LAMY
REVUE

REVUE LAMY

Droit des Affaires

Les données à caractère personnel et l'entreprise

Emmanuel DAOUD, Géraldine PÉRONNE et Flora PLÉNACOSTE

– Recodification du Code de la consommation : S.O.S. d'un pénaliste en détresse
Jean-Marie BRIGANT

– Les tribunaux de commerce spécialisés en ordre de marche…
Entretien avec Jean-Luc VALLENS

– Dépister une aide d'État
Nicole COUTRELIS, Thomas GOURDEAU et Sandra CAUSSANEL

– Droit de préemption légal du preneur à bail commercial et procédures collectives : quelle articulation ?
Fabien KENDÉRIAN

119 | MENSUEL
OCTOBRE 2016

Wolters Kluwer

Le point sur...

Les données à caractère personnel et l'entreprise

Les technologies permettent aujourd'hui aux entreprises privées d'exploiter les données comme jamais auparavant dans le cadre de leurs activités. L'ampleur de la collecte et du partage des données est inédite. On ne cesse en outre d'évoquer l'idée d'une « révolution digitale » à laquelle les entreprises devraient se préparer.

Ces évolutions ne pourront toutefois se faire que dans le strict respect des limites posées par le droit quant au traitement des données à caractère personnel. Or, le droit des données personnelles est à l'aube de mutations juridiques importantes. Régie depuis près de trente ans par la loi dite « loi informatique et libertés » à laquelle tous étaient habitués, la protection des données est aujourd'hui encadrée par un règlement européen ayant pour objectif d'uniformiser le niveau de protection en Europe.

Ce texte européen intitulé « règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) », sera directement applicable dans les pays de l'Union européenne le 25 mai 2018.

Il laisse donc deux ans aux personnes physiques et aux personnes morales pour adapter leurs pratiques et leurs politiques. Il conduira nécessairement les entreprises et leurs dirigeants à la mise en œuvre de plans de conformité efficaces et plus généralement au développement de leur activité de compliance.

Le règlement est en cela particulièrement incitatif puisqu'il renforce les obligations des responsables de traitements de données et sanctionne les manquements en imposant des amendes administratives aux montants inégalés. Les autorités de contrôle nationales, la Commission nationale informatique et libertés en France, chargées de la mise en œuvre de ces sanctions, sont ainsi placées au cœur du droit des données à caractère personnel.

Les sanctions administratives ne constituent pas les seuls risques auxquels s'exposent les particuliers et les entreprises. Le risque pénal ne doit pas être éludé. Le règlement prévoit que les États membres sont libres de déterminer le régime des sanctions applicables en cas de violation du texte (Règl. n° 2016/679 préc., consid. 149). Pour l'heure, les amendes pénales et peines d'emprisonnement des articles 226-16 à 226-24 du code pénal restent applicables. Il conforte en outre la possibilité d'actions en responsabilité civile afin d'obtenir réparation du dommage subi en raison d'une violation des obligations imposées par le règlement (Règl. n° 2016/679, art. 82).

À l'aune de ces nouveaux enjeux, il paraît essentiel de procéder à une analyse croisée des différentes obligations auxquelles seront assujettis les responsables de traitement relativement à la sécurité des données, aux transferts des données, aux droits des personnes et de mettre en lumière les nouveaux pouvoirs des autorités de contrôle. ■

SOMMAIRE

La sécurité des données à caractère personnel dans l'entreprise P.22

L'encadrement des transferts des données à caractère personnel dans des pays tiers.. P.26

Le renforcement des droits des personnes sur leurs données : mythe ou réalité ? P.28

Les nouveaux pouvoirs de la CNIL : vers un changement de philosophie ? P.32

RLDA 6024

La sécurité des données à caractère personnel dans l'entreprise

Par Emmanuel DAOUD
Avocat associé Cabinet Vigo Membre du Conseil de l'Ordre

Et Flora PLÉNACOSTE
Avocate Cabinet Vigo

Le règlement européen n° 2016/679 affiche l'objectif clair de renforcer la sécurité des données à caractère personnel, ce qui engendre une nécessité pour l'entreprise de s'engager dans un processus de mise en conformité.

Le règlement européen n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dit règlement général sur la protection des données ; ci-après, le Règlement) prévoit que l'entreprise est tenue, au titre de la sécurité des données, d'assurer « *la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées* »(1). Il développe donc les obligations prévues par la loi dite « informatique et libertés »(2) indiquant seulement que l'entreprise doit prendre « *toutes précautions utiles (...)* [pour] *notamment empêcher que* [les données] *soient déformées, endommagées, ou que des tiers non autorisés y aient accès* »(3).

Le Règlement semble ainsi tenir compte de l'accroissement des actions illégales ou malveillantes auxquelles les entreprises font face envers leur réseau ou système d'information et qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées. Une étude a recensé en 2015, une progression de 38 % des cyberattaques au niveau international, et de 51 % en France(4).

Le Règlement tend ainsi à susciter la confiance qui favorise le développement de l'économie numérique en étoffant le cadre juridique relatif à la sécurité des données. Il renforce les obligations pesant sur les entreprises relatives à la mise en œuvre de mesures de sécurité (1), inscrit l'exigence de sécurité des données dans le cadre de nouveaux concepts (2) et uniformise le niveau de responsabilité entre responsable de traitement et sous-traitant en la matière (3).

1. Des obligations renforcées pour l'entreprise

La mise en place de « mesures techniques et organisationnelles » assurant la sécurité des données

Contrairement à la loi *informatique et libertés* qui n'apporte pas de précisions sur les « précautions utiles »(5) que l'entreprise doit mettre en place afin d'assurer un niveau de sécurité des données, le Règlement énumère un certain nombre de « mesures techniques et organisationnelles » que le responsable de traitement sera tenu de mettre en œuvre(6).

L'entreprise devra, entre autres, assurer « *la pseudonymisation et le chiffrement des données à caractère personnel* », mettre en place des moyens « *permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* » et « *de rétablir*

(1) Règl. n° 2016/679, art. 5.

(2) L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés.

(3) L. n° 78-17, art. 34.

(4) Étude The Global State of Information Security® Survey 2016 réalisée par le cabinet d'audit et de conseil PwC, en collaboration avec CIO et CSO : <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>.

(5) L. n° 78-17, art. 34.

(6) Règl. n° 2016/679, art. 32.

la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique », ainsi que concevoir « *une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ». Des mesures supplémentaires pourront être déterminées, « selon les besoins »[7].

Cependant, si le Règlement donne les objectifs que devront permettre de réaliser la mise en place de telles mesures, il n'en énonce pas précisément la nature ou le détail. Il prévoit néanmoins que les outils utilisés et le niveau de sécurité devront être modulés et adaptés en fonction de « *l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement* »[8], ainsi que du niveau de risque que le traitement représente pour les droits et libertés des personnes physiques qui résulterait par exemple de la destruction, de la perte ou de la divulgation non autorisée des données[9]. En pratique, les entreprises devront s'assurer que le système d'information dispose des fonctionnalités minimales en matière de sécurité (intégrité, mises à jour, etc.) et adapter les mesures supplémentaires au cas par cas.

