont-elles été appliquées par l'autorité nationale de contrôle et quelles sanctions additionnelles ont-elle été adoptées en plus de celles explicitement prévues par le GDPR ?

Application des sanctions par la CNIL[37]

La CNIL dispose d'une chaîne répressive complète lui permettant de recevoir des signalements par des canaux divers, de réaliser des contrôles dont les suites peuvent aller de la clôture, à la mise en demeure ou à la sanction financière ou non. Dans certains cas, une **publicité** peut être décidée en fonction de la gravité des cas.

Le signalement peut provenir d'une plainte, autosaisine, faits signalés par la presse ou par le signalement des autres autorités nationales de contrôle des autres États membres.

La CNIL a le pouvoir d'effectuer des contrôles auprès de l'ensemble des organismes qui traitent des données à caractère personnel, soit les entreprises privées, associations ou encore organismes publics. Ces contrôles peuvent se dérouler sur place, sur pièces, sur audition ou en ligne.

À l'issue de contrôle ou plaintes, en cas de méconnaissance des dispositions du RGPD ou de la loi n° 78-17 de la part des responsables de traitement et sous-traitants, la formation restreinte de la CNIL peut prononcer des **sanctions** à l'égard des responsables de traitements qui ne respecteraient pas ces textes.

Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut :

- Prononcer un rappel à l'ordre ;
- Enjoindre de mettre le traitement en conformité, y compris sous astreinte ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte ;
- Prononcer une amende administrative (voir le RGPD).

Ces sanctions peuvent être rendues publiques[38].

À compter de la date de notification de la décision de la formation restreinte, l'organisme mis en cause dispose d'un délai de deux mois pour former un recours devant le Conseil d'État contre la décision de la CNIL.

Notons que le Président de la CNIL peut adresser à un responsable de traitement ou à un sous-traitant une **mise en demeure** de cesser un ou plusieurs manquement(s) constaté(s) au RGPD dans un délai fixé. Elle intervient après une plainte reçue par la CNIL ou un contrôle (en ligne

[37] Source : site de la CNIL.

[38] Pour des exemples, voir : https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil.

ou sur place) effectué auprès d'un organisme. Une mise en demeure n'est pas une sanction. Une mise en demeure peut-être publique[39]. Dans ce cas, le bureau de la CNIL, composé du Président et des vice-présidents, adopte une délibération dans laquelle il explique les raisons pour lesquelles il décide de rendre publique la mise en demeure. La mise en demeure publique fait l'objet d'un communiqué synthétique sur le site de la CNIL et la décision est publiée sur Légifrance. Celle-ci est anonymisée au bout de 2 ans, mais reste toujours accessible sur Légifrance. Si l'organisme s'est mis en conformité, la clôture de la mise en demeure est également rendue publique et anonymisée au bout de deux ans.

D'après le rapport annuel de la CNIL, 310 contrôles ont été effectués en 2018 avec 11 sanctions prononcées, dont 9 sanctions pécuniaires publiques, 1 avertissement non public et un non-lieu. Par ailleurs, 11077 plaintes ont été déposées, soit une augmentation de 32% et un chiffre record lié à l'entrée en application du RGPD.

Traditionnellement, la CNIL met l'accent sur ses missions pédagogique et d'accompagnement des responsables de traitement et sous-traitants dans le respect de la réglementation des données personnelles, plutôt que sur sa mission de sanction.

Sanctions additionnelles

S'agissant des sanctions additionnelles, l'article 84§1 du RGPD prévoit que "les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives".

Le paragraphe 2 précise que chaque État membre doit notifier à la Commission les dispositions légales qu'il adopte en vertu du paragraphe 1 au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant.

Les sanctions pénales en cas de manquement aux règles en matière de protection des données étaient déjà prévues en droit français avant l'adoption du RGPD et réprimées par les articles 226-16 à 226-24 du Code pénal (section 5 du chapitre VI du titre II du livre II du code pénal). Elles peuvent aller jusqu'à une amende de 300 000 euros et 5 ans d'emprisonnement.

