

Les motifs de publicité des décisions de la Cnil

Quels sont les enseignements qui peuvent être tirés des délibérations de la Cnil rendues en 2017 alors qu'à la veille de l'entrée en application du RGPD, elle apparaît, plus que jamais, comme voulant s'inscrire dans une démarche moralisatrice, semblant se préparer progressivement au vent nouveau insufflé par la réforme européenne ?



Par Virginie BENSOUSSAN-BRULÉ

*Lexing Alain Bensoussan Avocats
Avocate à la Cour d'appel de Paris
Directrice du pôle Contentieux numérique*



Et Johanna CHAUVIN

*Lexing Alain Bensoussan Avocats
Avocate à la Cour d'appel de Paris
Doctorante à l'Université Paris Sud*

→ RLDI 5189

La décision de la Commission nationale de l'informatique et des libertés (Cnil) de sanctionner les sociétés Facebook Inc. et Facebook Ireland, le 27 avril 2017, en raison de manquements répétés à de multiples articles de la loi du 6 janvier 1978 modifiée⁽¹⁾, a fait parler d'elle. Les leaders des réseaux sociaux ont été condamnés au versement de 150 000 euros, soit l'amende la plus forte que la Commission était en mesure de prononcer à cette date. Cette décision regroupe un panel significatif de principes fondamentaux à respecter lors du traitement de données à caractère personnel et est, également, révélatrice de la tendance, empruntée ces derniers mois par la Commission, à la publication des sanctions prononcées.

Le développement constant des outils numériques et des nouvelles technologies, notamment par le biais de plates-formes en ligne, dans tous les domaines (réseaux sociaux, places commerciales, sites collaboratifs, sites de rencontres) est source de progrès et d'attrait pour leurs utilisateurs, mais est indéniablement le pendant d'une recrudescence des risques encourus en matière de traitement des données à caractère personnel, en fonction de l'usage qui est fait de ces dernières.

Leur collecte massive, par les géants du numérique mais également par les nouveaux entrants, laisse place à de sombres perspectives en matière de protection des utilisateurs. La compétition accrue, présente dans tous les secteurs d'innovation technologique, pousse les acteurs à chercher à se démarquer, et pour cela « tous les coups sont permis ». Contrepartie à la gratuité des outils proposés, les citoyens ne sont plus perçus que comme des marchandises et toute information alors semée est récupérée puis analysée par le biais d'algorithmes particulièrement sophistiqués.

(1) L. n° 78-17, 6 janv. 1978, « relative à l'informatique, aux fichiers et aux libertés », JO 7 janv., p. 227.

La finalité de ce processus ? Modéliser les habitudes des consommateurs et être en mesure de leur proposer des services prédictifs, cette fois-ci payants. Sortir du lot, être toujours plus innovants, voici le maître mot des plates-formes en ligne et des acteurs de l'internet aujourd'hui. Le progrès est trop rapide et la pression concurrentielle est double : être suffisamment attractifs pour les utilisateurs et suffisamment compétitifs pour résister aux nouveaux entrants. Autant d'éléments qui ne leur permettent pas de délaissier le moindre outil à disposition. Et pour ceux qui ne seraient pas en mesure de disposer de tels algorithmes, la solution a été rapidement trouvée : la commercialisation des données simples et isolées collectées auprès des grands groupes.

Les données à caractère personnel, mine d'or pour les entreprises, sont donc devenues, en parallèle, un véritable enjeu de société. Elles sont de plus en plus déposées sur des serveurs en ligne, volontairement, mais face à cette massification, de nouvelles revendications apparaissent de plus en plus fermement en matière de sécurité et de protection. C'est là tout le paradoxe de l'économie numérique. L'aisance des opérateurs à la consultation comme à la conservation et à la communication des données inquiète les utilisateurs de l'internet, ce dernier passant de vecteur de liberté à outil de sujétion.

Mais alors que cette crainte ne les conduit pas à cesser ou du moins à encadrer ou à restreindre leurs pratiques, c'est au législateur qu'il appartient d'intervenir, afin de poser les règles au marché de la commercialisation des big data. Le laisser-aller et la vision ultralibérale de l'internet n'ont pas permis d'éviter les comportements déviants et abusifs des opérateurs de plates-formes et l'ère de la régulation est apparue nécessaire. Le législateur, national comme européen, a rapidement compris les enjeux liés à la circulation de ces données et a su réagir. Il n'a eu de cesse de chercher à protéger davantage les intervenants non professionnels contre les atteintes portées à leurs droits et libertés en la matière. Néanmoins, des évolutions réglementaires ont été nécessaires au gré des progrès technologiques et mutations des pratiques des opérateurs.

En France, la loi « Informatique et libertés » a vu le jour dès le 6 janvier 1978⁽²⁾, encadrant et protégeant les données à caractère personnel. Mais l'impact de leur commercialisation étant croissant, le législateur européen s'est également intéressé au sujet, par le biais de différents instruments, venant transformer et adapter la législation française : la Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel⁽³⁾, la directive n° 95/46/CE « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel⁽⁴⁾ », la Charte des droits fondamentaux de l'Union européenne par le biais de son article 8⁽⁵⁾, la directive n° 2008/52/CE « sur certains aspects de la médiation en matière civile et commerciale⁽⁶⁾ ».

Jusqu'alors, les instruments régionaux utilisés laissaient une grande marge de manœuvre aux États et aux régulateurs nationaux : choix d'adhérer ou non à la Convention de 1981, liberté de moyens mis en œuvre dans le cadre de la transposition des directives ou de la mise en œuvre des principes généraux de la charte. Mais les évolutions numériques avaient toujours une longueur d'avance, obligeant les régulateurs à ne prendre souvent que des mesures correctives et non préventives.

Cette situation a été profondément bouleversée avec l'adoption du règlement (UE) n° 2016/679 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 », plus couramment dénommé « règlement général sur la protection des données »⁽⁷⁾. Adopté le 27 avril 2016, il sera applicable dès le 25 mai prochain et renforce considérablement la protection des données à caractère personnel. Le choix du règlement n'est, par ailleurs, pas anodin, puisque cet instrument est directement applicable et obligatoire dans l'ordre juridique des États membres. Les nouvelles mesures sont importantes et nombreuses, de quoi redonner confiance aux citoyens dans le contrôle de leurs données.

Certaines d'entre elles portent sur les sanctions administratives qui se voient fortement amplifiées, puisque les amendes imposées par les autorités de contrôle peuvent aller jusqu'à 10 000 000 d'euros ou 2 % du chiffre d'affaires annuel mondial total de l'exercice pré-

cedent, le montant le plus élevé étant retenu. Le montant de ces amendes pouvant être doublé (20 000 000 d'euros et 4 % du chiffre d'affaires) en cas de circonstances aggravantes. Le nouveau règlement européen procède donc à un durcissement des sanctions sans commune mesure avec ce qui était précédemment prévu.

Aujourd'hui, à la veille de l'entrée en application du RGPD, la Cnil apparaît, plus que jamais, comme voulant s'inscrire dans une démarche moralisatrice, semblant se préparer progressivement au vent nouveau insufflé par la réforme européenne. Cette sensibilisation accrue de l'autorité française pour la protection des données à caractère personnel se retranscrit dans les sanctions pécuniaires prononcées, l'exemple de la décision « Facebook » en témoigne. Mais cela transparait également, certes de manière moins perceptible, tant dans les sanctions complémentaires formulées, telles que la publicité des décisions de la formation restreinte, que dans les motifs qui y sont associés.

Lorsque l'on étudie les délibérations de la Cnil sur l'année 2017, la systématisation de la publicité des décisions est tout à fait palpable. Étant précisé à titre liminaire que par décisions sont entendues celles relatives aux sanctions pécuniaires, mais également aux mises en demeure et aux avertissements. En effet, depuis un an, parmi l'ensemble de ces décisions, il est possible de mentionner trois avertissements qui n'ont pas fait l'objet de publication⁽⁸⁾, mais la pratique de la Cnil tend à l'assortiment de sanctions complémentaires, pour les amendes comme pour les avertissements, tendance qui s'étend jusqu'aux mises en demeure.

Or, si le pouvoir de sanction de la Cnil est précisément encadré par la loi « Informatique et libertés » (I.), il n'en est pas de même de sa prérogative en matière de publicité des sanctions. Initiée par la loi du 29 mars 2011, « relative au Défenseur des droits »⁽⁹⁾, la formation restreinte de la Cnil peut désormais rendre publiques ses délibérations sans avoir à avancer pour motif la mauvaise foi de l'organisme concerné. Néanmoins, si la pratique n'est pas strictement circonscrite, cette sanction complémentaire doit être motivée et proportionnelle, et en matière de motifs, la Cnil n'hésite pas à user d'un éventail particulièrement large (II.).

I. – LA SANCTION DES MANQUEMENTS À LA LOI « INFORMATIQUE ET LIBERTÉS »

Le législateur français a souhaité initier une réglementation « Informatique et libertés » suffisamment étendue pour permettre la prise en compte de l'ensemble des traitements de données à caractère personnel envisageable (A.). Néanmoins, si le champ d'application de la loi du 6 janvier 1978 semble ne souffrir d'aucune exception, la sanction de ses violations a nécessairement dû être encadrée. Ainsi, la Cnil bénéficie d'une palette conséquente d'outils répressifs mis à sa disposition, mais dont l'usage doit être motivé et contrôlé par le Conseil d'État (B.).

(2) L. n° 78-17 précitée.

(3) Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel du 28 janvier 1981, Série des traités européens n° 108.

(4) Parlement européen et Conseil, Dir. n° 95/46/CE, 24 oct. 1995, « relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données », JOCE 23 nov., n° L 281, p. 31-50.

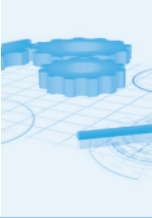
(5) Charte des droits fondamentaux de l'Union européenne, JOCE 18 déc. 2000, n° C 346, p. 1-22.