Par ailleurs, le responsable de traitement devra veiller à ce que les personnes physiques agissant sous son autorité, c'est-à-dire les salariés, ne traitent les données à caractère personnel auxquels ils ont accès que sur son instruction[10].

L'obligation de notification des violations de données

Le Règlement définit la violation des données à caractère personnel comme étant une « *violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* »[11]. Il reprend en cela les termes essentiels de la loi *informatique et libertés*[12]. Il peut s'agir de la simple perte d'un smartphone par un employé ou de l'intrusion d'un virus informatique dans le système de l'entreprise.

(7) Règl. n° 2016/679, art. 32 (1).
(8) Règl. n° 2016/679, art. 32 (1).
(9) Règl. n° 2016/679, art. 32 (2).
(10) Règl. n° 2016/679, art. 32 (4).
(11) Règl. n° 2016/679, art. 4.
(12) L. n° 78-17, art. 34 bis : « *Pour l'application du présent article, on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques* ».

Le Règlement souligne qu'une telle violation, si l'on n'intervient pas à temps et de manière appropriée, entraîne un risque de causer des dommages physiques, matériels ou encore un préjudice moral aux personnes concernées (par exemple, une usurpation d'identité)[13].

Par conséquent, alors que la loi *informatique et libertés* fait uniquement peser l'obligation de notification de ces violations sur les opérateurs de communication électronique[14], le Règlement étend l'obligation de notification à l'ensemble des responsables de traitement[15]. Toutes les entreprises seront donc soumises à l'obligation de notifier les violations de données à la Commission nationale de l'informatique et des libertés (CNIL) ainsi qu'à la personne concernée, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne[16].

La notification à personne physique n'est toutefois pas nécessaire dans certains cas, et notamment celui dans lequel le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les personnes concernées n'est plus susceptible de se matérialiser. L'entreprise effectuera plutôt une communication publique ou procèdera à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace[17].

2. L'inscription de l'exigence de sécurité dans de nouveaux principes posés par le Règlement

Le règlement européen consacre de nouveaux concepts et obligations tels que le respect de la protection des données dès la conception dit « Privacy by design », le principe de protection des données par défaut ou encore le principe de responsabilité dit « accountability ». Ces nouvelles règles jouent un rôle incontournable dans l'objectif de renforcement de la sécurité que vise le Règlement.

Une sécurité exigée « dès la conception » et « par défaut »

Le responsable du traitement doit adopter des règles internes et mettre en œuvre des mesures en matière de sécurité qui respectent les principes de protection des données dès la conception ou « privacy by design » ainsi que le principe de protection des données par défaut.

(13) Règl. n° 2016/679, consid. 85.
(14) L. n° 78-17, art. 34 bis.
(15) Règl. n° 2016/679, art. 33 et 34.
(16) Règl. n° 2016/679, art. 34 (1).
(17) Règl. n° 2016/679, art. 34 (3).

Le principe du « privacy by design » implique que les fabricants de produits, les prestataires de services et les producteurs d'applications prennent en compte la protection des données à caractère personnel, y compris les exigences en matière de sécurité, dès le moment de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits impliquant le traitement des données pour remplir leurs fonctions[18]. Pour cela, le responsable du traitement devra mettre en œuvre des mesures techniques et organisationnelles appropriées, telles que la mise en place, dès que possible, de la pseudonymisation, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même[19]. Dans cette démarche, une pondération doit être faite par le responsable de traitement entre coûts, état de l'art, contexte, finalités des traitements concernés et risques pour les droits et libertés des individus, etc.[20]. La conciliation entre ces concepts laissera une grande place à une appréciation au cas par cas. Concrètement, la direction des systèmes d'information devra assurer la sécurité des données dès la conception d'un projet informatique. Elle devra également coopérer étroitement avec le service juridique afin d'assurer le respect du Règlement.

Le principe de protection des données par défaut implique quant à lui que le responsable du traitement mette en œuvre les mesures techniques et organisationnelles garantissant que, par défaut, et sans l'intervention de la personne concernée, les données à caractère personnel ne sont rendues accessibles qu'à un nombre déterminé de personnes[21]. Cela permettra à la personne de garder un contrôle sur les données qui sont traitées par l'entreprise et d'inciter le responsable de traitement à mettre en place des dispositifs encadrant l'accès aux données, notamment par les employés.

Le principe de responsabilité ou « accountability » en matière de sécurité

En application du principe d'« accountability », le responsable de traitement doit s'assurer et être en mesure de démontrer que le traitement est effectué conformément au Règlement, y compris en matière de sécurité[22]. Ce principe implique notamment la tenue d'une documentation et la mise en place de mesures qui doivent être réexaminées et actualisées si nécessaire[23]. Lorsque cela est proportionné au regard des activités de traitement, le responsable de traitement doit également mettre en œuvre une politique appropriée[24].

En outre, la réalisation d'une analyse d'impact, l'élaboration d'un code de conduite et l'obtention d'une certification ou encore la tenue d'un registre participent au respect, par l'entreprise, du principe de responsabilité.

➜ *L'examen des mesures de sécurité dans le cadre de l'analyse d'impact*

Lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes du fait d'un recours à de nouvelles technologies, le responsable du traitement est tenu d'effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel[25]. L'analyse d'impact est, par exemple, obligatoire lorsqu'il est procédé au profilage[26] ou encore dans le cadre de traitements à grande échelle de données sensibles telles que l'origine raciale ou les opinions religieuses[27].

Dans le cadre de cette analyse, l'entreprise doit notamment examiner les dispositions, garanties et mécanismes mis en place pour assurer la sécurité des données, et apporter la preuve au regard de cet ensemble que les exigences du Règlement en la matière sont bien respectées[28].

S'il ressort de l'analyse que le traitement engendrerait un risque élevé pour les droits et libertés des personnes physiques en l'absence des garanties, de mesures de sécurité et de mécanismes mis en place pour atténuer ce risque, et que le responsable du traitement est d'avis que le risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts de mise en œuvre, ce dernier doit consulter l'autorité de contrôle avant le début des opérations de traitement, laquelle devra répondre aux questions du responsable de traitement dans un délai déterminé[29].

➜ *La certification et l'élaboration de règles de conduite en matière de sécurité*

Dans le prolongement du principe d'« accountability », le Règlement préconise la mise en place de règles de bonne conduite et de certification qui peuvent servir d'éléments pour démontrer le respect des exigences.

Les codes de conduite définissent et précisent les modalités d'application de l'entreprise de leurs obligations, et notamment celles relevant de la sécurité des données,

(18) Règl. n° 2016/679, consid. 78.
(19) Règl. n° 2016/679, art. 25 (1).
(20) Règl. n° 2016/679, art. 25 (1).
(21) Règl. n° 2016/679, art. 25 (2).
(22) Règl. n° 2016/679, art. 24 (1).
(23) Règl. n° 2016/679, art. 24 (1).
(24) Règl. n° 2016/679, art. 24 (2).
(25) Règl. n° 2016/679, art. 35 (1).
(26) Règl. n° 2016/679, art. 35 (3) a).
(27) Règl. n° 2016/679, art. 35 (3) b).
(28) Règl. n° 2016/679, art. 35 (7) d).
(29) Règl. n° 2016/679, art. 36.

telles que la pseudonymisation[30]. Les entreprises doivent soumettre le projet de code de conduite à la CNIL qui l'approuve si elle estime qu'il offre des garanties appropriées suffisantes[31]. Lorsque le code de conduite porte sur des activités de traitement menées en France, la CNIL l'enregistre et le publie. Lorsque le projet de code de conduite concerne des activités de traitement menées dans plusieurs États membres, l'entreprise doit également obtenir l'approbation de la Commission qui peut décider par voie d'exécution que le code de conduite est d'application générale au sein de l'Union européenne[32].

