Note numéro 34
septembre 2018

Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

Souveraineté et confiance : les enjeux du RGPD [1]

Par le Chef d'escadron Jérôme LAGASSE et l'Aspirant Anthony BRUILLARD

Texte long et austère, sujet complexe et technique, le Règlement général sur la protection des données (RGPD)[2] s'est paradoxalement vu porté, tout au long du printemps 2018, à la une de l'actualité. Notoriété inégalée pour un texte de droit européen : tout le monde connaît désormais le RGPD ; même si souvent c'est au prix d'une compréhension réductrice, « facebookienne », puisque ses principaux vulgarisateurs sont les réseaux sociaux. À l'ère numérique, le RGPD acte du passage de nos sociétés à un droit plus souple (*soft law*). D'un côté, l'État est davantage appelé à jouer un rôle d'accompagnateur, de régulateur, de facilitateur ; et de l'autre, les citoyens et les acteurs économiques sont toujours plus responsabilisés et « en-capacités » (*empowerment*). En outre, il souligne l'influence mondiale que l'Union européenne (UE) entend exercer en faveur des droits de ses citoyens dans l'espace numérique.

Nous verrons, dans un premier temps, pourquoi l'UE avait besoin de se doter de ce nouveau texte et en quoi il représente un acte de souveraineté européen dans le cyberespace. Nous étudierons ensuite la révolution culturelle que représente le règlement, tant du point de vue des responsables de traitement (RT) que des conseillers juridiques et de l'autorité de contrôle (en France, il s'agit de la Commission nationale de l'informatique et des libertés – CNIL).

I. - LE RGPD : UN ACTE QUI AFFIRME LA SOUVERAINETÉ EUROPÉENNE DANS LE CYBERESPACE

A. Pourquoi le RGPD ?

Avant le RGPD, le néant ? – La Commission européenne s'est saisie de la protection des données personnelles au début des années 1990, au moment de l'essor de l'informatique, soit bien après le Conseil de l'Europe et l'OCDE[3]. En la matière, le premier texte substantiel de l'Union est la directive de 1995[4], où figurent déjà les grands principes du RGPD : intégrité des données, licéité de la collecte, régime spécial des données sensibles, droit d'accès et d'opposition, etc. Cependant, ce texte souffrait de son statut de directive, car – contrairement à un règlement – il n'était pas applicable directement dans les États membres et laissait donc subsister, entre les législations nationales, d'importantes disparités d'appréciation. Une divergence dénoncée dès les années 2000 – par la Commission, le Parlement et le Contrôleur européen à la protection des données – comme un obstacle au bon fonctionnement du marché unique. Dans ce contexte, le 4 novembre 2010, la Commission initiait le processus qui, cinq ans et demis plus tard, aboutirait à l'adoption du RGPD. Période marquée par des crises récurrentes en matière de protection des données (affaire *Snowden* notamment) qui ont conduit la Cour de justice de l'UE (CJUE) à développer une jurisprudence[5], dont le règlement porte la marque.

1- Cette note se propose de synthétiser les propos des intervenants de l'atelier de recherche gendarmerie organisé par le CREOGN le 31 mai 2018, à Paris-Bercy. Elle prolonge une réflexion déjà ouverte par le CREOGN dans sa Note n° 22 : https://www.gendarmerie.interieur.gouv.fr/crgn/content/download/818/11959/version/1/file/RGPD-V-4P.pdf

2 - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE – URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679etfrom=FR

3 - L'Organisation pour la croissance et le développement économique. Ses « Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel » datent de 1980. Quant au Conseil de l'Europe, sa Convention n° 108 pour la protection des données personnelles date de 1981.

4 - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données – URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046etfrom=FR

5 - En 2014, dans son arrêt *Google Spain*, la CJUE a réaffirmé le droit à l'oubli, et dans *Digital Rights*, elle limitait le temps de conservation à une durée raisonnable ; en 2016, elle consacrait dans l'arrêt *Schrems* la libre circulation des données hors UE sous réserve d'une protection équivalente à celle de l'UE.