L'article 41 de la loi n° 78-17 de la nouvelle LIL dispose que "le procureur de la République avise le président de la Commission nationale de l'informatique et des libertés de toutes les poursuites relatives aux infractions prévues par la section 5 du chapitre VI du titre II du livre II du code pénal et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'objet de l'audience de jugement par lettre recommandée adressée au moins dix jours avant cette date.

La juridiction d'instruction ou de jugement peut appeler le président de la Commission nationale de l'informatique et des libertés ou son représentant à déposer ses observations ou à les développer oralement à l'audience".

[39] Pour des exemples, voir : https://www.cnil.fr/fr/thematique/cnil/mises-en-demeure.

Ces dispositions permettent la coopération entre les autorités judiciaires et la CNIL, autorité administrative indépendante. Il faut cependant noter que si le montant des sanctions pénales est élevé, ces dispositions n'ont pratiquement pas été appliquées par les juridictions françaises.

Question 12 : Votre système légal prévoit-il historiquement une réparation des dommages pour les préjudices moraux (dans ce domaine ou dans d'autres) ? Si oui, comment de tels dommages sont-ils calculés ?

Le droit français prévoit effectivement une indemnisation des préjudices moraux avec l'octroi de dommages-intérêts. Généralement, les actions sont fondées sur les articles 1240 et 1241 nouveaux (anciennement 1382 et 1383) du code civil et non sur la LIL. Il découle des principes régissant responsabilité civile délictuelle que le préjudice doit être réparé dans son intégralité, sans toutefois excéder le montant de ce préjudice. Or, aucune disposition ne prévoit une sanction spécifique ou un montant en cas de préjudice moral. Une analyse de la jurisprudence montre qu'en raison du fait que le préjudice moral est difficilement quantifiable, la réparation de celui se fait selon une «logique rétributive et non réparatrice par volonté de dissuasion d'actes jugés antisociaux »[40]. Au demeurant, la réparation du préjudice moral repose sur une appréciation *in concreto* de la situation. Dès lors, pour obtenir réparation d'un tel préjudice, il convient de vérifier l'existence de conditions de mise en jeu de la responsabilité civile délictuelle, c'est-à-dire l'existence d'une faute, d'un dommage et d'un lien de causalité entre les deux.

Une analyse de la jurisprudence montre que les juridictions ne suivent pas de règles spécifiques pour établir le montant du préjudice moral qu'elles accordent à la victime. Ainsi, dans un arrêt du 7 mars 2017, la Cour d'appel de Paris a octroyé 5 000 € au titre de son préjudice moral et explique, dans sa décision que « la SAS Concepson a dévalorisé la valeur et l'intérêt de ce site par sa banalisation et lui a fait perdre sa visibilité sur internet »[41]. Or, la juridiction d'appel ne donne aucune explication sur le choix de ce montant.

Dans une autre affaire de 2011, la chambre correctionnelle du TGI de Clermont-Ferrand a condamné une ancienne salariée d'une société pour vol de données sur des fichiers clients et fournisseurs afin de les exploiter à son profit[42]. Au-delà de la condamnation pénale, la personne est également condamnée à payer la somme de 3000 € pour le préjudice moral. Dans cette affaire également, la juridiction ne donne aucune explication sur les modalités de calcul du montant octroyé.

Dans une affaire de 2018, le TGI de Paris a condamné une société pour avoir diffusé sur internet les photos représentant un modèle sans son autorisation écrite, ou son consentement implicite[43]. Pour ces atteintes au droit à l'image, elle devra lui verser 4 000 € en indemnisation de son préjudice moral. Là encore, les juges du fond n'ont pas justifié le montant de la somme attribuée pour ce titre.