Le mécanisme de certification, de labels et de marques quant à lui permet aux personnes d'évaluer rapidement le niveau de protection des données offert par les produits et services de l'entreprise en question. Elle est délivrée à l'entreprise par des organismes de certification agréées ou par l'autorité de contrôle pour une durée de 3 ans renouvelable[33].

➜ *La tenue d'un registre comportant les mesures de sécurité*

Le Règlement prévoit que l'entreprise doit tenir un registre de traitements comportant notamment, et « dans la mesure du possible », une description générale des mesures de sécurité techniques et organisationnelles[34]. Cette obligation ne s'applique cependant pas aux entreprises comptant moins de 250 employés, sauf dans certains cas, et notamment celui où le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et libertés des personnes concernées[35].

3. Une uniformisation du niveau de responsabilité des acteurs en matière de sécurité

Bien que la responsabilité conjointe des responsables de traitement soit reconnue par la CNIL[36], elle n'est pas prévue par la loi *informatique et libertés*. Le Règlement remédie à cela et encadre précisément la responsabilité conjointe du traitement qui est qualifiée lorsque deux responsables du traitement, ou plus, déterminent conjointement les finalités et les moyens du traitement[37]. Dans ce cas, les responsables du traitement doivent définir de manière transparente leurs obligations respectives en matière de sécurité, par exemple par voie d'accord entre eux[38].

Par ailleurs, le règlement européen sur la protection des données vise à responsabiliser les acteurs des traitements de données en uniformisant les obligations et le niveau de responsabilité pesant sur les responsables de traitements et les sous-traitants[39]. L'entreprise sous-traitante sera par conséquent tenue des mêmes obligations en matière de sécurité que le responsable de traitement.

Le responsable de traitement doit néanmoins veiller à faire appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, et ce notamment en matière de sécurité des données.

Le traitement par un sous-traitant peut être régi par un contrat qui lie le sous-traitant à l'égard du responsable du traitement, et qui prévoit notamment que le sous-traitant prend toutes les mesures requises en matière de sécurité des données. Le sous-traitant aide également le responsable du traitement, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant, à garantir le respect des obligations en matière de sécurité[40].

Lorsqu'un sous-traitant recrute un autre sous-traitant, les mêmes obligations que celles figurant dans le contrat liant le responsable de traitement au sous-traitant s'imposent à lui en matière de sécurité[41]. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations[42].

Tout comme le responsable de traitement, l'entreprise sous-traitante peut appliquer un code de conduite ou un mécanisme de certification afin de démontrer l'existence de garanties suffisantes en la matière[43]. ■

(30) Règl. n° 2016/679, art. 40 (2).
(31) Règl. n° 2016/679, art. 40 (5).
(32) Règl. n° 2016/679, art. 40 (7) (8) (9).
(33) Règl. n° 2016/679, art. 42 et s.
(34) Règl. n° 2016/679, art. 30 (1) (g).
(35) Règl. n° 2016/679, art. 30 (5).
(36) G. Desgens-Pasanau, La protection des données personnelles, Lexisnexis 2015.
(37) Règl. n° 2016/679, art. 26 (1).
(38) Règl. n° 2016/679, art. 26 (1).
(39) Règl. n° 2016/679, art. 28 (1).
(40) Règl. n° 2016/679, art. 28 (3)
(41) Règl. n° 2016/679, art. 28 (4)
(42) Règl. n° 2016/679, art. 28 (4)
(43) Règl. n° 2016/679, art. 28 (5).

RLDA 6025

L'encadrement des transferts des données à caractère personnel dans des pays tiers

Par Emmanuel DAOUD
Avocat associé Cabinet Vigo Membre du Conseil de l'Ordre

Et Flora PLÉNACOSTE
Avocate Cabinet Vigo

Le règlement européen n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dit règlement général sur la protection des données) n'opère pas de modification substantielle de la règlementation préexistante en matière de transfert des données à caractère personnel dans des pays tiers à l'Union européenne. Il précise toutefois son cadre juridique et consacre la légalité de pratiques existantes jusqu'alors.

Dans le prolongement de la directive 95/46/CE[1], le règlement européen n° 2016/679 du 27 avril 2016 (ci-après, le Règlement) reconnaît une importance aux flux transfrontaliers de données et énonce qu'ils sont « *nécessaires au développement du commerce international et de la coopération internationale* »[2].

Il prévoit cependant que les transferts de données qui font ou sont destinés à faire l'objet d'un traitement à des responsables du traitement, sous-traitants ou autres, situés dans des pays tiers, doivent avoir lieu dans le plein respect de ses dispositions, y compris pour les transferts ultérieurs de données au départ du pays tiers vers un autre pays tiers[3].

Le Règlement autorise ces transferts dans les cas où le pays tiers a fait l'objet d'une décision d'adéquation de la Commission européenne (1), lorsque ces transferts sont encadrés par des outils assurant un niveau de protection suffisant et approprié des personnes concernées (2), ou encore dans le cadre de situations dérogatoires particulières (3).

1. Le transfert de données autorisé par une décision d'adéquation de la Commission

Le Règlement consacre la faculté de la Commission d'apprécier le niveau de protection assuré par un pays tiers. Il prévoit qu'elle peut décider, avec effet dans l'ensemble de l'Union, qu'un pays tiers ou un territoire ou un secteur déterminé dans un pays tiers, offre un niveau adéquat de protection des données. Ce caractère adéquat du niveau de protection est évalué au regard notamment du respect des droits de l'homme et des libertés fondamentales dans le pays tiers en question ou encore de ses engagements internationaux pris en matière de protection des données[4].

Dans le cas où la Commission considère que le pays tiers offre un niveau de protection adéquat, elle prend un acte d'exécution qui autorise les transferts de données à caractère personnel vers ce pays[5]. L'acte d'exécution prévoit un examen périodique au moins tous les quatre ans. Dans ce cadre, la Commission peut, sur justifications, révoquer la décision d'adéquation[6], auquel cas le transfert de données vers ce pays tiers est interdit, sauf si des garanties appropriées autres sont prises en faveur de la personne concernée afin de compenser

(1) Dir. PE et Cons. 95/46/CE, 24 oct. 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, art. 26.

(2) Règl. (UE) n° 2016/679, considé. 101.

(3) Règl. (UE) n° 2016/679, art. 44.

(4) Règl. (UE) n° 2016/679, art. 45 (2)(a)(b)(c).

(5) Règl. (UE) n° 2016/679, art. 45 (3).

(6) Règl. (UE) n° 2016/679, art. 45 (5).

l'insuffisance de la protection des données dans ce pays tiers[7].