(6) Parlement européen et Conseil, Dir. n° 2008/52/CE, 21 mai 2008, « sur certains aspects de la médiation en matière civile et commerciale », JOCE 24 mai, n° L 136, p. 3-8.

(7) Parlement européen et Conseil, Règl. (UE) n° 2016/679, 27 avr. 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) », JOUE 4 mai, n° L 119, p. 1-88.

(8) Un avertissement du 13 septembre 2016 relatif à une société de courtage en assurance, un avertissement du 3 novembre 2016 relatif à une société de vente à distance et un avertissement du 15 décembre 2016 relatif à une association.

(9) Loi organique n° 2011-333, 29 mars 2011 « relative au Défenseur des droits », JO 30 mars, p. 5497.



A. – Le champ d'application de la loi « Informatique et libertés »

Afin de déterminer l'applicabilité de la loi « Informatique et libertés », la Cnil propose, dans un encart « Suis-je concerné ? »⁽¹⁰⁾, une infographie listant quatre interrogations qu'il convient de se poser successivement. Ainsi, dès lors qu'il est question de données à caractère personnel, soumises à traitement, hors d'un cadre d'activités exclusivement personnelles et que le responsable et/ou les moyens du traitement sont situés sur le territoire français, la loi du 6 janvier 1978 sera applicable.

Ces questions permettent donc d'identifier les trois critères cumulatifs à remplir pour que le traitement de données tombe dans le champ de la loi « Informatique et libertés » : un critère matériel, fonctionnel et géographique. Les deux premiers répondent finalement à la condition de l'identification de données à caractère personnel soumises à traitement (1^o) et le troisième critère permet de s'interroger sur la participation de l'organisme aux traitements concernés (2^o).

1^o Des données à caractère personnel soumises à traitement

La loi « Informatique et libertés » prévoit deux éléments pour que des données collectées entrent dans son champ d'application. Ces données doivent être considérées comme ayant un caractère personnel et être traitées en dehors du cadre d'une activité personnelle.

Un critère matériel : des données à caractère personnel. Le critère matériel est posé à l'article 2, alinéa 2, de la loi « Informatique et libertés » et dispose que « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».

La solution adoptée par le législateur se veut particulièrement extensive dans la mesure où elle ne se limite pas à l'identification directe de la personne concernée (par nom, prénom ou photographie), mais prend également en compte son identification potentielle. Ainsi, dès lors qu'un identifiant numérique permet de remonter jusqu'à l'identification d'une personne il sera considéré comme une donnée à caractère personnel. Tel sera le cas, notamment, du numéro de sécurité sociale (numéro personnel unique par excellence), d'un numéro de téléphone (qui renvoie au détenteur de la ligne), d'une plaque d'immatriculation (qui permet d'avoir connaissance du propriétaire du véhicule via la carte grise), mais également d'un numéro de dossier ou de contrat.

Seront également pris en compte les éléments du corps humain et données biométriques tels que l'ADN ou les empreintes digitales, ainsi que les recoupements d'informations qui permettront d'identifier indirectement une personne via plusieurs canaux. Dès lors qu'un lien peut être fait avec une personne physique, les données qui ont permis ou pourraient permettre cette identification seront considérées comme personnelles.

Il convient de préciser que la loi « Informatique et libertés » ne restreint pas son champ d'application aux données strictement privées. Seront ainsi considérées comme ayant un caractère personnel les données également professionnelles (des éléments propres à la formation professionnelle individuelle, un numéro de badge d'accès au lieu de travail, par exemple), financières (avis d'imposition, numéro de compte bancaire, factures, par exemple) ou patrimoniales (les adresses immobilières, la taxe foncière, par exemple).

L'article 2, alinéa 2, de la loi « Informatique et libertés » poursuit comme tel : « Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. » Par conséquent, peu importe la manière dont le responsable du traitement aura eu accès à ces données, et donc peu importe que ces dernières soient publiques ou non. La lettre de l'article prend, en effet, en compte les données auxquelles peut avoir accès le responsable du traitement au sens large. Cette notion d'accessibilité fait directement référence à la publication volontaire ou non de certaines informations. Ainsi, un profil renseigné sur un réseau social sera composé de données personnelles, bien que celles-ci aient été renseignées par leur titulaire et rendues publiques de son plein gré. Il en est de même de la publication de curriculum vitae en ligne ou de la publication d'informations sur une plate-forme d'échange de biens ou services CtoC.

Le RGPD retient plus ou moins une définition similaire, puisqu'il entend par donnée à caractère personnel, à son article 4, « toute information se rapportant à une personne physique identifiée ou identifiable » ; la potentialité de l'identification est donc conservée par la réglementation européenne.

Le texte poursuit en précisant qu'est « réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Les voies d'identification d'une personne sont diverses et non exhaustives, ce qui se situe dans le prolongement de la vocation particulièrement large de la réglementation des données personnelles.

Pour conclure, la seule exception au champ de l'article 2 de la loi « Informatique et libertés » sera les données soumises à anonymisation, à condition néanmoins que cette dernière soit complète et qu'il ne puisse pas être procédé à une restauration des données initiales, laquelle permettrait une quelconque identification.

Un critère fonctionnel : un traitement opéré en dehors du cadre privé. L'article 2, alinéa 3, de la loi « Informatique et libertés » dispose que « constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment 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 ».

(10) <<https://www.cnil.fr/fr/informatique-et-libertes-suis-je-concerne>>.

La définition retenue se veut, elle aussi, particulièrement extensive, d'autant que la liste de traitements énoncée n'est pas exhaustive. Ainsi, la loi vise les traitements informatiques de données (tels que les bases de données, les fichiers bureautiques, les sites internet), mais les traitements manuels ne sont pas écartés pour autant de son champ d'application. En effet, l'alinéa premier de l'article 2 précise que la loi « s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles ».

Sont donc concernés les traitements de « fichiers de données à caractère personnel », lesquels sont définis à l'article 2, alinéa 3, comme « tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés ». En conséquence, les traitements de données papier entrent également dans le champ d'application de la loi (tels que des bulletins de participation à des jeux concours, des annuaires téléphoniques) dès lors qu'ils ne figurent pas encore dans un fichier informatique, mais qu'ils sont seulement appelés à l'être. Or la simple numérisation d'un fichier papier constitue un fichier informatisé.

Par ailleurs, la loi ne procède à aucune distinction entre la création, la modification ou la suppression de fichiers de données à caractère personnel et leur simple consultation ou visualisation. Ainsi, dès lors qu'il sera seulement possible d'avoir accès à ces fichiers, il s'agira d'un traitement de données personnelles. Sur ce point encore le législateur a voulu étendre au possible le champ d'application de la loi puisqu'en prenant en compte la notion d'accès, il brasse un nombre bien plus conséquent de situations que s'il se limitait à une action positive sur ces données.

L'article 4 du RGPD opère une définition tout à fait semblable de la notion de « traitement », car s'il énumère une typologie plus conséquente de traitements, celle-ci n'est pas exhaustive pour autant.

En outre, l'alinéa premier de l'article 2 de la loi « Informatique et libertés » précise que constitue une exception les « traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles ». Le critère fonctionnel d'applicabilité de la loi est donc précisé en ces termes. Néanmoins, il convient d'être attentif à la définition du concept d'« exclusivement personnelles ». Si la Cnil ne l'a pas défini, le considérant 12 de la loi du 6 janvier 1978 précise à titre d'exclusion les « activités exclusivement personnelles ou domestiques, telles la correspondance et la tenue de répertoires d'adresses ».

Une analyse rapide voudrait opposer les notions de « personnel » et de « professionnel ». Mais le législateur a spécifiquement rattaché l'idée d'exclusivité, ce qui permet de ne pas se restreindre au domaine professionnel. En effet, avec le développement croissant des réseaux sociaux, de nombreuses données à caractère personnel, mises en ligne, dépassent largement le cadre domestique et désormais strictement personnel. Néanmoins, il est vrai que les traitements les plus courants et les plus aisément admis sont ceux effectués dans le cadre des activités professionnelles, traitements qui ne laissent que peu ou pas de place au doute quant à l'applicabilité de la loi.

L'article 2 du RGPD prévoit, d'ailleurs, la même exception en ces termes : « Le présent règlement ne s'applique pas au traitement

de données à caractère personnel effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique. »

Finalement, rares sont les données qui ne sont pas prises en compte par la loi « Informatique et libertés », et ce dans un souci d'une meilleure protection des personnes concernées. La notion de « donnée à caractère personnel », comme celle de « traitement » sont admises dans leur conception la plus extensive possible, tout comme le troisième critère d'applicabilité de la loi, le critère géographique.

2°/ La participation de l'établissement aux traitements concernés

La loi du 6 janvier 1978 s'applique aux traitements de données à caractère personnel dont le responsable et/ou les moyens usités pour y procéder sont situés sur le territoire français. Cette règle de territorialité constitue le droit commun de nombreuses réglementations nationales, néanmoins, dans le cadre « Informatique et libertés », elle impose d'être en mesure d'identifier le responsable du traitement.

L'identification du responsable du traitement. Le responsable du traitement de données à caractère personnel est défini à l'article 3-I de la loi « Informatique et libertés » qui prévoit qu'il s'agit, « sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, [de] la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ». Le RGPD encadre de manière similaire cette notion.

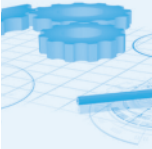
Or, la législation nationale comme régionale opère une distinction entre responsable du traitement et sous-traitant, lequel intervient dans le traitement des données à caractère personnel, mais selon des critères fixés par le responsable initial. Ce dernier ne peut, ainsi, se dégager des obligations qui lui incombent sur seule invocation de la mise en place d'une relation de sous-traitance. En effet, dès lors que le traitement est effectué pour son compte⁽¹¹⁾, il ne pourra invoquer sa faible latitude d'action pour s'exonérer de sa responsabilité ; *a contrario*, il lui revient de mettre en œuvre tous les moyens dont il dispose pour garder le contrôle de la situation et prévenir les éventuelles fuites ou dégradations de données⁽¹²⁾. Tout au plus, les différents intervenants se verront qualifiés de coresponsables de traitement.

