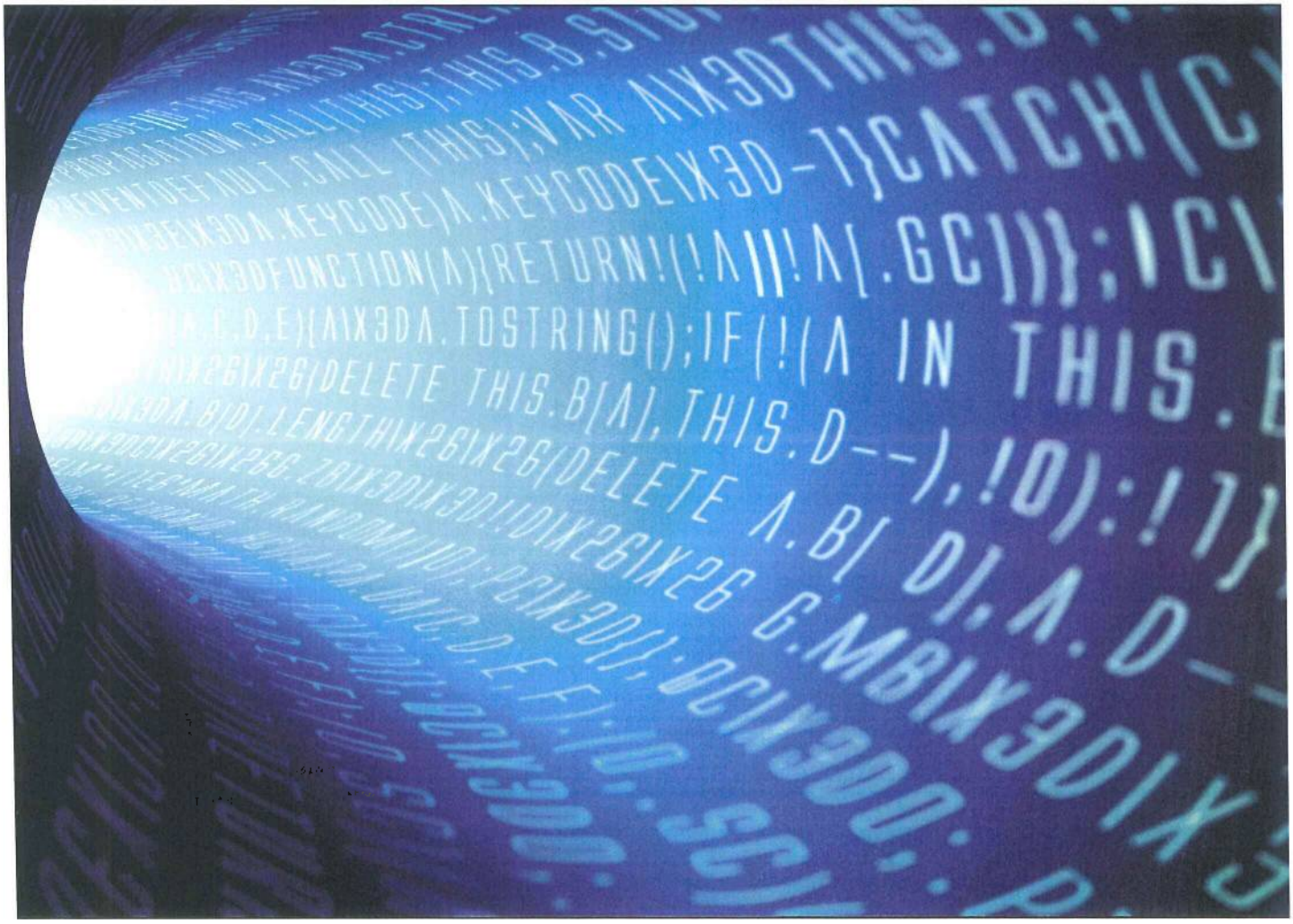
REVUE PRATIQUE DE LA PROSPECTIVE ET DE L'INNOVATION

JUSTICE - DROIT - SOCIÉTÉ

Direction :
Louis DEGOS

OCTOBRE 2017 - **N°2**
2e ANNÉE - ISSN 2497-2703



LexisNexis®

Lexis Kiosque

CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

2

Data Protection Officer et mise en conformité selon le RGPD

Hélène LEGRAS,
DPO New AREVA,
vice-présidente de l'Association Data Protection Officers

LA QUESTION

Qu'apporte le règlement européen du 27 avril 2016 [1] (règlement général sur la protection des données) en matière de protection des données personnelles en Europe ? Concerne-t-il uniquement les pays de l'Union européenne ? Uniformise-t-il les législations européennes, comme le souhaitait Vivien Reding [2] le 25 janvier 2012 lors de sa proposition à la Commission européenne ?