2. Le transfert de données encadré par des outils appropriés

En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant doit prendre des mesures apportant des garanties appropriées en faveur de la personne concernée, qui respectent les exigences en matière de protection des données.

Tout d'abord, le Règlement mentionne explicitement la possibilité pour les groupes d'entreprises de recourir à des « *règles d'entreprise contraignantes* ». Les groupes d'entreprises pourront donc définir des règles internes qui, si elles sont approuvées par la Commission nationale de l'Informatique et des Libertés (CNIL), constitueront des garanties appropriées[8]. Ces règles d'entreprise doivent comporter certaines précisions, notamment les mécanismes mis en place au sein du groupe pour garantir le respect de ces règles (audits, mise en place de méthodes, etc.)[9].

Ces garanties peuvent également être apportées par la conclusion d'un contrat comportant les clauses types de protection des données adoptées par la Commission. Une nouveauté réside dans le fait que ces clauses types pourront désormais être adoptées par la CNIL, puis approuvées par la Commission[10].

Par ailleurs, le Règlement prévoit l'option pour les acteurs du traitement d'élaborer des clauses spécifiques, et de les insérer dans les contrats conclus entre le responsable de traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel se situant dans le pays tiers. La CNIL décidera, au regard de ces clauses, d'autoriser ou non le transfert[11].

Enfin, la mise en place d'un code de conduite approuvé par la CNIL assortie de l'engagement contraignant et exécutoire pris par le responsable de traitement ou le sous-traitant[12], ou encore le mécanisme de certification, constituent des outils nouveaux ainsi que des garanties appropriées permettant le transfert des données[13].

3. Dérogations autorisées pour les transferts dans le cadre de situations particulières

Le Règlement définit et précise les dérogations autorisées pour les transferts de données, sur la base des dispositions existantes de la directive 95/46/CE[14]. Il prévoit qu'en l'absence de décision d'adéquation ou de garanties appropriées, le transfert de données dans un pays tiers peut avoir lieu notamment lorsque la personne concernée a donné son consentement explicite, ou encore lorsque le transfert est nécessaire à l'exécution d'un contrat conclu entre la personne concernée et le responsable du traitement, ou enfin s'il est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable de traitement et une autre personne physique ou morale[15]. ■

(7) Règl. (UE) n° 2016/679, consid. 107.
(8) Règl. (UE) n° 2016/679, art. 47 (1) (a).
(9) Règl. (UE) n° 2016/679, art. 47 (2) (b).
(10) Règl. (UE) n° 2016/679, art. 46 (2) (c) et (d).
(11) Règl. (UE) n° 2016/679, art. 46 (3) (a).
(12) Règl. (UE) n° 2016/679, art. 46 (2) (e).
(13) Règl. (UE) n° 2016/679, art. 46 (2) (f).
(14) Dir. 95/46/CE préc., art. 26.
(15) Règl. (UE) n° 2016/679, art. 49.

RLDA 6026

Le renforcement des droits des personnes sur leurs données : mythe ou réalité ?

Par Emmanuel DAOUD
Avocat associé
Cabinet Vigo
Membre du Conseil de l'Ordre

Et Géraldine PÉRONNE
Avocat
Docteur en droit
Cabinet Vigo

Parmi les nouveautés annoncées du règlement européen sur la protection des données figure le renforcement des droits des personnes sur leurs données. Ce renforcement entraîne des contraintes significatives pour l'entreprise qui devra adapter ses procédures de collecte et de traitement de données aux nouvelles dispositions. Celles-ci permettent-elles seulement une protection effective des données ?

C'est le règne du « droit à » au sein du règlement européen sur la protection des données[1] : « droit à l'information », « droit à l'effacement », « droit à la limitation des données », « droit à la portabilité des données », etc. Les personnes dont les données font l'objet d'un traitement se voient ainsi reconnaître de nombreux droits dont le responsable de traitement est le débiteur.

Un constat s'impose : il y a plus de « droits à » qu'auparavant. Un chapitre entier du règlement, le chapitre III, leur est ainsi consacré. Si certains de ces droits figuraient déjà dans la loi dite « informatique et libertés », le Règlement leur donne une nouvelle dimension. Surtout, il fait naître de nouveaux droits au bénéfice de la personne concernée. Concomitamment, il assujettit les entreprises, responsables de traitement, à des obligations plus lourdes et plus onéreuses.

Cette inflation de droits subjectifs au sein du Règlement accentue la personnalisation du droit des données à caractère personnel, dont l'assimilation à un droit de la personnalité ne fait plus de doutes[2]. L'objectif poursuivi par le législateur européen est de renforcer les droits des personnes sur leurs données afin de garantir la protection des données[3]. Renforcement des droits des personnes et protection effective des données apparaissent ainsi consubstantiels.

Le renforcement des droits des personnes transparaît de l'octroi aux personnes physiques d'un droit élargi à l'information sur leurs données et d'un pouvoir de contrôle accru sur celles-ci, mais ces droits permettent-ils seulement d'atteindre leur fin, celle d'une réelle protection des données ?

Si les droits des personnes sur leurs données semblent dotés d'une portée nouvelle (1), la protection effective des données par ce biais est questionnée, de telle manière que le renforcement des droits doit être relativisé (2).

1. La portée nouvelle des droits des personnes sur leurs données

Afin de renforcer le droit des personnes sur leurs données, le Règlement favorise le droit à l'information, dont il étend le champ d'application et attribue à la personne concernée des moyens de contrôle plus grands sur ses données.

(1) Règl. PE et Cons. 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, ci-après « le Règlement ».

(2) Sur la tension entre personnalisation et patrimonialisation des données, voir Le numérique et les droits fondamentaux, Étude annuelle du Conseil d'État, La Documentation française, 2014, p. 264-269. V. égal. Quelle politique européenne en matière de données personnelles ?, Note d'analyse – Digital New Deal Foundation, sept. 2015, p. 10-16.

(3) Règl. n° 2016/679, considé. 11.

Élargissement du droit à l'information de la personne sur ses données

Le chapitre dédié aux droits de la personne concernée s'ouvre sur une disposition générale qui précise les qualités que doit revêtir l'information communiquée par le responsable de traitement. La communication de l'information doit être « *concise, transparente, compréhensible et aisément accessible en des termes clairs et simples (...)* »[4].

Outre ces précisions nouvelles, on peut observer que le nombre d'informations à fournir est plus important que sous le régime de la loi *informatique et libertés*.

Cela se vérifie, dans un premier temps, au moment de la collecte des données. L'article 32 de la loi *informatique et libertés* prévoyait déjà la communication d'informations portant sur l'identité du responsable de traitement, sur la finalité poursuivie, le caractère obligatoire ou facultatif des réponses, les conséquences éventuelles d'un défaut de réponse, les destinataires des données, le droit d'opposition, l'existence de transferts de données, etc.

L'article 13 du Règlement ajoute à cette liste plusieurs nouvelles obligations d'information : sur la durée de conservation, sur le droit de demander au responsable de traitement l'accès, la rectification ou l'effacement des données ainsi que le droit de demander une limitation du traitement, l'existence du droit de retirer son consentement, le droit d'introduire une réclamation auprès d'une autorité de contrôle, sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat, l'existence d'une prise de décision automatisée, l'obligation de communiquer les coordonnées du délégué à la protection des données, le cas échéant.