Lorsque le responsable du traitement est en mesure d'être identifié, il convient de procéder à la vérification du critère géographique d'applicabilité de la loi « Informatique et libertés », prévu à son article 5-I. Deux options permettent de faire entrer un traitement de données à caractère personnel dans le cadre de la législation française : l'établissement du responsable du traitement sur le territoire français ou le recours à des moyens de traitement de données sur le territoire français.

L'existence d'un établissement en France. Dès lors que le responsable du traitement est situé sur le territoire français la législation

(11) Loi « Informatique et libertés », 6 janv. 1978 modifiée, art. 35 ; règlement général sur la protection des données, art. 4-8.

(12) Loi « Informatique et libertés », 6 janv. 1978 modifiée, art. 34.



nationale sera applicable. Or, l'article 5-I-1) de la loi « Informatique et libertés » précise que « *le responsable du traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, est considéré comme établi* ». Ainsi, il n'est pas fait de distinction en fonction du siège social ou des filiales d'une entité, le législateur ayant, à nouveau, cherché à étendre au maximum le champ d'application de la loi française.

La décision « Facebook » du 27 avril 2017⁽¹³⁾ précise notamment certains éléments qui permettront de caractériser l'existence d'un établissement en France. Constitueront ainsi des indices le fait d'être immatriculé au registre du commerce et des sociétés en France, de proposer des services en France, d'avoir un siège social en France et de fournir des services marketing en France. Il est, par ailleurs, fait mention que la qualité de sous-traitant sera sans impact sur la qualification d'établissement stable exerçant une activité réelle et effective.

La logique retenue par le RGPD est identique, néanmoins, elle se veut, du moins explicitement, plus étendue. En effet, celui-ci aura vocation à s'appliquer « *au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement du responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union* »⁽¹⁴⁾. Le législateur européen a précisément mentionné l'ensemble des établissements concernés par le traitement des données à caractère personnel, qu'il s'agisse de ceux du responsable comme de ceux du sous-traitant. Ainsi, si cette idée transparaît de l'interprétation de la loi française, la réglementation européenne est plus complète et ne laissera que peu de place aux doutes et questions préjudicielles sur ce point.

Le recours à des moyens de traitement en France. La territorialité des moyens de traitements utilisés par le responsable est le second critère géographique alternatif visé par la loi française. L'article 5-I-2) dispose, en effet, que seront concernés par la réglementation « Informatique et libertés » les traitements « *dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne* ».

Le législateur n'ayant pas souhaité désigner précisément les moyens entendus, l'interprétation de cet article est extensive et y inclut tant les moyens humains que matériels. La décision « Facebook » du 27 avril 2017⁽¹⁵⁾ est encore source d'information sur l'interprétation à donner à cette notion, laquelle semble particulièrement vaste. En effet, le fait d'assurer la promotion d'espaces publicitaires de l'entreprise participe à en assurer la viabilité, et dès lors que cette activité est la contrepartie de la gratuité du service de réseau social proposé, elle est « *indissociable du traitement des*

données des utilisateurs et notamment de leur combinaison ». Ainsi, en contribuant à la perception de revenus publicitaires, la société Facebook France participait, « *dans le cadre de ses activités, aux traitements en cause* ».

Néanmoins, une première restriction dans le champ d'application de la loi « Informatique et libertés » transparaît dans l'article 5-I-2), car géographiquement sont exclus les moyens utilisés par un responsable du traitement situé sur le territoire français (qui se verra appliquer l'article 5-I-1), mais également par un responsable situé sur le territoire « *d'un autre État membre de la Communauté européenne* ». Si la notion de « *Communauté européenne* » a disparu avec l'entrée en vigueur du traité de Lisbonne le 1^{er} décembre 2009, il semble que cette exception se reporte sur l'Union européenne qui l'a remplacée.

Toutefois, cette exclusion du territoire de l'Union dans le champ d'application de la loi « Informatique et libertés » se comprend dès lors que le législateur a souhaité ne pas créer de conflit de lois inutile. Si dans un pays tiers il n'est pas certain de retrouver une protection analogue des données à caractère personnel, la loi française est notamment issue de l'interprétation de plusieurs directives européennes, dont la directive n° 95/46/CE du 24 octobre 1995⁽¹⁶⁾, lesquelles sont applicables à l'ensemble des États membres. Ainsi, sauf défaut majeur d'interprétation, l'ensemble des États membres de l'Union devrait posséder une réglementation comparable en la matière.

Également dans un souci de prévenir d'éventuels conflits de lois et de ne pas surcharger le régulateur français de missions inutiles, sont exclus du champ d'application de la loi du 6 janvier 1978 les traitements ne faisant que transiter par la France. En effet, ces derniers n'auront que peu d'impact sur le territoire, et en cas de conflit entre deux réglementations, celle du territoire d'exploitation aura plus de légitimité que celle du territoire de transit (d'autant que plusieurs États, et donc plusieurs législations, peuvent être concernés par un transit de données).

Quant au règlement européen, s'il ne vise pas spécifiquement des moyens de traitement sur le sol européen dans le cadre de son champ d'application territorial, cette idée se comprend néanmoins implicitement des procédés décrits à son article 3-2. Ce dernier mentionne que, dès lors que des personnes se trouvant sur le territoire de l'Union sont concernées par le traitement de données à caractère personnel, le règlement s'appliquera même si le responsable où le sous-traitant sont situés à l'étranger, si les activités de traitement sont liées « *à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* ».

Le champ d'application de la loi « Informatique et libertés » est donc particulièrement large et réunit en son sein un panel de situations très étendu. La réglementation européenne s'inscrit dans cette volonté de protection des individus face au traitement de leurs données à caractère personnel. Les législateurs nationaux et européens ont précisé spécifiquement et exhaustivement les

(13) Cnil, délibération de la formation restreinte n° SAN-2017-006 du 27 avril 2017, prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland.

(14) RGPD, art. 3.

(15) Cnil, délibération de la formation restreinte n° SAN-2017-006 du 27 avril 2017 précitée.

(16) Voir *supra*.

exceptions au champ d'application matériel de leur réglementation, faisant finalement entrer toute situation non visée. Quant au champ d'application territorial, il est si étendu que les dispositions sur la protection des données personnelles s'appliqueront dès lors qu'un élément de rattachement sera invocable, qu'il s'agisse de l'établissement des responsables du traitement ou sous-traitants, ou des moyens qu'ils utilisent.

La décision « Facebook » du 27 avril 2017⁽¹⁷⁾ est particulièrement instructive sur l'interprétation, par la Cnil, de la loi « Informatique et libertés » et de la directive n° 95/46/CE qu'elle transpose. Elle précise notamment que « *le droit applicable d'un État membre dépend de deux conditions cumulatives : l'existence d'un établissement du responsable de traitement sur le territoire d'un État membre et la mise en œuvre du traitement de données dans le cadre des activités de cet établissement* ». Par ailleurs, la Cnil n'a pas hésité à étayer son raisonnement par l'interprétation par la Cour de justice de ces deux conditions.

Or, si le législateur a souhaité étendre l'application de la loi « Informatique et libertés », il en a fait de même avec le pouvoir de sanction du régulateur mis en place, la Cnil.

B. – Le pouvoir de sanction de la Cnil, une compétence étendue

La Cnil a été dotée de différentes prérogatives par l'article 11 de la loi du 6 janvier 1978. S'il est possible de les résumer en quatre catégories – informer et protéger, accompagner et conseiller, contrôler et sanctionner, anticiper – c'est évidemment celles relatives au contrôle et à la sanction qui sont le plus craintes des responsables du traitement. Du moins, si elles ne le sont pas encore, elles le deviendront très vite avec l'application prochaine du règlement général sur la protection des données qui vient considérablement renforcer ses pouvoirs en la matière.

La Cnil est, ainsi, en mesure de sanctionner l'ensemble des manquements à la réglementation « Informatique et libertés » constatés dès lors que le délai imparti aux entreprises responsables du traitement pour les corriger a été échu (1%). Si cette sanction recouvre aujourd'hui plusieurs formes, elle prendra souvent celle d'une amende pécuniaire, de plus en plus assortie d'une publicité de la décision afférente (2%).

1°/ La sanction des manquements constatés au-delà du délai imparti

Lors de ses contrôles, si elle note des défaillances dans le traitement de données à caractère personnel, la Cnil peut entamer une procédure de constatation des manquements. Au-delà du délai octroyé au responsable du traitement pour se mettre en conformité, elle sera en mesure de sanctionner les comportements fautifs.

La procédure de constatation des manquements. La Cnil établit un programme annuel de contrôle sur certaines problématiques identifiées, contrôles largement complétés, car en 2016 la part afférente au programme annuel n'était que de 25 %. D'autres

contrôles, à hauteur de 20 %, ont été diligentés pour instruire les plaintes reçues par la Cnil et d'autres encore ont été spécifiquement dédiés à la vérification des dispositifs de vidéosurveillance et de vidéoprotection (20 % également). La part de contrôles la plus importante a concerné les suites données à une procédure déjà entamée, qu'il s'agisse de courriers d'observation, de mises en demeure ou de sanctions, part ayant représenté 35 % de la masse totale de contrôles⁽¹⁸⁾.