Un texte qui promeut la croissance économique par la confiance des consommateurs dans l'économie numérique – Le RGPD vient protéger un droit fondamental, celui du « droit à la protection des données à caractère personnel », reconnu à tout citoyen européen, depuis 2000, par la Charte des droits fondamentaux de l'UE dans son article 8[6]. De cette manière, il a pour finalité de stimuler la croissance et la compétitivité des entreprises européennes en renforçant la confiance des consommateurs dans l'économie numérique. Ces derniers disposent désormais de toute une gamme de moyens d'action (*e.g.* notification en cas de perte de données ou de faille de sécurité, portabilité des données, droit d'accès, d'opposition, d'effacement, de limitation du traitement, etc.) qui sont pour eux autant d'« outils de réduction de l'incertitude ». Toujours dans ce sens, le RGPD oblige les RT : à utiliser des traitements conçus pour respecter la confidentialité des données (*data protection by design ;* par exemple la pseudonymisation des données collectées) et à ne collecter que les seules données nécessaires (*data protection by default)*[7]. Le règlement impose également aux RT de prouver à tout moment la bonne utilisation et la protection adaptée des données qui leurs sont confiées. Pour coûteuse et longue que soit cette mise en conformité, il permet aux entreprises de disposer *in fine* d'une base de données pertinente et intègre, représentant pour elle un authentique avantage concurrentiel.

Un texte qui introduit un droit plus souple – Le RGPD étend des mesures de droit souple à l'ensemble des États membres de l'Union : code de conduite, certification, analyse d'impact, registre d'activité et, surtout, obligation de disposer d'un délégué à la protection des données (DPD). C'est un changement de paradigme, plus bouleversant dans certains États membres que dans d'autres. Ainsi, l'autorité de contrôle s'oriente vers un rôle d'accompagnateur, de régulateur et de facilitateur. Quant aux RT, ils passent de la logique de déclaration à celle de conformité et de responsabilité (*accountability).* Facteur d'harmonisation, le RGPD laisse néanmoins aux États membres d'importantes marges d'autonomie pour décliner ses dispositions dans leur droit national. Pour la France, le contenu du règlement a été intégré à la loi « Informatique et Libertés » de 1978, par la loi du 20 juin 2018[8]. Cette harmonisation bénéficie également aux entreprises – y compris extra-européennes – en tant qu'outil de cohérence de leurs pratiques et de conformité de leurs systèmes de traitement, mais surtout comme outil favorisant une nouvelle culture d'entreprise, dans laquelle confiance et respect de la vie privée se rejoignent. Le RGPD n'a pourtant pas une vocation générale, certains traitements continuant de relever de plusieurs textes différents et complémentaires. Ainsi, les transferts de données dans le cadre de la coopération policière et pénale internationale sont régis par la nouvelle directive 2016/680[9], et les télécommunications par la directive 2002/58 (jusqu'à son remplacement par le futur règlement *e-Privacy*).

B. Un texte à vocation internationale, témoignage du soft power *européen au XXIe siècle*

Un acte de souveraineté de l'Union européenne – Le RGPD est une illustration du *soft power* européen. Par son biais, l'UE affiche sa volonté de garantir à ses citoyens une protection appropriée de leurs droits à l'ère numérique, mais également son ambition de faire adopter largement ses normes dans le cyberespace (les transferts de données hors UE étant conditionnés à l'existence d'une protection adéquate dans le pays destinataire). Plusieurs États travaillent d'ailleurs déjà à rapprocher leurs normes de celles du RGPD[10].