Alors que la collecte indirecte de données faisait l'objet d'un simple paragraphe dans la loi *informatique et libertés* et renvoyait à l'article 39 I du texte, le Règlement y consacre un article entier, ce qui reflète sans nul doute, la croissance de ce mode d'obtention des données[5].

Le législateur européen se montre plus strict que dans la loi *informatique et libertés* car il impose une contrainte temporelle au responsable de traitement : les informations précitées doivent être fournies « *dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois* ». En outre, si les données doivent être utilisées aux fins de la communication avec la personne concernée, les informations doivent être fournies « *au plus tard au moment de la première communication* ».

(4) Règl. n° 2016/679, art. 12.

(5) Règl. n° 2016/679, art. 14.

L'accroissement du nombre d'informations à transmettre se vérifie encore, dans un second temps, au cours du traitement des données. Le Règlement instaure en effet des obligations de notification et de communication ponctuelles.

D'une part, le responsable de traitement doit notifier à chaque destinataire auquel les données à caractère personnel ont été communiquées « *toute rectification, tout effacement des données à caractère personnel ou toute limitation du traitement* ». Le responsable de traitement est tenu de donner des informations sur les destinataires à la personne concernée, si elle en fait la demande[6].

D'autre part, le Règlement introduit une obligation de communication à la personne concernée, d'une violation de données à caractère personnel. Bien que présente dans la loi *informatique et libertés*, cette obligation de communication sur les failles de sécurité était circonscrite à un certain type d'opérateurs économiques : le fournisseur de services de communications électroniques accessibles au public[7]. Le Règlement procède à une généralisation de cette obligation à tous les responsables de traitement. Le principe est donc celui de la communication d'informations, sauf exceptions limitativement énumérées[8].

Ces obligations d'information, nouvelles ou renforcées, permettent ou du moins tendent à faciliter la maîtrise, par la personne concernée, de ses données.

Intensification du contrôle de la personne sur ses données

L'affirmation d'un contrôle accru de la personne sur ses données repose sur l'octroi de nouveaux droits à la personne concernée, afin que celle-ci puisse, non plus seulement avoir un droit de regard sur les données, mais un pouvoir d'action sur celles-ci[9].

Ce contrôle accentué sur les données est illustré par trois nouveaux « droits à » : le droit à l'oubli, le droit à la limitation du traitement et le droit à la portabilité des données.

L'article 40 de la loi *informatique et libertés* prévoyait déjà la possibilité pour toute personne physique justifiant de son identité d'exiger du responsable de traitement de rectifier ou d'effacer certaines données. Le Règlement distingue plus clairement ces possibilités en consacrant l'article 16 au droit de rectification et l'article 17 au droit à l'effacement ou droit à l'oubli.

(6) Règl. n° 2016/679, art. 19.

(7) L. n° 78-17, art. 34 bis (loi *informatique et libertés*).

(8) Règl. n° 2016/679, art. 34.

(9) Le Règlement s'inscrit dans la droite ligne de « l'autodétermination informationnelle », principe issu de la jurisprudence constitutionnelle allemande et plébiscité par le Conseil d'État dans son étude annuelle, précitée, p. 264.

Sous l'empire de la loi *informatique et libertés*, la rectification ou l'effacement des données n'était possible que lorsque les données étaient « *inexactes, incomplètes, équivoques, périmées* » ou « *la collecte, l'utilisation, la communication ou la conservation* [était] *interdite* ». L'article 17 du Règlement reformule ces motifs et en ajoute d'autres : l'effacement est également possible lorsque la personne concernée retire le consentement sur lequel est fondé le traitement et qu'il n'existe pas d'autre fondement juridique au traitement. En outre, le responsable de traitement est contraint de procéder à l'effacement « *dans les meilleurs délais* ».

Le droit à la limitation du traitement est, quant à lui, une réelle nouveauté, au même titre que le droit à la portabilité des données.

Le droit à la limitation du traitement pourrait être envisagé comme une situation de suspension temporaire du traitement. Ce droit est ouvert à la personne concernée, en cas de contestation par elle, de l'exactitude des données ou lorsque le traitement est illicite et la personne concernée s'oppose à leur effacement ou encore, lorsque le responsable du traitement n'a plus besoin des données à caractère personnel mais que celles-ci sont encore nécessaires à la personne concernée pour l'exercice de droits en justice[10].

Enfin, le droit à la portabilité des données, accorde un double droit à la personne concernée. Elle peut, d'une part, demander au responsable du traitement à recevoir ses données dans un « *format structuré, couramment utilisé et lisible par machine* » afin notamment de les transmettre à un autre responsable du traitement sous certaines conditions. Elle peut, d'autre part, obtenir que les données soient transmises directement d'un responsable de traitement à un autre « *lorsque cela est techniquement possible* ».

La violation des droits des personnes est lourdement sanctionnée, ce qui montre l'importance qui leur est conférée par le règlement[11]. Si le Règlement favorise un droit à l'information élargi ainsi qu'un contrôle accru sur les données, cela va-t-il nécessairement de pair avec une meilleure protection des données ?

2. L'effectivité relative des droits des personnes sur leurs données

On observera l'existence de limites au droit à l'information et quant au contrôle que l'individu peut exercer sur ses données. Plus fondamentalement, la possibilité d'un contrôle sur les données ne garantit pas nécessairement la protection de celles-ci.

Les droits des personnes sur leurs données ne sont pas absolus

Les droits des personnes sur leurs données ne sont pas absolus. Ils comportent des limites, prévues par le Règlement lui-même et qui restreignent la protection des données.

Les obligations d'information sont assorties d'exceptions. Le responsable de traitement en est notamment dispensé si la fourniture de ces informations exige « *des efforts disproportionnés* ».

On peut s'interroger sur le sens à donner à cette limite : faut-il prendre en considération le coût économique, le nombre de personnes concernées ? En l'absence de critère clair, il pourrait être aisé pour le responsable de traitement de se retrancher derrière cette exception afin de contourner son obligation d'information.

De même, si le règlement assoit le principe du droit à l'oubli, il ne manque pas de lui assortir des limites liées à l'exercice du droit à la liberté d'expression et d'information, au respect d'une obligation légale ou l'exécution d'une mission d'intérêt public ou encore à la constatation, l'exercice ou la défense de droits en justice.

D'aucuns argueront que le consentement de l'individu comme condition de licéité du traitement, tel que figurant dans le Règlement, constitue bel et bien la marque d'un contrôle sur les données[12]. Certains observateurs ont beaucoup commenté cette disposition, accentuant le caractère novateur du Règlement sur ce point et laissant présumer que la protection des personnes en était renforcée. Cette appréciation doit être relativisée.

En premier lieu, le consentement a toujours été une des conditions de la collecte licite de données et il l'est encore avec le Règlement. Les nouveautés sont semble-t-il plus modestes. Elles résident principalement dans les précisions apportées sur les modalités du consentement[13] et l'encadrement particulier du consentement de l'enfant de moins de 16 ans[14].