En France, la loi de 1978 [3] appelée « loi informatique et libertés » vise à protéger les personnes. Elle instaure une obligation de déclaration des traitements automatisés de données à caractère personnel auprès de la CNIL (Commission nationale informatique et libertés). Elle a été révisée par une loi du 6 août 2004 [4] et son décret d'application du 20 octobre 2005 [5] qui ont permis la nomination de Correspondants Informatique et Libertés dans les organismes privés et publics. Le régime déclaratif subsiste mais certains organismes ont nommé des CIL, auxquels ils déclarent les traitements mis en œuvre, qui sont répertoriés dans un registre que le CIL tient à la disposition de la CNIL. Le RGPD prévoit la nomination de Data Protection Officer (DPO).

EXPERTISE

Le règlement général sur la protection des données (RGPD) a enfin été adopté le 27 avril 2016, abrogeant la directive 95/46 [6] et transformant l'obligation déclarative en **obligation de conformité**.

Le RGPD, tout en conservant les principes de base de la loi « informatique et libertés », va modifier la protection des données personnelles, qui permettent d'identifier directement ou indirectement une personne et que les entreprises, comme les acteurs du web, ont tendance à beaucoup collecter.

Le RGPD devait à l'origine uniformiser les lois des pays de l'Union européenne. Dans les faits, les particularismes des lois nationales perdurent. Ainsi la loi pour une République numérique du 7 octobre 2016, dite loi Lemaire [7], continuera de s'appliquer concernant le principe du droit à la mort numérique qui permet à une personne d'indiquer, de son vivant, les conditions dans lesquelles ses données personnelles seront conservées et communiquées après sa mort.

De même on pouvait penser que ce règlement européen ne concernait que les 28 pays de l'Union européenne (l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, la Croatie, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lituanie, la Lettonie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni, la Slovaquie, la Slovénie et la Suède). Suite au référendum du 23 juin 2016 en faveur du Brexit, le Royaume-Uni a prévu de quitter l'Union européenne, probablement d'ici 2020, mais va voter une loi avec des dispositions similaires à celles du RGPD.

Le RGPD prévoit que « *Tout traitement de données à caractère personnel qui a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union* » soit effectué conformément au règlement, « *que le traitement lui-même ait lieu ou non dans l'Union* ». Ainsi la filiale américaine d'une société française, qui traite des données en France, devra respecter le RGPD.

Les entreprises devront attester qu'elles sont en conformité avec le texte. Fort heureusement, le RGPD prévoit la nomination de **Data Protection Officer**, devenu délégué à la protection des données en français. Le DPO est une nouvelle fonction différente du CIL. En charge de la conformité, le DPO est amené à contrôler les actions effectuées lors de la mise en place d'un traitement et ce dès sa conception. Il devient l'élément incontournable participant à toutes les réunions et réflexions, donnant son avis et émettant conseils et recommandations.

La CNIL a indiqué 6 étapes pour se mettre en conformité avec le RGPD, dont la première est la nomination d'un pilote. Ce pilote sera le DPO, désigné pour ses connaissances à la fois de l'entreprise, du droit et de l'informatique. Le DPO pilote n'est toutefois pas seul dans l'avion. Il est communicant et s'entoure des autres métiers de son entreprise avec lesquels il échange. Il dispose d'un solide réseau interne constitué des autres experts de l'entreprise car, s'il n'est pas juriste, l'appui de la direction juridique sera précieux pour comprendre et

1. *PE et Cons. UE, règl. 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 n° L 119, 27 avr. 2016, p. 1 ; http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR.*
2. Vice-présidente de la Commission européenne et Commissaire à la justice, aux droits fondamentaux et à la citoyenneté de 2010 à 2014.
3. *L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés : JO 7 janv. 1978.*
4. *L. n° 2004-801, 6 août 2004 : JO 7 août 2004, texte n° 2.*
5. *D. n° 2005-1309, 20 oct. 2005 : JO 22 oct. 2005, texte n° 31.*
6. *PE et Cons. UE, dir. 95/46, 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 : JOUE n° L 281, 23 nov. 1995, p. 31-50.*
7. *L. n° 2016-1321, 7 oct. 2016 pour une République numérique : JO 8 oct. 2016, texte n° 1* ; V. dans ce numéro *RPPI 2017, entretien 4, avec A. Lemaire.*

appliquer tous les textes en vigueur. Le DPO sera aidé par la direction de l'audit et celle des risques pour faire des audits et mesurer les risques liés au traitement. Le RGPD prévoit une analyse d'impact *(Data Privacy Impact Assessment)* si le traitement présente des risques élevés. La direction informatique, le responsable de la sécurité des systèmes d'information seront ses piliers pour gérer la sécurité informatique, ainsi que l'éventuelle direction de la protection qui protège le patrimoine informationnel de l'entreprise car le DPO est le délégué à la protection des données. L'absence de précision peut laisser penser qu'il a en charge la protection de toutes les données de l'entreprise et pas seulement les données personnelles. Il aura aussi son réseau externe, composé principalement de CIL/DPO d'autres organismes, confrontés aux mêmes problématiques.