C'est l'article 44 de la loi du 6 janvier 1978 qui encadre la procédure de contrôle initiée par la Cnil. Il convient de noter que la loi comme le régulateur se sont mis à jour des technologies informatiques, car les contrôles peuvent se faire sur place, sur pièce, sur audition, et désormais également en ligne depuis le 17 mars 2014⁽¹⁹⁾. Ces différentes mesures ont pour finalité de vérifier notamment la bonne application de la loi « Informatique et libertés », et d'ici au 25 mai 2018 également celle du règlement général sur la protection des données.

L'article 21 précise également que « *les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la Commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche* ». La seule exception à cette coopération concerne finalement les limites relatives à l'exercice du secret professionnel. Cet article revêt toute son importance, dans la mesure où le degré de collaboration des responsables contrôlés sera pris en compte lors des éventuelles sanctions. En effet, toute entrave constitue déjà, en soi, un manquement à la loi « Informatique et libertés », appréhendé à l'article 51⁽²⁰⁾.

Les articles 60 à 62 du règlement général sur la protection des données viendront compléter la législation française en ce qu'ils prévoient une assistance mutuelle entre autorités et la possibilité d'avoir recours à des opérations conjointes de contrôle, permettant de prendre en compte des activités transfrontières et de les analyser dans leur globalité.

À l'issue du contrôle effectué, un procès-verbal des vérifications et visites menées est établi. L'article 44 de la loi du 6 janvier 1978 précise, en outre, qu'il « *est dressé* » contradictoirement lorsque « *les vérifications et visites sont effectuées sur place ou sur convocation* ». Dans le cas d'un contrôle en ligne, le procès-verbal est envoyé au responsable du site qui a fait l'objet du contrôle.

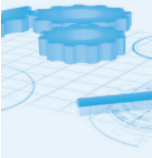
La Cnil est, ensuite, en mesure de demander au responsable identifié la communication de diverses pièces complémentaires. Après analyse, s'il s'avère qu'aucun manquement n'a été relevé, le contrôle fait l'objet d'une clôture, éventuellement assortie de recommandations. En revanche, si des manquements ont été constatés, le dossier est transmis à la formation restreinte de la Commission, en vue de suivre une procédure contentieuse.

(17) Cnil, délibération de la formation restreinte n° SAN-2017-006 du 27 avril 2017 précitée.

(18) <<https://www.cnil.fr/fr/programme-des-contrôles-2016-quelles-thématiques-prioritaires>>.

(19) L. n° 2014-344, 17 mars 2014, « relative à la consommation », JO 18 mars, p. 5400.

(20) Voir *infra*.



Une mise en demeure de faire cesser les violations à la loi « Informatique et libertés » sera préalablement envoyée au responsable du traitement, mise en demeure assortie d'un délai imparti pour ce faire. L'article 45 de la loi prévoit qu'en cas d'extrême urgence, ce délai peut être ramené à 24 heures. La mise en demeure rappelle les faits propres à l'affaire, mais surtout les manquements constatés à la loi « Informatique et libertés ». Le délai dont dispose le responsable du traitement pour mettre fin à son comportement y est précisé, ainsi que le détail des mesures à adopter. Il convient d'ajouter que ces mises en demeure peuvent être suivies d'une délibération de la Cnil décidant de les rendre publiques. C'est notamment le sort qui a été réservé aux sociétés Microsoft Corporation et W.M.G., respectivement le 12 juillet⁽²¹⁾ et le 3 octobre 2016⁽²²⁾.

Si à l'issue du délai octroyé la société visée s'est conformée à la mise en demeure, la procédure sera close et un courrier sera envoyé en ce sens. Étant mentionné que, si la mise en demeure avait été initialement publiée, la décision de clôture suivra le même sort⁽²³⁾. Ont, ainsi, notamment, été publiées les décisions du 28 juillet 2016, « relative à la clôture de la mise en demeure n° 2015-058 à l'égard de la société X » et du 14 octobre 2016, « relative à la clôture de la mise en demeure n° 2015-061 à l'égard de la société X ». Dans les décisions initiales de mise en demeure les sociétés concernées étaient déjà anonymisées, il est donc possible d'en déduire que si le nom de la société apparaît dans la mise en demeure, il sera conservé dans la décision de clôture.

À l'inverse, en cas de non-conformité à la mise en demeure, un rapporteur sera désigné et « pourra demander à la formation restreinte de la Commission de prononcer l'une des sanctions prévues par l'article 45 de la loi du 6 janvier 1978 »⁽²⁴⁾.

L'indifférence de la conformité avant audience. La Cnil se veut particulièrement sévère à l'égard des violations de la loi « Informatique et libertés ». Ainsi, dès lors que la procédure contentieuse est entamée, le rapporteur et la formation restreinte vont jusqu'au bout, peu importe les efforts fournis par le mis en cause pour faire cesser sa violation. Rappelons que le responsable du traitement dispose d'un certain délai pour faire cesser ces manquements. À son échéance, les conséquences sont binaires : le manquement a cessé, la procédure est close ; l'ensemble des consignes de la Cnil n'a pas été suivi, la procédure se poursuit jusqu'à la sanction.

Or, le monde ne fonctionne pas comme les systèmes informatiques et ne s'arrête pas à une succession de 0 et de 1. Il est donc possible que la société mise en cause face preuve d'une particu-

lière coopération au moment du contrôle et tout au long de la procédure⁽²⁵⁾. Il arrive également que la société ait fait preuve d'une grande réactivité dans la résolution de la violation de données et prenne certaines initiatives afin de renforcer la sécurité des traitements⁽²⁶⁾. Il arrive encore que les manquements soient corrigés au jour de l'audience mais ne l'étaient pas à l'issue du délai imparti par la Cnil⁽²⁷⁾. Peu importe pour l'autorité, dès lors que les manquements n'ont pas tous été corrigés à la date fixée, il ne sera pas possible d'échapper à la sanction.

Ce raisonnement du régulateur est particulièrement strict dans la mesure où les éventuels remèdes ne permettent pas d'alléger la sanction. Si le Parti socialiste n'avait écopé que d'un avertissement, les autres sociétés ayant malgré tout coopéré avec la Cnil se sont vues sanctionnées par des amendes administratives au même titre que des sociétés n'ayant fait aucun effort pour respecter la réglementation « Informatique et libertés », et ce parfois lourdement alors même qu'aucune extraction massive de données n'était relevée. À ce titre la décision à l'encontre de la société Hertz France est particulièrement lourde, car les défauts de sécurité étaient ceux du sous-traitant, les remèdes ont été apportés dès le signalement de la part de la Cnil, des audits spontanés de sécurité ont été mis en place et aucune extraction massive de données n'a été constatée, mais la société s'est vue sanctionnée à hauteur de 40 000 euros avec publicité de la décision de délibération⁽²⁸⁾.

La Cnil semble, néanmoins, faire preuve de moins de sévérité dans sa décision du 16 novembre 2017, prise à l'encontre de la société Web Éditions, dans la mesure où elle a su tenir compte des « mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées » – notamment sa

(21) Cnil, décision n° 2016-058 du 30 juin 2016 mettant en demeure la société Microsoft Corporation, assortie de la délibération n° 2016-185 du 12 juillet 2016 décidant de rendre publique la mise en demeure n° 2016-058 du 30 juin 2016 prise à l'encontre de la société Microsoft Corporation.

(22) Cnil, décision n° 2016-079 du 26 septembre 2016 mettant en demeure la société W.M.G., assortie de la délibération n° 2016-289 du 3 octobre 2016 décidant de rendre publique la mise en demeure n° 2016-079 du 26 septembre 2016 prise à l'encontre de la société W.M.G.

(23) L. « Informatique et Libertés », 6 janv. 1978, art. 46, al. 2.

(24) Disposition commune aux décisions de mise en demeure à l'encontre de la société Microsoft Corporation et de la société W.M.G.

(25) Cas notamment de la société Allocab dans le cadre de la procédure ayant donné lieu à la délibération de la formation restreinte n° SAN 2017-002 du 13 avril 2017 prononçant une sanction pécuniaire à l'encontre de la société Allocab ; de la société Hertz France dans le cadre de la procédure ayant donné lieu à la délibération de la formation restreinte n° SAN 2017-010 du 18 avril 2017 prononçant une sanction pécuniaire à l'encontre de la société Hertz France ; ou encore de la société Établissements Darty et Fils dans le cadre de la procédure ayant donné lieu à la délibération de la formation restreinte n° SAN 2018-001 du 8 janvier 2018 prononçant une sanction pécuniaire à l'encontre de la société Établissements Darty et Fils.

(26) Cas notamment du Parti socialiste dans le cadre de la procédure ayant donné lieu à la délibération de la formation restreinte n° SAN 2016-315 du 13 octobre 2016 prononçant une sanction pécuniaire à l'encontre du Parti socialiste ; ou de la société Hertz France dans le cadre de la délibération prononçant une sanction pécuniaire à l'encontre de la société Hertz France précitée.

(27) Cas notamment de la société Samadhi SAS dans le cadre de la procédure ayant donné lieu à la délibération de la formation restreinte n° SAN 2016-405 du 15 décembre 2016 prononçant une sanction pécuniaire à l'encontre de la société Samadhi SAS ; de la société Meeitic SAS dans le cadre de la procédure ayant donné lieu à la délibération de la formation restreinte n° SAN 2016-406 du 15 décembre 2016 prononçant une sanction pécuniaire à l'encontre de la société Meeitic SAS ; ou de la société Établissements Darty et Fils dans le cadre de la délibération prononçant une sanction pécuniaire à l'encontre de la société Établissements Darty et Fils précitée.

(28) Délibération prononçant une sanction pécuniaire à l'encontre de la société Hertz France précitée.

grande réactivité – et du « degré de coopération avec la Commission », pour alléger la sanction proposée⁽²⁹⁾.