En deuxième lieu, le consentement, n'est qu'une condition de la collecte licite de données parmi d'autres, telles que la nécessité d'un traitement pour l'exécution d'un contrat ou aux fins d'intérêts légitimes.

En troisième lieu, on ne peut manquer de souligner la faible valeur du consentement lorsque la relation entre les parties, comme cela est souvent le cas en matière de

(10) L'article 18 du Règlement relatif au droit à la limitation du traitement doit être lu à l'aune du considérant 67 du Règlement qui explicite les méthodes permettant cette limitation du traitement.

(11) Règl. n° 2016/679, art. 83, 5.

(12) Règl. n° 2016/679, art. 6.

(13) Règl. n° 2016/679, art. 7.

(14) Règl. n° 2016/679, art. 8.

données à caractère personnel, présente un déséquilibre significatif. Ainsi que l'explique un auteur, « *un tel déséquilibre résulte de l'asymétrie fondamentale de moyens existant entre les deux cocontractants privés, dont l'un, l'auteur du traitement, est très majoritairement institutionnel et l'autre, la personne fichée, nécessairement une personne physique* »(15).

Le contrôle sur les données ne garantit pas la protection des données

La notion de contrôle sur les données est traditionnellement associée à la protection des données. Ce lien est rarement remis en question.

Pourtant, lorsque le contrôle n'est qu'une faculté, il offre peu de garanties.

Le contrôle sur les données, découle de « droits à ». La multiplication de ces droits ne signifie pas que l'individu va exercer effectivement son « droit à ». Le « droit à » fait finalement naître un infini potentiel de « droits de ne pas ». L'individu, roi de ses données, investi de pouvoirs et repu de contrôle, pourrait finalement n'être qu'un roi nu.

C'est semble-t-il le corollaire nécessaire d'un transfert du pouvoir vers l'individu, sommé d'assurer la défense de ses données et d'un transfert corrélatif des devoirs vers le responsable de traitement et le sous-traitant, tenus de faire appliquer les droits de la personne concernée(16).

Il est vrai que le Règlement consacre des possibilités d'actions à la personne concernée, tant devant l'autorité de contrôle, que devant le juge judiciaire afin de faire reconnaître ses droits et les faire appliquer(17). Il reste toutefois à savoir si elles seront exploitées(18).

En outre, lorsque le contrôle induit des comportements à risques, il s'avère contreproductif.

Une étude a ainsi mis en évidence le paradoxe du contrôle (*control paradox*) dans le domaine de la protection de la vie privée(19). Selon cette étude, la capacité d'une personne de contrôler certains risques obscurcirait la conscience qu'elle a de l'existence d'autres risques qu'elle ne peut contrôler. En conséquence, la possibilité d'un contrôle affecterait la perception qu'une personne a de la protection de sa vie privée, à un point tel que plus l'existence d'un contrôle serait perçue par un individu, plus sa volonté de révéler certaines informations sensibles serait grande. Cela s'expliquerait par la confiance placée dans le contrôle.

Il ne faudrait pas déduire de cette étude, seulement brièvement évoquée ici, que l'attribution à l'individu d'un contrôle sur ses données serait néfaste ou inutile. Elle permet de souligner en revanche la faiblesse d'un contrôle qui ne serait pas accompagné d'une politique de sensibilisation aux risques. De manière très opportune, le Règlement a investi les autorités de contrôle de cette mission importante(20).

La portée nouvelle des droits des personnes sur leurs données telle qu'elle transparaît du règlement européen est à la fois indispensable et insuffisante. Le renforcement de ces droits ne sera réel que s'il s'accompagne d'une action efficace de prévention et de répression de la part des autorités de contrôle nationales ou des autorités judiciaires. Seule la conjonction de ces éléments semble à même d'assurer une protection effective des données. ■

(15) N. Ochoa, Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition, RFD adm. 2015, p. 1157. En faveur d'une prise en considération de ce déséquilibre, voir toutefois le considérant 43 du Règlement.

(16) V. sur ce point, M. Bourgeois, Réforme européenne des données personnelles : le nouveau partage de responsabilité entre les acteurs d'un traitement, JCP E 2016, 1328.

(17) Règl. n° 2016/679, art. 77 à 82.

(18) Le recours au juge judiciaire a jusqu'à présent été largement délaissé au profit d'une approche règlementaire du contentieux relatif aux données à caractère personnel. V. C. Bloud-Rey, Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ?, D. 2013, 2795.

(19) Brandimarte L., Acquisti A., Loewenstein G., Misplaced Confidences : Privacy and the Control Paradox, 2012, Social Psychological and Personality Science 4(3) 340-347.

(20) Règl. n° 2016/679, art. 57.

RLDA 6027

Les nouveaux pouvoirs de la CNIL : vers un changement de philosophie ?

Par Emmanuel DAOUD
Avocat associé Cabinet Vigo Membre du Conseil de l'Ordre

Et Géraldine PÉRONNE
Avocat Docteur en droit Cabinet Vigo

Sous l'égide du règlement européen sur la protection des données, la Commission nationale de l'informatique et des libertés se dote de nouveaux pouvoirs de sanctions, plus dissuasifs. L'évolution est telle que l'on pourrait y voir l'amorce d'un changement de philosophie, la CNIL se transformant en une autorité répressive.

La disposition la plus médiatique du règlement européen sur la protection des données[1] est sans aucun doute celle qui octroie aux autorités de contrôle nationales, la Commission nationale de l'informatique et des libertés (ci-après, la CNIL) en France, le pouvoir d'imposer de lourdes sanctions pécuniaires en cas de violation des dispositions du Règlement.

La CNIL et les autres autorités de contrôle européennes devraient enfin être en mesure de se faire respecter par les grands acteurs de l'Internet, tels Google ou Facebook, peu effrayés jusqu'à présent par ces autorités[2].

Ces mesures étaient attendues car face aux défis du *big data*, des objets connectés, des objets autonomes, il semblait impératif de disposer de nouveaux moyens conséquents, tant de répression, que de dissuasion.

La CNIL disposait déjà de pouvoirs de sanction, mais elle était peu encline à en faire usage. Entre autres facteurs, la faiblesse du montant des amendes ne devait pas être étrangère à cette position. De fait, la CNIL a ainsi développé une approche plus pédagogique que comminatoire dans son appréhension du droit des données personnelles.

L'octroi de pouvoirs nouveaux de sanction serait susceptible de changer la philosophie de la CNIL et de l'orienter vers une approche plus répressive[3].

On observe le passage d'un usage modéré des pouvoirs comminatoires sous la loi *informatique et libertés* (1) à l'acquisition d'un réel pouvoir de dissuasion à l'aune du Règlement (2), ce qui n'est pas sans poser la question de l'articulation des pouvoirs de la CNIL et du juge pénal (3).

1. Des pouvoirs comminatoires traditionnellement peu utilisés

La CNIL a globalement peu recours à la contrainte pour veiller à la mise en conformité à la loi *informatique et libertés*. Cela s'explique par l'absence de vocation répressive de cette autorité, mais aussi par la faiblesse de ses pouvoirs de sanction.