Des influences réciproques – Si le droit européen de la protection des données personnelles influence bien au-delà des frontières de l'UE, la réciproque est tout aussi vraie. Ainsi, dans le RGPD, l'aggravation des sanctions et la notion *d'accountability* sont inspirées du modèle américain. Quant au concept de data *Privacy by design*, il a été développé au Canada dans les années 1990, par Ann Cavoukian[11], alors Commissaire à l'information et à la protection de la vie privée de l'Ontario. Plus globalement, le RGPD est fortement empreint de la conception américaine du droit souple (*soft law*), fondé sur l'autorégulation, la co-création des normes et les bonnes pratiques.

---

6 - Charte des droits fondamentaux de l'Union européenne, article 8. « 1) Toute personne a droit à la protection des données à caractère personnel la concernant. 2) Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3) Le respect de ces règles est soumis au contrôle d'une autorité indépendante. » - URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:12012P/TXTetfrom=FR

7 - *Data protection by design* et *by default* (en fr. « protection des données dès la conception » et « protection des données par défaut ») sont définies à l'article 25 du RGPD.

8 - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et Libertés », dernièrement modifiée par la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

9 - La directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil – URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679etfrom=FR

10 - Comme le Brésil, le Japon, la Corée du Sud ou Israël. cf. Adam Satariano, « G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog », *The New York Times*, 24 mai 2018 – URL : https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

11 - CAVUKIAN, Ann. « Privacy by Design », 2009. Disponible sur : http://www.ontla.on.ca/library/repository/mon/23002/289982.pdf

Une vocation extra-territoriale évidente, mais source de conflits – Étant donné l'étendue mondiale d'Internet et le fait que parmi les principaux RT actifs dans l'UE, beaucoup sont américains (réseaux sociaux, moteurs de recherche, fournisseurs de boîtes mail, etc.), le RGPD a naturellement vocation à s'appliquer à des entreprises qui n'ont pas leur siège dans l'UE. Certaines sociétés américaines emblématiques ont annoncé être ou se mettre en conformité avec le règlement. Inversement, d'autres puissances peuvent revendiquer l'application de leur législation à des entreprises européennes ou à des données stockées dans l'UE. A cet égard, l'affaire *Microsoft c/ USA* est symptomatique des enjeux que soulève la protection des données gérées par des multinationales, et les disparités de normes entre l'UE et le reste du monde. Cette bataille juridique avait débuté en 2013, après que *Microsoft* a refusé de divulguer les données d'un de ses clients – stockées en Irlande – que lui demandait le FBI. Or, sans attendre la décision de la Cour suprême des Etats-Unis, le Congrès a voté le 23 mars 2018, le *CLOUD Act*[12], intégré à la loi de finances. Ce « cavalier législatif » permet désormais aux autorités des États-Unis d'accéder aux données des entreprises américaines, sur le territoire national comme à l'étranger. Ce faisant, il entre en contradiction avec le RGPD, avec son article 48 notamment, qui prévoit que le transfert de données personnelles ne peut être demandé par un État tiers qu'en vertu d'un accord international. Le RGPD, à cet égard, marque le point de départ d'un long processus de négociations internationales

L'UE a démontré qu'elle souhaite jouer un rôle de premier ordre dans la gouvernance du cyberespace, en imposant des normes innovantes et en suscitant l'adhésion au-delà de ses frontières. Cependant, il reste à savoir dans quelle mesure elle se donnera les moyens de son ambition.

II. - UNE VÉRITABLE RÉVOLUTION CULTURELLE

A. Le RGPD vu par les responsables de traitement : entre opportunité et difficultés pratiques

La mise en œuvre du règlement : l'opportunité d'une meilleure valorisation des données – L'enjeu de la transformation demandée par le RGPD n'a été, globalement, que tardivement appréhendé. Il a souvent permis un *aggiornamento* des pratiques passées et entraîné une prise de conscience de la valeur des données personnelles. Le formalisme de la déclaration qu'adressaient les RT à la CNIL l'avait emporté sur le fond, à savoir la donnée. Le traitement des données sensibles, à l'instar des données de santé, a demandé un travail particulièrement important de mise en conformité. Le ministère de la Santé a ainsi élaboré un référentiel de sécurité dès 2016 ; et il travaille à la mise en place d'un système national des données de santé (SNDS) avec différents niveaux d'habilitation. Ainsi, la sécurité des données n'est-elle plus vue comme un problème de technicien, mais bien comme une affaire de gouvernance, un facteur de compétitivité et de performance, mais aussi – et plus fondamentalement – de bonne réputation.