La décision à l'encontre de la société Établissements Darty et Fils impose un constat mitigé dans la mesure où la Cnil a constaté qu'aucune donnée sensible ou numéro de carte bancaire ne faisait l'objet de la faille de sécurité, que « la société a réagi dès qu'elle a eu connaissance de la violation de données », qu'un audit de sécurité avait été effectué et que la société avait fait preuve de coopération avec la Cnil, mais que la sanction pécuniaire prononcée s'est élevée à 100 000 euros avec publication de la décision⁽³⁰⁾. La sanction initialement proposée par le rapporteur était toutefois de 200 000 euros, ce qui laisse à penser que la sanction a été allégée bien qu'elle reste particulièrement sévère. Une réelle évolution des sanctions est ainsi à noter depuis l'entrée en vigueur de la loi « Lemaire ».

En tout état de cause, l'autorité dispose d'une palette de sanctions relativement étendue lui permettant d'en moduler la sévérité.

2°/ La typologie des sanctions de la Cnil : un vaste panel

La Cnil dispose de trois types de sanctions lorsque sa mise en demeure de faire cesser les manquements mentionnés est restée lettre morte, allant de l'avertissement à l'injonction de cesser le traitement, en passant par l'amende administrative. Elle dispose également de certaines sanctions complémentaires, dont la plus usitée est la publicité de ses décisions.

De l'avertissement à l'injonction de cesser le traitement. L'article 45 de la loi du 6 janvier 1978 a été modifié par la loi « pour une République numérique » (ou loi « Lemaire »)⁽³¹⁾. Il prévoit désormais que lorsque le responsable du traitement n'a pas exécuté les mises en demeure qui lui ont été formulées par la Cnil, cette dernière peut prononcer les sanctions suivantes : un avertissement, une sanction pécuniaire (à l'exception des cas où le traitement est mis en œuvre par l'État), une injonction de cesser le traitement ou le retrait d'une éventuelle autorisation accordée.

La loi « pour une République numérique » ajoute au texte initial que, « lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable et après une procédure contradictoire, les sanctions [susmentionnées] ».

La loi « Lemaire » a donc durci le cadre des pouvoirs de sanction de la Cnil. Elle vient également augmenter considérablement le plafond des amendes administratives que la Cnil peut prononcer, passant de 150 000 euros à 3 millions d'euros⁽³²⁾, anticipant légèrement, ainsi, les futures modifications nécessaires avec l'entrée en application du règlement général sur la protection des données.

(29) Cnil, décision n° SAN 2017-012 du 16 novembre 2017, prononçant une sanction pécuniaire à l'encontre de la société Web Éditions.

(30) Délibération prononçant une sanction pécuniaire à l'encontre de la société Établissements Darty et Fils précitée.

(31) L. n° 2016-1321, 7 oct. 2016 « pour une République numérique », JO 8 oct., p. 1.

(32) L. « Informatique et libertés », 6 janv. 1978, art. 47, al. 1^{er}.

Par ailleurs, en cas de violation de l'identité humaine, des droits de l'homme, de la vie privée ou aux des libertés individuelles ou publiques, la Cnil est autorisée à prendre des mesures plus drastiques s'inscrivant dans le cadre d'une procédure d'urgence contradictoire. Peut ainsi être ordonnée l'interruption de la mise en œuvre du traitement pour une durée maximale de trois mois (à l'exception notamment de ceux intéressant la sûreté de l'État), prononcer un avertissement, décider le verrouillage de certaines données à caractère personnel traitées, informer le Premier ministre afin qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée⁽³³⁾. De plus, en cas d'atteinte grave et immédiate à ces droits et libertés, « le président de la Commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés »⁽³⁴⁾.

Des sanctions complémentaires à disposition. La Cnil peut assortir ses décisions de sanctions complémentaires. Ainsi, elle peut dénoncer au procureur de la République les manquements à la loi « Informatique et libertés » appréhendés aux articles 226-16 à 226-24 du Code pénal. Elle peut surtout, depuis la loi du 29 mars 2011 « relative au Défenseur des droits »⁽³⁵⁾, prononcer la publicité de ses sanctions, sans avoir à démontrer spécifiquement la mauvaise foi de la société concernée.

L'article 46 de la loi « Informatique et libertés » dispose que « la formation restreinte peut rendre publiques les sanctions qu'elle prononce. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne aux frais des personnes sanctionnées. Le président de la Commission peut demander de rendre publique la mise en demeure ». Il est particulièrement intéressant de noter, ici, la distinction faite dans l'article 46 entre sanction et mise en demeure qui peuvent toutes deux être soumises à publicité. La Cnil rappelle, d'ailleurs, que la « mise en demeure ne revêt pas le caractère d'une sanction » et que lorsqu'elle aura été rendue publique, si la société visée se conforme aux exigences de l'autorité dans le délai imparti, la procédure « fera l'objet d'une clôture qui sera également rendue publique »⁽³⁶⁾.

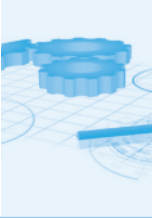
L'article 131-35 du Code pénal précise pourtant à son alinéa premier que « la peine d'affichage de la décision prononcée ou de diffusion de celle-ci est à la charge du condamné. Les frais d'affichage ou de diffusion recouvrés contre ce dernier ne peuvent toutefois excéder le maximum de l'amende encourue ». L'alinéa 2 poursuit ainsi : « La juridiction peut ordonner l'affichage ou la diffusion de l'intégralité ou d'une partie de la

(33) L. « Informatique et libertés », 6 janv. 1978, art. 45-II.

(34) L. « Informatique et libertés », 6 janv. 1978, art. 45-III.

(35) Voir supra.

(36) Cnil, décision n° 2016-058 du 30 juin 2016 mettant en demeure la société Microsoft Corporation, assortie de la délibération n° 2016-185 du 12 juillet 2016 décidant de rendre publique la mise en demeure n° 2016-058 du 30 juin 2016 prise à l'encontre de la société Microsoft Corporation ; et Cnil, décision n° 2016-079 du 26 septembre 2016 mettant en demeure la société W.M.G., assortie de la délibération n° 2016-289 du 3 octobre 2016 décidant de rendre publique la mise en demeure n° 2016-079 du 26 septembre 2016 prise à l'encontre de la société W.M.G.



décision, ou d'un communiqué informant le public des motifs et du dispositif de celle-ci. Elle détermine, le cas échéant, les extraits de la décision et les termes du communiqué qui devront être affichés ou diffusés. » L'alinéa 5 précise, quant à lui, que « la diffusion de la décision est faite par le Journal officiel de la République française, par une ou plusieurs autres publications de presse, ou par un ou plusieurs services de communication au public par voie électronique. Les publications ou les services de communication au public par voie électronique chargés de cette diffusion sont désignés par la juridiction. Ils ne peuvent s'opposer à cette diffusion ». Enfin l'alinéa 6 termine en mentionnant que « l'affichage et la diffusion peuvent être ordonnés cumulativement ».

L'analyse de cet article fait bien apparaître la notion de « peine » associée à la publication des décisions pénales. Or, il n'en est évidemment pas différemment des décisions prononcées par les autorités administratives. Si la publication des décisions de sanction de la Cnil ne pose aucun problème, il y a une contradiction évidente entre le droit pénal et la position de la Cnil lorsqu'elle prononce la publication de mises en demeure. Ces dernières, précise-t-elle, ne constituent pas une sanction alors qu'elles sont pourtant déjà assorties d'une peine.

Le Conseil d'État associe également la publicité des décisions à l'idée de peine, notamment dans sa décision du 28 septembre 2016⁽³⁷⁾, comprenant d'ailleurs certains considérants sur « la sanction complémentaire de publication ». La Haute Juridiction précise dans cet arrêt que la publicité sans limitation de durée est excessive. En effet, « en omettant de fixer la durée pendant laquelle la publication de l'avertissement resterait accessible de manière non anonyme sur ces deux sites, la formation restreinte de la Cnil doit être regardée comme ayant infligé une sanction sans borne temporelle ». Or, « la sanction complémentaire est, dans cette mesure, excessive ». Le Conseil d'État a eu l'occasion de préciser la durée maximale de publication d'une décision avant anonymisation, durée qui ne peut excéder deux ans⁽³⁸⁾.

La notion de « peine » est totalement présente dans le raisonnement du Conseil d'État, puisqu'il énonce au considérant 7 de l'arrêt du 28 septembre 2016 que, « dès lors qu'elle prononce une sanction complémentaire de publication de sa décision de sanction, la formation restreinte de la Cnil doit être regardée comme ayant légalement admis les manquements qui la fondent et que, dans l'hypothèse où la sanction serait ultérieurement jugée illégale, les personnes sanctionnées pourraient obtenir, outre son annulation, l'indemnisation du préjudice né de sa publication antérieurement à la décision d'annulation ainsi que la publication, dans les mêmes conditions, des éventuelles décisions prononçant la suspension ou l'annulation de la sanction ». Le Conseil d'État ajoute au considérant 9 que sa décision de publication de sanction « se trouve nécessairement soumise, et alors même que la loi ne le prévoirait pas expressément, au respect du principe de proportionnalité ; que la légalité de cette sanction s'apprécie, notamment, au regard du support de diffusion retenu et, le cas échéant, de la durée pendant

laquelle cette publication est accessible de façon libre et continue ».

Le respect du principe de proportionnalité est donc exigé en matière de publicité des décisions de la Cnil. Concernant la publicité des mises en demeure il est d'autant plus intéressant de constater que les décisions afférentes précisent que la nature de la délibération est un « avertissement »⁽³⁹⁾, de même que les décisions de clôture⁽⁴⁰⁾. La publication de ces dernières a du bon dans la mesure où elle permet d'informer les citoyens de la mise en conformité de la société visée avec les exigences de la loi « Informatique et libertés », mais elle rappelle également, par ce biais, une seconde fois, que ladite société avait fait l'objet d'une mise en demeure. La publicité peut donc paraître, dans certaines circonstances, comme une mesure particulièrement sévère.

