Note numéro 22
Mars 2017

Note du CREOGN

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

Le Règlement général de protection des données : vers une « grande charte des libertés » de l'identité numérique ?

Publié au Journal officiel de l'Union européenne du 4 mai 2016, le Règlement général (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 est entré en vigueur le 25 mai 2016. La publication de ce Règlement est à mettre en perspective avec le huitième centenaire de la *Magna Charta*[1] qui consacrait déjà comme idée essentielle la garantie des libertés. Le présent règlement aura force de loi à partir du 25 mai 2018 et sera *in extenso* opposable devant toutes les juridictions des 28 États membres de l'Union européenne. Durant cette période transitoire, aucun État membre ne pourra légiférer de manière contraire aux dispositions de celui-ci. Au final, ce texte achève d'unifier les 28 différentes législations Informatiques et Libertés des États membres en général et plus particulièrement en France à travers la loi n°78-17 informatique et libertés du 6 janvier 1978[2]. Désormais, la protection des données à caractère personnel relève d'un *corpus* juridique unique transposable de manière directe dans la législation des États de l'UE. Nous verrons au cours des commentaires de cette note qu'un des effets majeurs de ce texte réside dans une définition commune relative aux données à caractère personnel, définition somme toute mouvante qui n'a cessé jusqu'à présent d'alimenter le débat tant dans la doctrine que dans la jurisprudence. S'agissant de la philosophie générale qui a guidé les rédacteurs, ce règlement se veut, selon la Commission européenne, la posture politique et juridique adaptée « *afin de mieux répondre aux défis posés par la rapide évolution des nouvelles technologies* [3]». Le contenu de ce règlement contient des dispositions dont la mise en application et l'interprétation vont influencer de manière profonde les fondements des sociétés démocratiques en Europe durant la décennie à venir. Ce texte devrait impacter indirectement les modalités concrètes des politiques de sécurité publique des États européens sous le couvert de deux directives publiées à la même date. La présente note se cantonnera aux points essentiels du Règlement qui constituent, en ce sens, les fondements d'une grande charte « numérique » européenne des libertés, destinée à protéger les citoyens des excès actuels et potentiels de ce nouvel espace. Le Règlement général de protection des données (RGPD) donne une définition commune de la donnée à caractère personnel et des données sensibles qui, *de facto,* délimite une sorte de bulle de protection (I) au profit des citoyens. Dans le cadre de cette bulle, ces derniers bénéficient de droits renforcés (II) qui permettront, face à des actes susceptibles de porter atteintes à leurs droits fondamentaux en matière d'identité numérique, de mieux répondre à ces formes d'ingérence. Enfin, les sanctions de nature administrative, la nomination de délégués à la protection des données alliées à un mode de gouvernance des données fondé sur les principes d'*accountability*[4] et de *compliance*[5] devraient rendre le dispositif efficient (III).

1 *Magna Carta Libertatum,* Grande Charte des libertés (anglaise), imposée par les barons anglais au roi Jean sans Terre en 1215, pour le contraindre à reconnaître et à protéger les libertés et les privilèges de la noblesse – Dictionnaire de la science politique et des institutions politiques, Armand Colin, 8e édition, 2015, p.176.

2 On pourra se reporter au rapport d'information de l'Assemblée nationale (AN n°4544), du 22 février 2017, rédigé par Mme Anne-Yvonne Le Dain et M. Philippe Gosselin, Députés. http://www.assemblee-nationale.fr/14/pdf/rap-info/i4544.pdf

3 JOUE - 04052016- L119/2 – Considérant 6.

4 *Def : « Terme anglais signifiant l'obligation de rendre compte de son action et d'en assumer la responsabilité ». Cf, Lexique de science politique, vie et institutions politiques, Dalloz, 3éme édition, p.2*

5 Anglicisme pouvant se définir comme *« la conformité et l'ensemble des processus qui permettent d'assurer le respect d'une part, des valeurs et d'un esprit éthique insufflées par les dirigeants. Leur non-respect peut entraîner des sanctions judiciaires ou administratives, des pertes financières ou une atteinte à leur image ou à la réputation».*

I - Une définition unique de la donnée à caractère personnel au sein de l'espace européen

Le Règlement européen ne s'applique pas aux champs qui touchent à la souveraineté *lato sensu* des États membres en matière de sécurité nationale[6]. S'agissant de la France, la loi du 24 juillet 2015 relative au renseignement en est par nature exclue. Le RGPD n'interfère pas non plus avec certains aspects ayant trait aux traditions, cultures et croyances des peuples qui composent l'Union européenne. Ainsi, les données à caractère personnel des personnes décédées ne relèvent pas de la compétence du règlement[7]. Globalement, le RGPD étend sa protection aux individus dans leurs actes touchant à la vie sociale, professionnelle et économique. Toutefois, le règlement prend soin de ne pas entraver les activités de nature innovante, prenant leur source dans le traitement des données à caractère personnel, dès lors qu'elles sont fondées sur des fins d'intérêt général.