Le DPD : le difficile rôle d'un chef d'orchestre – Le passage du correspondant Informatique et Libertés (CIL, prévu par la loi de 1978) au DPD n'est pas une révolution, mais une évolution qui répond à la nouvelle philosophie du RGPD. Au carrefour du droit et des nouvelles technologies, le DPD est beaucoup plus polyvalent que son prédécesseur. Surtout, il n'est pas seul, même si sa caractéristique est d'être indépendant. Il agit, en effet, en coordonnateur d'un réseau, ce qui n'était pas le cas du CIL. C'est ainsi qu'en amont des traitements, il se fait l'interface entre le RT, le responsable de la sécurité des services d'information (RSSI) et les concepteurs des systèmes de traitement. Chargé de l'évaluation et de l'analyse juridique en amont, puis de l'analyse d'impact, mais également de la sensibilisation et de la formation des personnels, le DPD entre en relation directe avec les services chargés des traitements. Pour autant, son positionnement varie en fonction de la nature de l'établissement, de sa taille, de sa culture professionnelle et de sa responsabilité sociétale.

La situation des collectivités territoriales : faire face à la dissémination géographique et au manque de moyens – L'étude intitulée *Données personnelles et collectivités territoriales*[13], commanditée par le CREOGN, a permis d'identifier leurs problématiques. Tout d'abord, les rédacteurs ont insisté sur le véritable « trésor national » que représentent les données personnelles détenues par ces collectivités pour le bon fonctionnement de leurs services. Elles sont un véritable livre ouvert sur la vie privée des usagers. Par ailleurs, il apparaît dans cette étude que les pratiques des élus et des agents ne sont pas toujours en conformité avec les règles de protection des données personnelles. Rares sont, dans l'échantillon étudié, ceux qui ont une véritable culture de la sécurité, aussi bien informatique que physique. Tant le stockage que le transfert des données se font souvent sans aucun processus de sécurité adapté. Par exemple, aucune des collectivités sondées n'utilisait de technique de cryptage. Enfin, les RT (en l'occurrence, le maire ou le

12 - Acronyme de *Clarifying Lawful Overseas Use of Data Act* (en fr. Loi précisant l'usage légal de données à l'étranger).

13 - LE HÉNANFF, Anne, DANET, Didier, DE BOISBOISSEL, Gérard. Données personnelles et collectivités territoriales : usages actuels et recommandations, *Étude pour le CREOGN,* 2018. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/content/download/969/14826/version/3/file/Etude%20anonymis%C3%A9e%20donne%CC%81es%20personnelles%20et%20collectivit%C3%A9s%20territoriales_CREOGN%20annexes-1.pdf

président de communauté de communes) avaient une vague conscience de leurs responsabilités, se reportant pour cette question sur leurs services juridiques et techniques. La crise causée en 2016 par le *ransomware*[14] *Locky* avait déjà sonné comme un rappel à l'ordre. Si un changement de culture est déjà en marche, l'application du RGPD pose surtout un problème de moyens aux petites collectivités. Ni les élus, ni les directeurs généraux des services ne sont des experts. Aussi l'étude préconise-t-elle la désignation de « structures de soutien » aux échelons national, régional et local, l'encadrement des relations aux prestataires extérieurs et le recrutement du DPD au niveau de l'intercommunalité.