II. – LES MOTIVATIONS DE LA PUBLICITÉ DES DÉCISIONS DE LA CNIL

Il est possible de déterminer deux volets dans les motifs avancés par la Cnil pour justifier de la publicité de ses décisions, le premier concernant la volonté de sanctionner les comportements déviants (A.), le second celle d'informer et d'anticiper (B.). Ces deux aspects sont finalement à inscrire dans le cadre des missions de la Cnil précédemment invoquées : informer et protéger, accompagner et conseiller, contrôler et sanctionner, anticiper.

A. – La volonté de sanctionner

Dans le cadre de la publicité des décisions pour sanctionner, la Cnil fait mention de différents motifs, certains découlant des caractéristiques mêmes de la faute commise (1°) d'autres pouvant être considérés comme « annexes » (2°).

1°/ Les motifs découlant des caractéristiques de la faute commise

Lorsque la Cnil analyse les manquements à la loi du 6 janvier 1978 commis par une société, elle étudie le contexte factuel qui les entoure, c'est-à-dire tant les droits et libertés violés, que le comportement du responsable du traitement, notamment lors des contrôles effectués et des suites qui y ont été données, et que l'éventuel caractère répété ou multiple de ces manquements.

Une sanction répondant à la nature des manquements perpétrés. L'une des premières justifications avancées par la Cnil pour la publication de ses décisions tient à la nature des infractions commises par la société concernée, c'est-à-dire qu'elle sanctionne en

(39) Cnil, décision n° 2016-058 du 30 juin 2016 mettant en demeure la société Microsoft Corporation, assortie de la délibération n° 2016-185 du 12 juillet 2016 décidant de rendre publique la mise en demeure n° 2016-058 du 30 juin 2016 prise à l'encontre de la société Microsoft Corporation ; et Cnil, décision n° 2016-079 du 26 septembre 2016 mettant en demeure la société W.M.G., assortie de la délibération n° 2016-289 du 3 octobre 2016 décidant de rendre publique la mise en demeure n° 2016-079 du 26 septembre 2016 prise à l'encontre de la société W.M.G.

(40) Cnil, décision du 28 juillet 2016, relative à la clôture de la mise en demeure n° 2015-058 à l'égard de la société X ; et Cnil, décision n° 2015-061 du 14 octobre 2016, relative à la clôture de la mise en demeure n° 2015-061 à l'égard de la société X.

(37) CE, 9^e et 10^e ch. réunies, 28 sept. 2016, n° 389.448.

(38) Précisé notamment dans la décision CE, 9^e et 10^e ch. réunies, 19 juin 2017, n° 396.050.

premier lieu l'atteinte aux droits et libertés des utilisateurs, pouvant porter sur l'intégralité des dispositions de la loi « Informatique et libertés ». Les dernières décisions rendues sont particulièrement éclairantes à ce titre, la nature de la décision (sanction pécuniaire, avertissement, mise en demeure ou clôture de procédure) n'ayant aucune incidence en la matière.

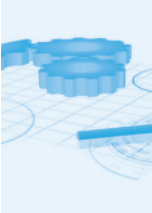
Elle sanctionne ainsi les violations à l'obligation de procéder à des formalités préalables de mise en œuvre d'un traitement (chapitre IV de la loi « Informatique et libertés »)⁽⁴¹⁾, ainsi que les manquements à l'obligation de respecter la vie privée et les libertés individuelles (article 1^{er} de la loi « Informatique et libertés »)⁽⁴²⁾. Sont également sanctionnées les violations à l'obligation de procéder à une collecte ou à un traitement loyal des données (art. 6-1)⁽⁴³⁾ ou de veiller à l'adéquation, à la pertinence et au caractère non excessif des données (art. 6-3)⁽⁴⁴⁾. La Cnil sanctionne aussi les violations à l'obligation de définir et mettre en œuvre une durée de conservation des données (art. 6-5)⁽⁴⁵⁾. Elle réprime les violations de l'obligation de disposer d'une base légale pour la mise en œuvre du traitement (art. 7)⁽⁴⁶⁾ ou les manquements à l'obligation de recueillir le consentement de la personne concernée pour le traitement des données sensibles (art. 8)⁽⁴⁷⁾.

Par ailleurs seront également sanctionnés les manquements à l'obligation d'informer les personnes (art. 32-I)⁽⁴⁸⁾ et notamment d'obtenir l'accord préalable des personnes concernées avant d'inscrire des cookies sur leur terminal de communications électroniques ou d'accéder à celles-ci, et de mettre en œuvre un mécanisme valable d'opposition (art. 32-II)⁽⁴⁹⁾. La Cnil sanctionne encore les manquements à l'obligation d'assurer la sécurité et la confidentialité des données (art. 34)⁽⁵⁰⁾. De même, elle sanctionne les manquements à l'obligation de respecter le droit d'accès à ses données à caractère personnel (art. 39-I et 43)⁽⁵¹⁾. Enfin sont sanctionnés les manquements à l'obligation de respecter les règles relatives aux transferts de données à caractère personnel hors de l'Union européenne (art. 68 et 69)⁽⁵²⁾.

Ainsi, la Cnil est en mesure de sanctionner toute atteinte aux dispositions de la loi « Informatique et libertés », ce qui fait référence aux droits et libertés des utilisateurs mais aussi aux obligations du responsable du traitement. Or, une attention particulière est réservée à l'analyse de la coopération de la société visée avec les services de la Cnil lors du contrôle. Ainsi, les entraves aux actions de la Cnil ou l'absence de réponse fournie à ses différentes demandes d'information entreront en compte lors de l'établissement de la sanction en tant que violation de l'article 21 de la loi du 6 janvier 1978, et constitueront une circonstance aggravante, favorisant

- (41) Délibération prononçant une sanction pécuniaire à l'encontre de la société *Brandalley* ; décision mettant en demeure la société Microsoft Corporation, assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée (pour les traitements de lutte contre la fraude et d'exclusion).
- (42) Décision mettant en demeure la société W.M.G., assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société W.M.G. précitée.
- (43) Délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland précitée.
- (44) Décision mettant en demeure la société Microsoft Corporation, assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée ; délibération prononçant une sanction pécuniaire à l'encontre de la société BDE.
- (45) Délibération prononçant une sanction pécuniaire à l'encontre de la société *Brandalley* précitée ; délibération prononçant une sanction pécuniaire à l'encontre du Parti socialiste précitée ; délibération prononçant une sanction pécuniaire à l'encontre de la société Allocab précitée ; délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland précitée.
- (46) Décision mettant en demeure la société W.M.G., assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société W.M.G. précitée ; délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland précitée.
- (47) Délibération prononçant une sanction pécuniaire à l'encontre de la société Samadhi SAS précitée (sur le traitement de données relatives à l'orientation sexuelle) ; délibération prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS précitée (sur le traitement de données relatives à l'orientation sexuelle) ; délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland précitée (sur le traitement de données relatives aux opinions politiques ou religieuses et à la vie sexuelle).

- (48) Décision mettant en demeure la société Microsoft Corporation, assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée ; délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland précitée.
- (49) Délibération prononçant une sanction pécuniaire à l'encontre de la société *Brandalley* précitée ; décision mettant en demeure la société Microsoft Corporation, assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée ; délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland précitée. Citons également la décision n° SAN 2017-012 du 16 novembre 2017, prononçant une sanction pécuniaire à l'encontre de la société Web Éditions, même si, dans ce cas, la sanction assortie à ce manquement semble plus être l'amende administrative.
- (50) Délibération prononçant une sanction pécuniaire à l'encontre de la société *Brandalley* précitée ; décision mettant en demeure la société Microsoft Corporation, assortie de la décision de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée ; délibération prononçant une sanction pécuniaire à l'encontre du Parti socialiste précitée ; délibération prononçant une sanction pécuniaire à l'encontre de la société Allocab précitée ; délibération prononçant une sanction pécuniaire à l'encontre de la société BDE précitée ; délibération prononçant une sanction pécuniaire à l'encontre de la société Hertz France précitée ; délibération prononçant une sanction pécuniaire à l'encontre de la société Établissements Darty et Fils précitée.
- (51) Délibération prononçant une sanction pécuniaire à l'encontre de la société d'exercice libéral à responsabilité limitée X précitée.
- (52) Délibération prononçant une sanction pécuniaire à l'encontre de la société *Brandalley* précitée ; décision mettant en demeure la société Microsoft Corporation, assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée (sur l'obligation de disposer d'une base légale pour le transfert des données).



dès lors l'adoption d'une peine complémentaire de publicité de la décision⁽⁵³⁾.

Une sanction répondant au cumul des manquements commis. La Cnil justifie également ses décisions de sanction comme de publicité au regard du cumul des violations commises, qu'il s'agisse d'un manquement unique réitéré à de nombreuses reprises, ou bien d'un nombre varié de divers manquements. Ce cumul constituera alors lui aussi une circonstance aggravante propre à inciter l'adoption d'une peine complémentaire de publicité. La décision de publicité de la mise en demeure adressée à la société Microsoft Corporation se justifie ainsi notamment « *par les nombreux manquements constatés et l'atteinte consécutive aux droits des personnes concernées* »⁽⁵⁴⁾.

De même dans sa décision « Allocab », elle avance pour motif que les manquements « *ont persisté bien au-delà de l'échéance du délai imparti par la mise en demeure de la présidente de la Commission* », et justifie spécifiquement la publicité de la sanction « *compte tenu de la persistance dans le temps de plusieurs manquements formulés à l'encontre de la société* »⁽⁵⁵⁾. La même formulation a été employée dans la décision « société d'exercice libéral à responsabilité limitée X »⁽⁵⁶⁾ et dans la décision « société BDE » pour laquelle les manquements ont perduré pendant plus d'un an⁽⁵⁷⁾.