a – Une harmonisation de la définition des données à caractère personnel et sensibles

Cette définition consolidée va conduire les Autorités de contrôle indépendantes[8] (ACI) et les juridictions à rendre leur décision en se référant au contenu de l'article 4 du Règlement qui entend par données à caractère personnel : « *Toute information se rapportant à une personne physique identifiée ou identifiable [ ] ;est réputée être* ***"une personne physique identifiable"*** *une personne physique qui peut être identifiée, directement ou indirectement, notamment* ***par référence à un identifiant****, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale».* Le Règlement européen a vocation à réguler le rôle de tout responsable d'un traitement automatisé de données, ses éventuels sous-traitants proposant des biens ou des services à l'égard de personnes situées dans l'Union européenne[9]. Le législateur européen a précisé de manière plus spécifique les notions des données sensibles touchant la génétique, la biométrie et la santé[10]. De même, sur le plan de la capacité juridique des mineurs à consentir à la finalité du traitement de leurs données à caractère personnel, le règlement laisse une marge d'appréciation aux États. L'article 8 du Règlement encadre cette capacité juridique entre 13 et 16 ans [11].

b – Une conciliation de l'intérêt général et de l'intérêt particulier

Les rédacteurs ont eu le souci de trouver un point d'équilibre délicat, qui veille au respect des droits fondamentaux de la personne, sans pour autant entraver les échanges de flux de données à caractère personnel. Ce point d'équilibre veut créer un pôle de stabilité et de confiance au sein des sociétés démocratiques pour éviter de les fragiliser dans leur fondement. Le considérant n°4 du Règlement dispose : *« Le droit à la protection des données à caractère personnel* ***n'est pas un droit absolu*** *; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux,* ***conformément au principe de proportionnalité ».*** L'article 9-2 prévoit trois cas d'exception que sont le respect d'une obligation légale, l'accomplissement d'une mission d'intérêt public et enfin permettre l'exercice d'une compétence d'une autorité publique. Dans ces trois hypothèses, l'article 9-1 qui pose pour préalable la prohibition de révéler certaines données à caractère personnel[12] ne s'applique pas.

---

6 Deux directives européennes ont été publiées le même jour que le règlement : directive 2016/680 relative à la protection des personnes physique 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 ; directive 2016/681 relative à l'utilisation des données passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité ainsi que pour les enquêtes et les poursuites en la matière. Sur ce dernier point, cf note n°19 du CREOGN.
http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Fichier-PNR-surveillance-electronique-de-masse-ou-nouveau-paradigme-de-la-securite

7 Cf : JOUE, 04/05/2016 – L119/5 - Considérant n°27.

8 En France, la Commission nationale informatique et liberté.

9 Le terme Union européenne comprend ici les États membres de l'espace économique européen, c-a-d : les 28 membres de l'UE ainsi que l'Islande, le Liechtenstein et la Norvège.

10 Cf Art.4-13,14 et 15 du RGPD p. L.119/34

11 Droit positif français du traitement des données à caractère personnel d'un mineur : cf Loi 2016-331 du 7 octobre 2016 *pour une République numérique* – Art. 56, 63 – Dispositions reprises et insérées respectivement aux articles 58 et 40 de la Loi 78-17 du 6 janvier 1978 *informatique et libertés.*

12 Art9.1 : *« Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits ».*

II – Des droits et des contrôles renforcés, assortis de sanctions administratives dissuasives

Le RGPD accorde à toute personne une capacité d'agir vis-à-vis de tout responsable ou sous-traitant d'un système de traitement automatisé de données (STAD). Ces deux acteurs doivent s'assurer du consentement libre et éclairé de celui qui accepte de confier des éléments substantiels de sa personnalité parfois intime. Dans ce dispositif, l'ACI tient un rôle clé en termes de contrôle externe et de prononcé de sanctions administratives. De plus, sur le plan du contrôle interne, le règlement prévoit, en fonction de l'effectif de l'entreprise et/ou de la nature de ses activités, de nommer un *Data protection officer (DPO)*[13] doté d'un mandat spécifique. Tous ces changements ne sont pas neutres dans l'édification d'un nouveau mode de gouvernance des données.