L'absence de vocation répressive de la CNIL

La CNIL n'a pas été instituée afin de constituer le bras armé de la loi *informatique et libertés*. En d'autres termes, elle n'avait pas de vocation répressive[4].

(1) Règl. PE et Cons. 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, ci-après « le Règlement ».

(2) La CNIL a imposé une sanction de 150 000 euros à l'encontre de Google qui constituait la sanction maximale pour un premier manquement (CNIL, délib. n° 2013-420, 3 janv. 2014).

(3) Déjà, v. C. Bloud-Rey, Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ?, D. 2013, 2795.

(4) En ce sens, v. T. Dautieu, La proposition de règlement européen en matière de protection des données personnelles et ses conséquences sur la future stratégie de contrôle de la CNIL, Comm. com. électr. 2012, étude 20.

Pour s'en convaincre, il suffit de relire la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version initiale, qui prévoyait : « *Pour l'exercice de sa mission de contrôle, la commission (...) peut (...) charger un ou plusieurs de ses membres (...) de procéder, à l'égard de tout traitement, à des vérifications sur place et de se faire communiquer tous renseignements et documents utiles à sa mission* » et « *(...) prescrire des mesures de sécurité pouvant aller jusqu'à la destruction des supports d'informations* », mais aussi « *(...) adresser aux intéressés des avertissements (...)* »[5].

Le seul pouvoir de sanction dont elle disposait résidait donc dans la possibilité d'adresser des avertissements.

Il a fallu attendre la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, pour que la CNIL se dote d'un éventail plus large de sanctions : avertissement, mise en demeure et si le responsable de traitement ne répond pas à la mise en demeure, sanction pécuniaire, injonction de cesser le traitement, retrait d'une autorisation de traitement donnée par la CNIL, etc[6].

Dans le texte de loi, ces sanctions arrivent bien après la liste des missions de la CNIL. Ces missions, représentatives des activités principales de la Commission, ne sont pas de nature répressive.

La Commission a ainsi pour mission d'informer, de veiller à la conformité des traitements au texte législatif, de répondre aux demandes d'avis émanant d'organisations professionnelles ou d'institutions, de délivrer des labels, de se tenir informée de l'évolution des technologies de l'information et de rendre publique son appréciation le cas échéant, etc[7].

Les missions premières de la CNIL relèvent du contrôle, de l'information et de la consultation.

Pour assurer sa mission de contrôle, la CNIL dispose de pouvoirs d'investigations, telles la possibilité d'accéder aux locaux d'un organisme et de se faire communiquer des documents[8]. La loi n° 2014-344 du 17 mars 2014 relative à la consommation renforce les pouvoirs d'investigation de la CNIL en permettant à celle-ci de contrôler à distance, sur Internet, des manquements éventuels à la loi *informatique et libertés*.

La Commission exerce également un contrôle *a priori* par le biais des déclarations de traitements de données et demandes d'autorisations pour certains traitements sensibles, effectuées par les responsables de traitements.

(5) L. n° 78-17, art. 21 (loi *informatique et libertés*).

(6) L. n° 78-17, art. 45.

(7) L. n° 78-17, art. 11.

(8) L. n° 78-17, art. 11, 2°, f), et L. n° 78-17, art. 44.

Si la notion de contrôle est souvent associée à celle de sanction, la CNIL fait un usage très modéré de ce pouvoir et ce, d'autant plus que le montant des sanctions pécuniaires qui peuvent être imposées sont faibles.

Des pouvoirs de sanction faibles

Parmi les sanctions dont la CNIL dispose, l'avertissement, l'injonction ou le retrait d'une autorisation de traitement paraissent constituer de faibles moyens de répression et de dissuasion. La sanction pécuniaire, à l'inverse, est susceptible de toucher un point sensible chez les acteurs économiques qui seraient à l'origine de manquements.

En l'état du droit positif, la CNIL peut imposer de telles sanctions : pour un premier manquement, le montant de la sanction pécuniaire ne peut excéder 150 000 euros. En cas de manquement réitéré dans les cinq années, il ne peut excéder 300 000 euros[9]. Néanmoins, le montant de ces amendes semble dérisoire, dès lors que les auteurs de manquement réalisent des chiffres d'affaires de plusieurs milliards[10].

La publicité des sanctions, à laquelle la CNIL a recouru assez fréquemment et qui peut avoir des effets désastreux sur la réputation d'une société et partant constituer une sanction très dissuasive, n'a que très peu de conséquences sur des sociétés étrangères telles que Google ou Facebook, par ailleurs très populaires.

En conséquence, la CNIL a adopté une approche pragmatique en privilégiant une démarche pédagogique d'accompagnement des acteurs vers la mise en conformité. Elle a tissé des relations de confiance avec les Correspondants informatiques et libertés, multiplié les supports d'information, les fiches détaillées. Elle offre une permanence téléphonique aux particuliers comme aux professionnels afin de répondre à leurs questions et informe même des campagnes de contrôles qu'elle compte mener.

Participe de cet esprit la procédure même de sanction qui suppose une mise en demeure préalable de l'auteur du manquement. Il s'avère d'ailleurs que cette procédure conduit à la mise en conformité des auteurs de manquements dans la majorité des cas[11].

De fait, la CNIL impose donc peu de sanctions, mais cela pourrait changer à l'aune du Règlement.

(9) L. n° 78-17, art. 47.

(10) Google a réalisé un chiffre d'affaires de 75 milliards de dollars en 2015. V. P. Escande, Google, Apple et le prix du rêve, Le Monde, 2 févr. 2016.

(11) Le rapport annuel de la CNIL pour l'année 2015 est en cela éloquent. Il fait état de 93 mises en demeure et de 10 sanctions dont 3 sanctions financières et 7 avertissements (CNIL, Rapport d'activité 2015, p. 3).

2. La consécration nouvelle d'un réel pouvoir de dissuasion

Au sein du Règlement, les missions de contrôle, de conseil et d'information des autorités de contrôle sont confortées[12]. L'apport du Règlement réside surtout dans l'attribution d'un réel pouvoir de dissuasion, par l'octroi de pouvoirs répressifs significatifs et par la possibilité d'actions conjointes de plusieurs autorités de contrôle.

Des pouvoirs répressifs significatifs

L'article 83 du Règlement pose les conditions générales pour imposer une amende administrative. L'accent est mis sur la proportionnalité de la sanction par le biais d'une liste de facteurs à prendre en considération afin de décider du principe de la sanction et de son montant.

À la différence du régime de la loi *informatique et libertés*, le Règlement ne prévoit pas de mise en demeure préalable à l'imposition d'une sanction. Dans ces conditions, l'imposition d'amendes aura un caractère beaucoup plus strict et systématique que par le passé, le manquement entraînant immanquablement une sanction, sans préavis et possibilité d'y remédier.

Cette interprétation du texte doit sans doute être nuancée. En effet, parmi les facteurs à prendre en considération avant l'énoncé d'une sanction, figurent le fait qu'« *une mesure ait été prise par le responsable de traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées* »[13] et le « *degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs* »[14].

Afin de donner un réel effet à ces dispositions, il conviendrait de mettre en demeure ou du moins d'informer l'auteur du manquement afin de lui laisser l'opportunité de prendre les mesures qui s'imposent.