Ainsi, les circonstances entourant les violations de la loi « Informatique et libertés » sont couramment avancées par la Cnil pour justifier la publicité de la sanction prononcée. Mais d'autres motifs sont également énoncés pour justifier le volet répressif de la publicité.

2°/ Les motifs « annexes » utilisés par la Cnil pour justifier ses sanctions

La Cnil prête une attention particulière à la gravité de l'atteinte portée aux utilisateurs et cherche à adapter la sanction à l'organisme visé par la procédure.

Une sanction répondant à la gravité de l'atteinte portée aux utilisateurs. La répression de la Cnil, et notamment sa décision d'assortir sa sanction d'une peine complémentaire de publicité, est dépendante de la nature des données à caractère personnel auquel il aura été porté atteinte. Ainsi, plus les données violées seront conséquentes et diverses, plus cela sera perçu comme une circonstance aggravante et plus la sanction sera lourde. De même, plus le nombre de personnes concernées par les manquements constatés sera conséquent, plus la faille relevée sera considérée comme ayant une particulière gravité.

(53) Délibération prononçant une sanction pécuniaire à l'encontre la société d'exercice libéral à responsabilité limitée X précitée ; délibération prononçant une sanction pécuniaire à l'encontre de la société BDE précitée.
 (54) Délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée.
 (55) Délibération prononçant une sanction pécuniaire à l'encontre de la société Allocab précitée.
 (56) Délibération prononçant une sanction pécuniaire à l'encontre de la société d'exercice libéral à responsabilité limitée X précitée.
 (57) Délibération prononçant une sanction pécuniaire à l'encontre de la société la société BDE précitée.

Ainsi, la Cnil relève dans ses décisions « *le caractère particulièrement sensible des données en cause* »⁽⁵⁸⁾ ou tient compte « *de la nature des données traitées* », notamment lorsqu'elles sont susceptibles de se voir qualifiées de données sensibles, puisque afférentes notamment aux opinions politiques ou religieuses ou aux orientations sexuelles⁽⁵⁹⁾, ou bien lorsqu'il s'agit de données relatives à des infractions⁽⁶⁰⁾ et même à la vie privée⁽⁶¹⁾.

Le nombre de personnes concernées par la violation n'est également pas anodin pour la Cnil, puisqu'elle n'hésite pas à l'invoquer à l'appui de ses décisions de publicité, y compris dans le cadre des mises en demeure. Ainsi, elle a conclu dans sa décision à l'encontre de la société Microsoft Corporation que la mesure de publicité se justifie notamment « *par le nombre de personnes concernées par ses traitements (plus de dix millions d'utilisateurs de Windows 10 sur le territoire national)* »⁽⁶²⁾. La logique a été similaire dans la décision adoptée à l'encontre de la société W.M.G. puisqu'elle motive sa décision de publicité « *tant par le nombre d'utilisateurs de l'application [Gossip] (téléchargée 637 816 fois au 5 juin 2016) que par l'âge des personnes qui peuvent être concernées par les gossips (personnes mineures)* ». Ici, la violence des propos tenus, couplée avec le grand nombre de mineurs pouvant être concernés par les « potins » ont joué comme circonstance aggravante.

En matière de sanction pécuniaire également, la Cnil s'appuie sur cette justification, estimant « *les faits d'une particulière gravité au regard du volume de personnes concernées par les traitements en cause* »⁽⁶³⁾. S'agissant de la décision « Facebook », la Cnil estime que la publicité est nécessaire, « *compte tenu de la nature des données traitées et du nombre de personnes concernées par les traitements en cause, à savoir au moins 33 millions d'utilisateurs en France* »⁽⁶⁴⁾. Dans le cadre de la décision à l'encontre de la société Hertz France, la Cnil sanctionne « *l'accessibilité de données à caractère personnel variées et directement identifiables se rapportant à un volume important de clients, en l'occurrence 35 327 personnes* ». À l'occasion de sa délibération contre la société Web Éditions, la Cnil a tenu compte du « *nombre important d'utilisateurs, mais aussi de tiers visés dans les formulaires* » concernés par la faille de sécurité en cause⁽⁶⁵⁾. Enfin, dans la décision « Établissement Darty et Fils », la Cnil a tenu compte de

(58) Délibération prononçant une sanction pécuniaire à l'encontre du Parti socialiste précitée.
 (59) Délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland précitée.
 (60) Délibération prononçant une sanction pécuniaire à l'encontre de la société Web Éditions précitée.
 (61) Délibération prononçant une sanction pécuniaire à l'encontre de la société Établissements Darty et Fils précitée.
 (62) Délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée.
 (63) Délibération prononçant une sanction pécuniaire à l'encontre de la société Brandalley précitée. Voir également, pour une motivation analogue, la délibération prononçant une sanction pécuniaire à l'encontre de la société Samadhi SAS.
 (64) Délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland précitée.
 (65) Délibération prononçant une sanction pécuniaire à l'encontre de la société Web Éditions précitée.

« l'accessibilité de données à caractère personnel variées et directement identifiantes se rapportant à de nombreux clients »⁽⁶⁶⁾.

Une sanction adaptée à l'organisme concerné. La publicité des décisions de sanction de la Cnil étant associée à une peine complémentaire, il convient d'avancer la réunion de circonstances aggravantes pour la prononcer. Or, l'un des arguments de la Cnil consiste à se fonder sur les caractéristiques du responsable du traitement. Dès lors qu'il sera conséquent, il sera perçu comme étant parallèlement en mesure d'attirer un grand nombre d'utilisateurs et de données, mais également de connaître et maîtriser la réglementation applicable et de disposer de moyens nécessaires pour en assurer la sécurité et la bonne conservation. La publicité se justifie donc « par le statut et la taille de l'organisme en cause », tels que par exemple être leader mondial dans la commercialisation de systèmes d'exploitation et de logiciels pour le cas de Microsoft Corporation⁽⁶⁷⁾.

La taille de l'entreprise ou sa situation financière seront donc autant d'éléments qui participeront à l'individualisation des sanctions prononcées à l'encontre du responsable du traitement défaillant, tout comme, nous l'avons dit, son comportement lors du contrôle diligent par la Cnil. Or, elle a su tenir compte de ces éléments afin d'alléger la sanction proposée initialement par le rapporteur. Ainsi, dans sa décision contre la société Web Éditions, elle a relevé la composition de l'entreprise (quatre salariés), ainsi que sa situation financière⁽⁶⁸⁾.

B. – Le projet d'informer et anticiper

Suivant l'adage régulièrement visé par la jurisprudence du XIX^e siècle, la Cnil semble appliquer la prescription selon laquelle « il vaut mieux prévenir le mal que d'avoir à le punir ». Avec la multiplication des plates-formes collectant de plus en plus de données à caractère personnel, il est essentiel que chacun ait connaissance de ses droits en matière « Informatique et libertés » afin d'être en mesure de les défendre et de les faire valoir. La sensibilisation des organismes est tout aussi importante, en termes de sécurisation économique d'une part (les sanctions pécuniaires allant grandissant) et en termes de prévention d'autre part, puisqu'ils pourront chercher, par eux-mêmes, à se mettre en conformité avec la réglementation applicable.

La publicité des décisions de la Cnil a donc une vocation pédagogique certaine (1^o/), mais nous verrons qu'elle répond également à un contexte d'exposition de plus en plus forte des utilisateurs et de leurs données à caractère personnel (2^o/). Ces deux pans apparaissent d'ailleurs très explicitement comme justification de sa décision du 16 novembre 2017, prise à l'encontre de la Société Web Éditions⁽⁶⁹⁾.

(66) Délibération prononçant une sanction pécuniaire à l'encontre de la société Établissements Darty et Fils précitée.

(67) Délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée.

(68) Délibération prononçant une sanction pécuniaire à l'encontre de la société Web Éditions précitée.

(69) Délibération prononçant une sanction pécuniaire à l'encontre de la société Web Éditions précitée.

1^o/ Une ambition pédagogique

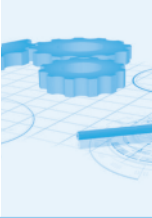
La vocation pédagogique de la publicité des décisions de la Cnil se comprend notamment s'agissant des mises en demeure ou de leur clôture. En effet, celles-ci n'étant pas censées revêtir le caractère de sanctions, la publicité ne devrait avoir aucun autre but que celui de prévenir de futures violations et d'avoir un effet dissuasif à l'égard des autres responsables du traitement. Toutefois, l'ambition nouvelle de la Cnil sur ce point ne se limite pas aux mises en demeure, les mêmes arguments étant avancés dans ses décisions de sanction également. Or, pour que l'information soit complète, elle doit couvrir à la fois les responsables du traitement et à la fois les utilisateurs de services, semant des données à caractère personnel partout sur leur passage.

Vers la sensibilisation des acteurs. La publicité des décisions de la Cnil doit permettre aux responsables du traitement de comprendre leurs obligations à travers l'interprétation qui est donnée de la loi « Informatique et libertés ». La Cnil a, ainsi, notamment précisé que cette mesure a vocation « à appeler l'attention de l'organisme en cause sur les manquements constatés et lui permettre de mettre en conformité dans les délais impartis par la mise en demeure »⁽⁷⁰⁾. En effet, ce qui se cache derrière la publicité, et qui est implicitement visé par la Cnil, c'est l'attention du public. Lorsque ce dernier aura connaissance des manquements dont s'est rendu coupable un organisme il sera peut-être plus frileux à lui laisser entre les mains ses données à caractère personnel. Or, cela a été mentionné, il n'est plus possible, pour les responsables du traitement, de se passer de la collecte des données à caractère personnel. Un retard en la matière creuserait un fossé difficile à combler au regard de la vitesse de développement des innovations à l'heure actuelle.