a – À espace nouveau, droits nouveaux

À l'instar de textes fondamentaux comme la *Magna Charta,* qui ont reconnu un certain nombre de droits pour s'opposer à l'arbitraire du pouvoir, le RGPD a la volonté de conférer aux citoyens des moyens visant à contrecarrer les excès des sociétés de l'information. Le coeur du dispositif de cette loi repose sur le consentement qui se définit, selon le règlement, comme : « *toute manifestation de volonté,* ***libre, spécifique****,* ***éclairée*** *et* ***univoque*** *par laquelle la personne concernée accepte par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement*[14] *»*. Ce consentement a pour effet de faire endosser l'obligation d'*accountability* à tout responsable de traitement.
Ledit consentement est aussi renforcé par l'octroi de prérogatives en faveur des internautes visant à s'assurer du respect de la bonne gouvernance des données par les STAD fondée sur les principes de transparence et de traçabilité. Ce « pack de bonne gouvernance des STAD » comprend tout un ensemble de droits qui fait l'objet d'un chapitre spécifique[15]. Parmi ceux-ci, deux mesures ont retenu l'attention des juristes : le droit à l'effacement (« droit à l'oubli ») et la pratique du profilage. L'article 17 du Règlement consacre le droit à l'effacement proclamé en son temps dans l'arrêt *Google Spain* par la Cour de Justice de l'Union Européenne (CJUE)[16]. Il en découle que, sous réserve d'un des six motifs prévus par l'article 17, *« la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais ».* En corollaire de ce qui précède, les décisions individuelles automatisées, plus connues sous la pratique du profilage[17], interrogent sur le devenir de la théorie juridique de l'autonomie de la volonté. En effet, le perfectionnement des algorithmes prédictifs couplés avec l'intelligence artificielle va accroître les capacités des décisions individuelles automatisées avec pour risque majeur des erreurs manifestes d'appréciation et une déresponsabilisation accrue. Pour prévenir ces deux écueils, l'article 22 reconnaît à « *la personne concernée le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire».* Pour autant, ce droit ne revêt pas un caractère général et absolu, il prévoit des exceptions dans un champ très limité… Enfin, dans le cadre des politiques de transparence et de confiance que devront susciter les sociétés de la nouvelle économie en direction des citoyens, les articles 33 et 34 obligent les entreprises de signaler toutes violations relatives aux données personnelles tant à l'ACI qu'au(x) personne(s) concernée(s).

b – Une régulation de la donnée combinant des dispositions de *hard law* et de *soft law*[18]

Le Règlement a tiré les conséquences des sanctions très limitées que prévoyait la directive 95/46/CE du 24 octobre 1995. Nombre de commentateurs avaient souligné que la sanction pécuniaire publique prononcée par

13 Terme anglais signifiant Délégué à la protection des données (DPD). Le DPD se substitue au Correspondant informatique et libertés (CIL) avec des prérogatives plus élargies. Pour des applications concrètes, Cf : www.cnil.fr/fr/consultation-reglement-europeen/dpo
14 Idem texte note 3 – L119/34, art. 4-11).
15 Cf Chapitre III : *Droits de la personne concernée, JOUE du 4mai 2016, L.119/39.*
16 Arrêt du 13 mai 2014 accessible sur le lien ECLI:EU:C:2014:317
17 Cf Art 4-4 définit le profilage comme : « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».*
18 Soft law : « *expression de langue anglaise désignant, dans le domaine du droit, les règles non obligatoires et qui ne sont passibles d'aucune sanction juridictionnelle », se traduit souvent par « droit mou », « droit souple » ou encore « droit flou ».*