Qu'en est-il de l'avertissement ? Le Règlement semble maintenir cette possibilité[15], sans toutefois le qualifier de sanction, contrairement à la loi *informatique et libertés*[16]. Il n'est pas exclusif d'une amende administrative[17]. Le considérant 148 prévoit une solution particulière pour les personnes physiques : un « rappel à l'ordre » en cas de violation mineure ou si l'amende constitue une charge disproportionnée.

Le recours à la sanction pécuniaire par les autorités de contrôle est donc susceptible de prendre une dimension inédite sous l'égide du Règlement.

Ces amendes, dont le montant est gradué en fonction du type de manquement, ont le mérite de la dissuasion. Un premier niveau de sanction prévoit des amendes pouvant s'élever jusqu'à 10 millions d'euros ou dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Cette sanction s'applique notamment en cas de violations des obligations du responsable de traitement relatives au consentement des enfants, à la sécurité, à la coopération avec la CNIL, aux notifications d'une violation de données[18]. Le second niveau de sanction prévoit des amendes pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial pour les violations les plus graves relatives notamment à la licéité des traitements, aux droits des personnes concernées, aux transferts de données hors Union européenne[19].

De nouveaux pouvoirs d'action conjointe

Une autre nouveauté importante du Règlement réside dans la désignation d'une « autorité chef de file »[20]. En vertu de l'article 56 du Règlement, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable de traitement ou du sous-traitant peut agir en tant qu'autorité chef de file dans le cas d'un traitement transfrontalier effectué par ce responsable de traitement ou ce sous-traitant.

L'article 62 prévoit même la possibilité de « mesures répressives conjointes », mais ce point n'est pas détaillé, laissant un doute sur les actions visées par cette disposition.

Certains commentateurs considèrent que cette disposition est susceptible d'entraîner une influence réciproque des autorités de contrôle[21], une autorité de contrôle ayant une politique forte de sanction, serait susceptible de susciter un nivellement général vers le haut du montant des amendes.

En réalité ce risque paraît assez limité, compte tenu de l'encadrement de l'autorité chef de file prévu par le Règlement. Le texte instaure des mécanisme de coopération[22] et de contrôle de la cohérence[23] très détaillés qui laissent supposer qu'il sera difficile pour une autorité de contrôle

(12) Règl. n° 2016/679, art. 57. V. M. Bourgeois, Réforme européenne des données personnelles : les nouvelles sanctions et voies de recours, JCP E 2016, 1329.

(13) Règl. n° 2016/679, art. 83, c).

(14) Règl. n° 2016/679, art. 83, f).

(15) Règl. n° 2016/679, art. 58, 2. a) et b).

(16) L. n° 78-17, art. 45.

(17) Règl. n° 2016/679, art. 58, 2. i).

(18) Règl. n° 2016/679, art. 83, 4.

(19) Règl. n° 2016/679, art. 83, 5.

(20) Règl. n° 2016/679, art. 56.

(21) V. C. Bloud-Rey, *op. cit.*

(22) Règl. n° 2016/679, art. 60.

(23) Règl. n° 2016/679, consid. 135.

d'adopter une position qui serait radicalement différente de celle qu'auraient prise les autres autorités.

En tout état de cause, la possibilité pour une autorité de contrôle de coordonner des actions conjointes et de concentrer les voix de plusieurs autorités de contrôle ajoute au pouvoir de dissuasion de ces autorités.

Ces pouvoirs répressifs plus marqués de la CNIL pourraient relancer le débat autour du caractère juridictionnel de cette autorité administrative indépendante[24], mais aussi sur la question de la place du juge pénal dans le contentieux des données personnelles.

3. Pouvoirs des autorités de contrôle et du juge pénal : quelle articulation ?

Dès lors que la CNIL acquiert un pouvoir de sanction significatif, se pose la question de l'articulation de ce pouvoir avec celui des autorités judiciaires, et en particulier du juge pénal. Si la coopération des deux autorités est confortée, la concurrence des sanctions soulève quelques interrogations.

Une coopération confortée

En application du texte européen, la CNIL peut porter les violations du présent Règlement à l'attention des autorités[25]. Il rappelle en cela l'article 11 de la loi *informatique et libertés* sur le fondement duquel la CNIL « *informe sans délai le procureur de la République des infractions dont elle a connaissance* ».

Le Règlement prévoit en outre que « [l]*es pouvoirs d'enquête en ce qui concerne l'accès aux installations devraient être exercés conformément aux exigences spécifiques du droit procédural des États membres, telle que l'obligation d'obtenir une autorisation judiciaire préalable* ».

Il rappelle en cela l'article 44 de la loi *informatique et libertés* qui régit les contrôles sur place de la CNIL et prévoit une information du procureur de la République, mais aussi le cas échéant, une autorisation du juge de la liberté et de la détention.

Toutefois, alors que la loi *informatique et libertés* prévoyait une information de la CNIL, par le procureur de la République, de toutes les poursuites relatives à une infraction pénale prévue aux articles 226-16 à 226-24 du code pénal[26], cette disposition n'est pas reprise dans le Règlement. Rien toutefois ne semble interdire un tel échange d'informations.

De manière assez cohérente, le Règlement n'innove pas et renvoie au droit procédural de chaque État membre.

Des sanctions concurrentes

Le Règlement laisse la possibilité aux États membres de déterminer le régime des sanctions pénales applicables en cas de violation de ses dispositions[27].

En conséquence, une violation du Règlement peut recevoir à la fois une sanction pénale et une sanction administrative.

Cela était déjà le cas sous l'empire de la loi *informatique et libertés*. Mais il semblerait que la faiblesse du contentieux judiciaire conjugué à un recours très modéré aux sanctions administratives n'ait pas conduit à une double sanction et partant n'ait pas soulevé de questions particulières.

Sous l'égide du Règlement, la fréquence potentiellement accrue des sanctions imposées par la CNIL et leur montant très significatif appellent un débat sur la possibilité d'un cumul des sanctions pénales et administratives.

Le Règlement n'est pas très explicite à cet égard. Il rappelle simplement que l'application d'une double sanction pénale et administrative « *ne devrait pas entraîner la violation du principe ne bis in idem tel qu'il a été interprété par la Cour de justice* »[28].

Ce principe de non-cumul ayant fait l'objet d'une mise en œuvre singulière dans le contexte des abus de marché[29], qui met en concurrence le juge pénal et une autorité administrative indépendante, ses conditions d'application s'agissant du contentieux des données personnelles devront nécessairement être éclaircies. ■

(24) Sur ce point, v. F. Brunet, De la procédure au procès : le pouvoir de sanction des autorités administratives indépendantes, RFD adm. 2013, p. 113.

(25) Règl. n° 2016/679, consid. 129 et art. 58, 5.

(26) L. n° 78-17, art. 52.

(27) Règl. n° 2016/679, art. 149.

(28) *Ibidem*.

(29) Le décret n° 2016-1121 du 11 août 2016, pris en application de la loi n° 2016-819 du 21 juin 2016, fixe des modalités de concertation entre le procureur de la République financier et l'Autorité des marchés financiers afin de déterminer qui de ces deux autorités engagera les poursuites relatives à un abus de marché.