La durée et l'étendue de la publicité de la décision vont donc tenir compte de la nécessité de sensibiliser les responsables du traitement sur leurs obligations⁽⁷¹⁾. Mais la vocation pédagogique de la publicité des décisions va même plus loin, car elle ne se limite pas à la sensibilisation des acteurs concernés. En effet, et cela sera d'autant plus vrai avec l'entrée en application du règlement général sur la protection des données, le 26 mai 2018, la seule évocation des sanctions encourues devrait suffire à inquiéter les autres responsables du traitement, suffisamment afin qu'ils ne commettent pas les mêmes violations que celles visées dans la décision.

(70) Délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée ; voir également la décision mettant en demeure la société W.M.G., assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société W.M.G. précitée.

(71) Délibération prononçant une sanction pécuniaire à l'encontre de la société Brandalley précitée ; voir également la délibération prononçant une sanction pécuniaire à l'encontre de la société Samadhi SAS précitée ou celle prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS précitée, pour une motivation similaire ; voir encore la délibération prononçant une sanction pécuniaire à l'encontre de la société Allocab précitée, la délibération du 18 mai 2017 prononçant une sanction pécuniaire à l'encontre la société d'exercice libéral à responsabilité limitée X précitée et la délibération prononçant une sanction pécuniaire à l'encontre de la société BDE précitée.



Vers une information croissante des utilisateurs. La publicité des sanctions de la Cnil permet, en parallèle de la sensibilisation des responsables du traitement, d'informer les utilisateurs sur leurs droits et libertés. Elle leur offre un accès aux décisions, et surtout aux motivations qui sont avancées. Or, ce sont ces dernières qui participent réellement à la facette pédagogique de la publicité, puisqu'elles permettent aux citoyens de bien saisir tous les enjeux de la réglementation « Informatique et libertés », ainsi que ses violations. Elles font, en effet, le point sur la législation applicable et l'interprétation qui en est faite par la Cnil, interprétation dont la valeur ne cesse d'augmenter en parallèle de l'augmentation du montant des sanctions encourues.

Ce sont les motifs concernant la peine prononcée qui offrent la possibilité d'appréhender ce qui sera vu comme une circonstance aggravante ou non et, surtout, du point de vue des utilisateurs, de comprendre quels manquements sont particulièrement dangereux pour la sauvegarde de l'intégrité de leurs données personnelles⁽⁷²⁾. La publicité des décisions leur offre des exemples concrets et appliqués, permettant de mettre en lumière leurs droits, afin qu'ils soient plus à même de pouvoir les défendre. Il en est ainsi, notamment de la décision « Microsoft » précitée, dans laquelle la Cnil justifie la publicité d'information « des utilisateurs de Windows 10 sur leurs droits, et plus particulièrement sur leur possibilité de contrôler les données à caractère personnel qui sont collectées »⁽⁷³⁾. De même, dans sa décision « Brandalley », la Cnil recherchait, par la publicité, à « sensibiliser les internautes et les responsables de traitement à leurs droits et obligations »⁽⁷⁴⁾. Enfin, dans les décisions « Web Éditions » et « Établissement Darty et Fils », il s'agissait de « sensibiliser les internautes quant au risque pesant sur la sécurité de leurs données »⁽⁷⁵⁾.

La sensibilisation des responsables du traitement et l'information des utilisateurs sont devenues un motif type et systématique de la décision de publicité des sanctions.

2°/ Une réponse au contexte actuel de violations répétées aux données personnelles

La multiplicité des plates-formes en ligne et des nouvelles technologies a conduit à une multiplicité de mise à disposition des données personnelles et de leur traitement. Or cette tendance a engendré une croissance des comportements déviants en la matière, obligeant la Cnil à contrecarrer, dans un objectif à la fois répressif et à la fois anticipatif. Il lui a été nécessaire d'établir un plan d'action et de mettre en place des outils lui permettant de lutter contre les différents manquements relevés.

Or, la publicité des sanctions est l'un de ces outils. Elle revêt un caractère dissuasif et pédagogique essentiel, missions dont la Cnil s'est investie et qui transparaissent clairement de ses décisions. Ainsi, elle rappelle, même dans ses décisions de clôture qui sont censées relever la mise en conformité de l'entreprise visée, « la nécessité de veiller au respect de la loi Informatique et libertés qui participe à la protection des données à caractère personnel, droit fondamental reconnu à chaque personne »⁽⁷⁶⁾, ou encore les enjeux de la prochaine réglementation européenne⁽⁷⁷⁾.

Cette volonté d'inscrire la publicité de ses délibérations en réponse aux violations croissantes de la loi du 6 janvier 1978 transparaît d'autant plus nettement dans sa décision de sanction à l'égard de la société Hertz France⁽⁷⁸⁾, ainsi que dans ses décisions à l'encontre de la société Web Éditions⁽⁷⁹⁾ et Établissement Darty et Fils⁽⁸⁰⁾. Ces dernières sont particulièrement intéressantes dans la mesure où elles ont été prononcées sous l'égide de la loi « Lemaire ». Or, il apparaît, à la lecture des délibérations, que le motif de sensibilisation des acteurs et d'information des utilisateurs se fait adjoindre celui de l'inscription dans le « contexte actuel dans lequel se multiplient les incidents de sécurité ».

S'agissant du règlement général sur la protection des données, il prévoit que l'amende administrative infligée à l'organisme défaillant tienne compte de différents éléments⁽⁸¹⁾, donnant par ce biais des pistes quant aux futurs motifs invoqués par la Cnil. Certains éléments se rapprochent fortement des justifications avancées jusqu'alors par la Cnil : la nature, la gravité et la durée de la violation, la mise en perspective avec la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ; la nature délibérée ou non ou l'éventuelle négligence du responsable dans la réalisation du manquement ; la réactivité du responsable pour atténuer le dommage subi par les personnes

(72) Décision mettant en demeure la société W.M.G., assortie de la délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société W.M.G. précitée, qui cherche à « informer les personnes concernées du traitement de leur numéro de téléphone (fixe ou mobile) associé à leur identité dès lors que ces données figurent dans le répertoire téléphonique ou parmi les données renseignées par les contacts Facebook de l'utilisateur qui procède au téléchargement de l'application Gossip, les potins anonymes ».

(73) Délibération décidant de rendre publique la mise en demeure prise à l'encontre de la société Microsoft Corporation précitée.

(74) Délibération prononçant une sanction pécuniaire à l'encontre de la société Brandalley précitée ; voir également la délibération prononçant une sanction pécuniaire à l'encontre de la société Samadhi SAS précitée ou celle prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS précitée ; voir encore la délibération prononçant une sanction pécuniaire à l'encontre de la société Allocacab précitée, la délibération du 18 mai 2017 prononçant une sanction pécuniaire à l'encontre la société d'exercice libéral à responsabilité limitée X précitée et la délibération prononçant une sanction pécuniaire à l'encontre de la société BDE précitée.

(75) Délibération prononçant une sanction pécuniaire à l'encontre de la société Web Éditions précitée.

(76) Décision du 28 juillet 2016, relative à la clôture de la mise en demeure n° 2015-058 à l'égard de la société X.

(77) Décision n° 2015-061 du 14 octobre 2016, relative à la clôture de la mise en demeure n° 2015-061 à l'égard de la société X ; et Délibération prononçant une sanction pécuniaire à l'encontre de la société Établissements Darty et Fils précitée.

(78) Délibération prononçant une sanction pécuniaire à l'encontre de la société Hertz France précitée.

(79) Délibération prononçant une sanction pécuniaire à l'encontre de la société Web Éditions précitée.

(80) Délibération prononçant une sanction pécuniaire à l'encontre de la société Établissements Darty et Fils précitée.

(81) RGPD, art. 83.

concernées ; le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles mises en œuvre ; la coopération instaurée avec les autorités de contrôle ; la nature des données concernées.

L'article 83 du règlement européen ajoute également de nouveaux motifs, non invoqués par la Cnil dans ses dernières décisions : la récidive dans les violations de la réglementation européenne ; la manière dont l'autorité de contrôle a eu connaissance de la violation (en tenant compte de la notification ou non par le responsable du traitement) ; la tenue de précédentes mesures à l'encontre du responsable de traitement ; l'application de codes de conduite ou de mécanismes de certification. Ces différents éléments sont à envisager comme de potentiels nouveaux motifs concernant la publicité des décisions prochaines de la Cnil.

CONCLUSION

Ainsi, lorsque la Cnil prononce la publicité de ses sanctions – ou mises en demeure –, elle n'avance rarement qu'une seule justification, mais use d'un panel particulièrement étendu de différents motifs. Cette diversité peut d'ailleurs paraître louable dans le cadre du principe de personnalisation des sanctions. Si les motifs utilisés semblent plus ou moins cohérents, c'est plus la décision

même de publicité qui peut souffrir d'une remise en cause. En effet, cette dernière est associée à une peine complémentaire et cette sanction peut parfois sembler stigmatisante pour les entreprises en cause.

Si l'on porte attention à la double vocation de la publicité – sanctionner et prévenir – la position de la Cnil peut se comprendre. Dans son volet anticipatif, la Cnil cherche à toucher un nombre de personnes le plus large possible, ce qui passe, en partie, par la publicité de ses sanctions, y compris des mises en demeure. Néanmoins, s'agissant de la publicité des mises en demeure et des débats qui les entourent, il aurait été possible d'envisager une publicité anonymisée afin de conserver les motifs et justifications de la Cnil, tout en ne sanctionnant pas l'entreprise en cause à ce stade de la procédure.

De même, la variété des motifs utilisés par la Cnil peut poser quelques difficultés en matière de sécurité juridique, dans la mesure où les justifications avancées peuvent paraître posées comme un cheveu sur la soupe. Elles ne sont, en effet, que peu détaillées, et il n'est pas évident de comprendre pourquoi tel motif a présidé à la sélection de tel autre. Or, cela engendre certaines problématiques en matière d'anticipation et de prévisibilité, notions pourtant essentielles dans le cadre d'une procédure contentieuse. ■