[40] F. Gras, « L'indemnisation des atteintes à la vie privée », *LEGICOM*, vol. 20, no. 4, 1999, pp. 21-25.
[41] CA Paris, Pôle 5 – Ch. 1, 7 mars 2017, *Sound Strategy / Concepson*.
[42] TGI Clermont-Ferrand, Chambre correctionnelle Jugement du 26 septembre 2011, *Sociétés X. et Y. / Mme Rose*.
[43] TGI de Paris, 17e ch., 21 novembre 2018, *Mme X. / Sarl Denim*.

Dans une autre affaire de 2015, la Cour d'appel de Paris a également accordé des dommages-intérêts à un photographe pour la reproduction et la numérisation non autorisées de ses clichés d'objets mis aux enchères[44]. En outre, il obtient la somme de 100 000 € au titre du préjudice moral. L'intérêt de cette décision repose sur le fait que la Cour a opéré une analyse *in concreto* du dommage subit par le photographe et a analysé plusieurs milliers de photos pour établir l'acte de contrefaçon. D'ailleurs, sans établir une grille de calcul précis, la Cour fonde son analyse sur de nombreux éléments factuels pour déterminer le montant de la somme attribuée.

Question 13 : Votre Etat membre a-t-il introduit des mesures législatives pour faciliter des actions de représentation ? Quel rôle ont eu les ONG dans l'application de la protection des données personnelles dans votre Etat et y a-t-il des mouvements alternatifs émergents au niveau national (comme des syndicats ou coopérations relatifs à la protection des données personnelles) pour combattre de telles asymétries ?

En France, l'action de groupe en matière de protection des données à caractère personnel a été introduite en 2016 par la LRN. Elle ne concernait que l'action en cessation de manquement. Le nouvel article 37 III de la LIL y ajoute désormais une action en réparation. La France a ainsi utilisé la clause ouverte laissée par l'article 80 §1 du RGPD. Les organismes concernés sont les associations déclarées, les associations agréées, les organisations syndicales de salariés ou de fonctionnaires, (cf. art. 37 IV LIL) qui peuvent agir avec (art. 38 LIL) ou sans mandat de la personne concernée. (art. 80§2 RGPD)
L'article 37 de la LIL pose néanmoins plusieurs difficultés de conformité[45] au regard du RGPD:

- D'une part, il limite explicitement les personnes à qui un mandat peut être donné: Associations régulièrement déclarées depuis 5 ans. Cette limitation issue du droit antérieur français n'a pas été supprimée, alors qu'il n'existe aucune limite temporelle dans le RGPD, (sous-adaptation du droit français).
- D'autre part, le droit français permet une action de groupe en réparation y compris lorsque la personne concernée n'a pas donnée de mandat. Or, l'article 80 §2 RGPD n'évoque une telle possibilité que pour une action en cessation de violation. (Sur-adaptation du droit français)

Dans la pratique, l'association Que Choisir? [46] et l'association la Quadrature du net[47] ainsi que l'Open Internet Society France[48] sont les trois entités françaises à s'être emparées de ces possibilités d'actions collectives.

[44] CA Paris, pôle 5 – chambre 1, 10 mars 2015, Stéphane B. / Artnet France et Artnet Worldwide Corporation.
[45] cf. Alexia Pato The National Adaptation of Article 80 GDPR, Towards the Effective Private Enforcement of Collective Data Protection Rights accessible ici https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf
[46] https://www.quechoisir.org/action-ufc-que-choisir-vie-privee-donnees-personnelles-action-de-groupe-contre-google-n68403/: Première action de groupe devant le TGI de Paris en juin 2019
[47] https://gafam.laquadrature.net/ :première plainte collective (art. 77 RGPD) en mai 2018
[48] http://www.lefigaro.fr/secteur/high-tech/la-premiere-action-de-groupe-contre-facebook-en-france-sera-lancee-en-septembre-20190327

Notons, qu'au-delà de la multiplication des associations de DPO[49], un syndicat des DPO a vu le jour en France en avril 2019[50]. Sa vocation est de protéger la profession des DPO, notamment dans leurs possibles conflits avec leurs employeurs responsables de traitements ou sous-traitants et de favoriser les médiations.