B. Regards croisés de l'autorité de contrôle et d'un praticien du droit

Le big-bang *du 25 mai n'a pas eu lieu…* – Le RGPD n'a pas été la grande révolution annoncée par certains ou redoutée par d'autres. La CNIL a d'ailleurs effectué une grande campagne de dédramatisation à ce sujet. Ainsi, dans la plupart des cas, le règlement ne fait que réaffirmer des obligations inscrites dans le droit français depuis quarante ans. La durée de conservation, l'obligation d'information des personnes ou le droit d'accès remontent à la loi de 1978. Le RGPD ne raisonne pas en terme de taille des entreprises, mais de sensibilité des informations traitées. Par conséquent, pour une structure modeste dont le métier n'est pas le traitement de données personnelles ou une petite collectivité territoriale, l'effort de mise en conformité est infime, si au préalable elle était en conformité avec la loi « Informatique et Libertés »...

Des efforts de mise en conformité très variables en fonction des RT – Les grandes entreprises ont généralement commencé rapidement à s'approprier le RGPD : entre 15 et 18 mois avant le 25 mai, soit quelques mois seulement après la publication du règlement. Pour les entreprises de taille intermédiaire (ETI) et les petites et moyennes entreprises (PME), l'effort a été beaucoup plus tardif (entre 5 et 9 mois auparavant). L'insuffisance des ressources (financières et/ou humaines) en est une raison, mais le manque d'informations est tout aussi déterminant, beaucoup d'entreprises s'étant d'ailleurs contentées d'attendre la publication des fiches rédigées par la CNIL. Quant à l'acculturation, elle dépend beaucoup du secteur d'activité. Enfin, la mise en œuvre des outils de gouvernance suppose une concertation entre services et des prises de décision de la part des directions qui font encore souvent défaut.

La CNIL, de moins en moins « gendarme », de plus en plus accompagnatrice – Le RGPD est un changement extrêmement profond pour la CNIL et ses homologues européens. La Commission profite de la fin des obligations de déclaration pour renforcer son rôle d'accompagnateur. Si la CNIL peut désormais sanctionner plus lourdement les contrevenants[15], elle ne souhaite pas s'inscrire dans une approche strictement répressive, mais jugera des objectifs fixés et des efforts entrepris par les RT. De plus, elle se trouve impliquée davantage dans le réseau européen des autorités de contrôle (le G29). L'harmonisation offerte par le RGPD et le système du « chef de file » offrent un front uni des autorités de contrôle face aux grandes plates-formes numériques qui se jouaient jusque-là des compétences nationales au sein de l'UE.

En somme, le RGPD n'est pas une construction *ex nihilo*, ni un *big-bang*. Nous avons vu combien il doit aux textes qui l'ont précédé et aux influences extérieures. Œuvre d'harmonisation, il poursuit la construction européenne en étendant des règles plus protectrices : témoin de sa puissance normative mise au service des droits de ses citoyens, et de son ambition de s'affirmer comme une grande puissance dans l'espace numérique. Cependant, le règlement impulse une véritable révolution culturelle et un nouveau rapport à la donnée. Les efforts liés à sa mise en œuvre ont souvent révélé le « trésor » que constituent les données personnelles. Celles-ci sont désormais au cœur de l'activité de toute entreprise, de toute administration. Avec le RGPD, l'UE pose un acte de souveraineté dans le cyberespace, et nombre de pays déjà se rallient à la vision européenne. Le *CLOUD Act*, d'une certaine manière, est la réponse américaine à ce *soft power* européen. Plus qu'une simple liste d'obligations, plus qu'un nouveau rapport à la donnée, le RGPD modifie les rapports géopolitiques des puissances dans le cyberespace.

14 - « Technique d'attaque courante de la cybercriminalité, le rançongiciel ou *ransomware* consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement. » (définition de l'ANSSI – cf. URL : https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/rancongiciel/

15 - En cas d'infraction, les CNIL peuvent désormais imposer des amendes atteignant 20 millions d'euros, ou 4 % du chiffre d'affaires global d'une entreprise (cf. article 83-6 du RGPD).