Le RGPD rend obligatoire le DPO dans 3 types de structures : les autorités et organismes publics (ministères, mairies, préfectures...) ; les organismes dont l'activité de base nécessite un suivi régulier et systématique à grande échelle des personnes concernées (les compagnies d'assurances, les banques...) ; les organismes traitant des données sensibles à grande échelle (les organismes de santé...).

En revanche, une grande entreprise qui gère ses salariés et n'a pas pour activité de base les traitements de ressources humaines, ne fera pas partie des organismes devant obligatoirement se doter d'un DPO. Néanmoins, il est fortement recommandé de désigner un DPO, surtout si l'entreprise avait nommé un CIL, alors que cette désignation était facultative. Le G 29 (Groupement des CNIL européennes) et l'Association Data Protection Officers recommandent la nomination de DPO. Effectivement, le DPO est le pilote de la conformité, qui saura amener son avion sur la piste d'atterrissage. Car on peut réellement parler de vol aérien, avec probablement quelques turbulences liées aux importantes exigences du RGPD. Quant à l'atterrissage, il est prévu **le 25 mai 2018**, date où les autorités de protection, comme la CNIL en France, pourront faire leurs premiers contrôles.

Et nous sommes bien au cœur du business des entreprises, la loi pour une République numérique prévoyant des sanctions pouvant aller jusqu'à 3 millions d'euros [8]. Ces sanctions seront fortement augmentées avec le RGPD, de 10 000 millions d'euros – ou 2 % du chiffre d'affaires mondial – à 20 000 millions d'euros – ou 4 % du chiffre d'affaires mondial – selon l'infraction commise par l'entreprise. Les droits des personnes, au cœur de la loi de 1978, modifiée en 2004, sont confirmés par le règlement qui sanctionne, par exemple, à hauteur de 20 millions d'euros le non-respect du recueil du consentement de la personne ou la collecte d'informations sensibles comme la santé de la personne, ses convictions religieuses ou ses opinions politiques.

La France, championne de la collecte de données à caractère personnel, va devoir apprendre à minimiser cette collecte. La CNIL veille à ce que la collecte de données soit adéquate, pertinente, limitée et proportionnelle avec la finalité du traitement. Le RGPD reprend ce principe dans son article 5. Pédagogue, le DPO devra rappeler au responsable de traitement qu'il faut bien réfléchir à la nécessité de collecter des données personnelles.

Ces données constituent une source de richesse pour les entreprises, que les « pirates de l'informatique » tentent de s'approprier pour en exiger des « rançons ». Tous les jours des piratages se produisent et fort récemment « WannaCrypt » et « Pétya » ont fait la une des journaux et entraîné la mise en place de cellules de crise au sein des entreprises.

C'est pourquoi le RGPD met l'accent sur la protection et la sécurité de ces données. Les entreprises devront mettre en place des mesures techniques et organisationnelles pour assurer une sécurité adaptée aux risques encourus. Cela peut se traduire par une pseudonymisation (transformer la donnée personnelle en un pseudonyme), qui contrairement à l'anonymisation permet de revenir en arrière. Le choix du chiffrement des données peut être décidé. L'entreprise peut aussi mettre en place des moyens permettant de garantir la confidentialité, l'intégrité et la disponibilité des données.

Les éventuelles failles de données personnelles devront être notifiées, dans les meilleurs délais et si possible dans les 72 heures suivant la découverte de la faille, à l'autorité de contrôle. Les personnes concernées par la violation devront aussi être informées, dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

Des procédures internes devront être rédigées et appliquées au sein des entreprises, que ce soit pour le respect du droit d'accès des personnes ou s'agissant de la manière de notifier une violation de données personnelles.

Les sociétés internationales ont des filiales dans des pays hors de l'Union européenne, qui n'ont pas forcément de législation pour protéger les données personnelles. Or, un groupe international doit pouvoir échanger des données avec ses filiales situées dans ces pays. Une solution sera de rédiger des *Binding Corporate Rules*, afin de mettre en place une politique interne d'entreprise pour sécuriser les flux transfrontaliers.

Le système déclaratif était quelque peu administratif. La conformité au RGPD est un vrai challenge pour les entreprises et leur DPO, qu'elles doivent nommer au plus tôt. La nomination doit être largement officialisée en interne et ne pas attendre la date butoir du 25 mai 2018. Il faut que le DPO soit rattaché au niveau hiérarchique le plus haut. Il doit disposer de moyens humains et financiers et d'une lettre de mission, pour lui permettre de faire face à ces travaux herculéens. Il va poser le socle de la maison et progressivement construire les étages. Outre ses qualités et connaissances professionnelles, il saura utiliser ses qualités humaines pour convaincre en interne et mener son organisme à la conformité attendue.

Mots-Clés : Informatique et libertés - Données personnelles - Traitement - Règlement 2016/679, 27 avr. 2016
Informatique et libertés - Data Protection Officer - Missions - Règlement 2016/679, 27 avr. 2016

8. *L. n° 2016-1321, 7 oct. 2016, préc., art. 65 : « La formation restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission. Le montant de la sanction ne peut excéder 3 millions d'euros ».*