la CNIL à l'encontre de la société Google Inc[19]pour un montant de 100 000 euros n'avait pas, comme le mentionne le Règlement, un caractère « *effectif, proportionné et dissuasif »*. Désormais, les ACI seront en mesure d'infliger des sanctions pouvant atteindre un *quantum* de 10 millions voire 20 millions d'euros ou pour une entreprise un montant égal à 2 ou 4 % du chiffre d'affaires annuel mondial global généré. Pour autant, le règlement laisse aux États l'initiative dans l'édiction de sanctions pour d'autres violations non prévues dans le Règlement. Ces dispositions de type *hard law* sont censées asseoir immédiatement la légitimité du RGPD face aux « *GAFA*[20] ». Le volet préventif est néanmoins présent en amont pour détecter les manquements intentionnels ou non que pourrait commettre un responsable de traitement ou un sous-traitant. Le Règlement instaure ainsi un *DPO* pour les autorités et organismes publics (sauf les juridictions) mais aussi les entreprises dont les activités de base touchent à des opérations à grande échelle. Investi d'un mandat, le *DPO* : « *ne reçoit aucune instruction en ce qui concerne l'exercice des missions* ». Ce dernier « *ne peut être relevé de ses fonctions ou pénalisé par le responsable […] pour l'exercice de ses missions* ». Le *DPO* aura par exemple vocation à contrôler la conformité du registre des activités de traitement (art.30), véritable certificat de traçabilité de l'ensemble des flux des données personnelles réalisé dans le temps. Le second volet de la régulation des données s'articule autour d'un droit souple (*soft law*). Ce droit repose sur des mécanismes de certification mais aussi d'incitation à rédiger dans tous les secteurs de traitement des codes de bonne conduite (art.40). En lieu et place de la déclaration préalable d'un STAD se substituera une obligation déclarative de conformités au règlement. Il reviendra aux structures concernées d'informer leurs clients et partenaires de l'obtention des certifications recommandées selon leur secteur de traitement. Dans une volonté de parvenir à des politiques d'harmonisation des normes de certification dans l'UE, le règlement mentionne qu'il sera possible de recourir à des certifications communes sous l'appellation d'un « *label européen de protection des données* ». De ce fait, la *e-réputation* d'une entreprise, plus spécifiquement son mode de gouvernance dans la gestion des données personnelles, s'appuiera principalement sur l'obtention de certifications de haut-niveau et le respect des clauses inscrites dans les codes de bonne conduite. Cette nouvelle approche dans la régulation des données personnelles oriente les pratiques normatives des entreprises et entités vers une tendance très marquée, notamment portée sur les valeurs nord-américaines de *compliance*[21].

Conclusion

Le RGPD pourrait constituer à terme un texte qui, par ses aspects, donne du sens à la construction européenne. Loi fondamentale en devenir, le règlement a pour ambition, par sa sphère de compétence territoriale qu'il entend assumer, d'influer sur les *GAFA* et par-delà la perception nord-américaine des données à caractère personnel. La philosophe du droit, Antoinette Rouvroy, rappelle dans son rapport[22],à destination du Conseil de l'Europe, cette opposition entre l'approche américaine dite « *law and economics* [23]*»* et celle de l'Europe qui consiste à considérer les données « *en fonction du pouvoir qu'elles confèrent à ceux qui les contrôlent, et à tenter de prévenir de trop grandes disparités informationnelles et de pouvoir entre les responsables de traitement et les individus »*. Il reviendra à la CJUE d'interpréter et de révéler toutes les potentialités de ce texte. Comme l'avait mis en évidence le philosophe français Claude Lefort, Machiavel découvre que : « d*ans une cité libre, la loi n'est pas une œuvre de la froide raison, mais le fruit du heurt de deux désirs illimités, le désir des Grands de toujours posséder davantage et celui du peuple de ne pas être opprimé. Aussi la loi n'est-elle jamais donnée une fois pour toute : elle demeure ouverte aux conflits qui toujours conduisent à la réformer*[24]*».*

19 Délibération n°2016-054 du 10 mars 2016 et formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000032291946

20 Acronyme désignant Google, Apple, Facebook et Amazon.

21 À la différence du mot français « conformité », qui désigne un é*tat* de correspondance à la norme, le mot anglais *compliance* désigne une procédure de *normalisation*, c'est-à-dire une programmation du fonctionnement de l'entreprise. Alain SUPIOT, *La Gouvernance par les nombres, Cours au Collège de France (2012-2014),*Fayard, Coll. Poids et mesure du monde, Paris, 2015, p.404 *www.cercledelacompliance.com/app/download/5783911672/Retranscription+Conf%C3%A9rence+Cercle+De+la+Compliance+26012012.pdf*

22 Rapport: « *des données et des hommes. Droit et libertés fondamentaux dans un monde de données massives » p.*7 http://docplayer.fr/13907024-Des-donnees-et-des-hommes-droits-et-libertes-fondamentaux-dans-un-monde-de-donnees-massives-antoinette-rouvroy.html

23 Cette approche « *incite à favoriser, dans la distribution des ressources (et les données numériques sont des ressources), les acteurs les plus susceptibles de les faire fructifier. C'est par l'organisation d'un marché des données, y compris les données personnelles considérées, dans cette perspective, comme des biens commercialisables[…], permettant aux individus de négocier la communication de « leurs » données contre rétribution pécuniaire ou contre d'autres avantages […] que les partisans de l'approche « law and economics » entendent favoriser la croissance et l'innovation dans l'économie numérique.*-Cf Ref idem n°22

24 Cf idem ouvrage note 21, p.114.