Question 14 : On constate l'émergence d'autres autorités de contrôle (autorités de la concurrence, de la consommation, ou de nouvelles autorités proposées propres à la régulation de l'internet ou de l'IA) pour la régulation du traitement de données. De telles tendances sont-elles visibles dans votre Etat membre ? En particulier, les autorités nationales de contrôle coopèrent-elles avec d'autres régulateurs ou ombudsperson de manière formelle ou informelle ?

Le développement du numérique a forcé les autorités nationales à mettre en place une meilleure coordination et coopération entre les différents régulateurs. Le 24 juin 2019, plusieurs régulateurs (l'Autorité de la concurrence, l'Autorité des marchés financiers, l'Autorité de régulation des activités ferroviaires et routières, l'Autorité de régulation des communications électroniques et des postes, la Commission nationale de l'informatique et des libertés, la Commission de régulation de l'énergie et le Conseil supérieur de l'Audiovisuel) se sont réunis afin de mettre en place des mutualisations entre ces autorités[51]. Ces mutualisations portent sur différents thèmes tels que la commande publique, la gestion des connaissances et les ressources humaines. Cette rencontre a permis d'établir un rapport rendu public le 8 juillet 2019 sur leur approche commune de « la régulation par la donnée »[52]

L'objectif de cette coopération est de développer une régulation par la donnée afin de permettre aux différents régulateurs d'acquérir de nouvelles compétences en matière d'échange de données ou encore d'appropriation de nouvelles technologies. Il ressort du rapport que le développement des nouvelles technologies engendre pour les régulateurs "de nouveaux besoins en compétence technique, notamment en matière d'analyse de données et d'algorithmes mais également de stockage et gestion de gros volumes de données". Partant, les régulateurs doivent mettre en place des outils performants de traitement de la donnée. Il est fondamental pour les régulateurs "d'exploiter pleinement le potentiel des données" en développant des technologies communes ou certains outils. Enfin, cette coopération doit leur permettre d'utiliser et contrôler des nouvelles technologies comme le big data et/ou l'intelligence artificielle. En effet, ces technologies peuvent être utiles dans le traitement de données et la régulation de celles-ci.

[49] A côté de l'ancienne Association Française des Correspondants à la Protection des Données à Caractère Personnel (AFCPD), l' Association des Data Protection Officers créée en 2016, et l'Union des Data Protections Officers

[50] Syndicat Français des Experts en protection des données et Data Protection Officers.

[51] https://www.cnil.fr/fr/cooperations-entre-regulateurs

[52] https://www.cnil.fr/sites/default/files/atoms/files/note-aai-regulation-par-la-data-juil2019.pdf

Question 15 : La notion de "sécurité nationale" est-elle définie dans la loi nationale ou dans la pratique administrative ? Les autorités nationales ont-elles accepté d'appliquer la charte de l'UE pour la conservation des données à des fins de sécurité nationale (après les décisions Tele 2 et Watson) ?

En droit français la notion de « sécurité nationale » est définie, à l'art. L 1111-1 du code de la défense. « *La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter. L'ensemble des politiques publiques concourt à la sécurité nationale* ».
Les autorités françaises ont manifesté une grande réticence à l'application des décisions *Tele2 et Watson*. Elles considèrent que la conservation des données est nécessaire afin de pouvoir faire face aux menaces. Cette conviction relative à l'utilité de la conservation des données se reflète dans les questions préjudicielles posées par le Conseil d'Etat dans les affaires en cours initiés à l'échelle nationale par la Quadrature du Net (aff. C-511 et C-512/18). Ainsi, le CE demande à la CJUE de préciser si "*L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive [2002/58/CE] du 12 juillet 2002 (1), ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 du traité sur l'Union européenn*e?" Ces interrogations sont assez proches de celles qui sont à l'origine d'autres questions préjudicielles C-623/17 (International Privacy), C-520/18 (Ordre des barreaux francophone et germanophone).