UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

DPO

DÉLÉGUÉ À LA PROTECTION
DES DONNÉES

LA REVUE DU DPO

Rétrospective 2018

MARS 2019 • N°1

SOMMAIRE

Nous avertissons le lecteur que les articles ont été écrits, pour la plupart d'entre eux, au premier semestre de l'année 2018.
Aussi, ces derniers ne font pas l'objet d'une actualisation des récents développements en matière de données personnelles.

LA PROTECTION DES DONNÉES PERSONNELLES : PANORAMA ANNUEL

Bénédicte FAUVARQUE-COSSON,
Professeur, université Paris II Panthéon-Assas
Co-directrice du Diplôme d'université « Délégué à la protection des données »,
université Paris II Panthéon-Assas

Le Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des données[1], dit « RGPD », s'applique depuis le 25 mai 2018. Ce règlement promeut un modèle européen ambitieux de protection des données. Il tient compte des enjeux de souveraineté numérique ainsi que de l'impératif de compétitivité des entreprises européennes sur la scène internationale. Il s'inscrit dans le paquet européen de protection des données qui établit un cadre global pour le traitement des données à caractère personnel, dans les secteurs public et privé, en matière civile et pénale, dans lequel se trouve aussi la directive (UE) 2016/680 relative aux traitements mis en œuvre 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[2] (directive « police », transposée par la loi de 2018 relative à la protection des données personnelles[3]).

Ce règlement ne construit pas sur terrain vierge. La protection des données existe depuis 40 ans en France et la France a été un pays moteur des développements du droit européen en la matière. Un socle européen a été établi par la directive 95/46/CE, 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[4]. C'est sur ce socle juridique, enrichi d'autres instruments et de toute la jurisprudence de la Cour de Justice de l'Union Européenne (« CJUE »), que s'est façonné le RGPD (I). Tout en construisant sur de solides bases, il a opéré de profonds changements et imposé de nouvelles exigences aux entreprises, qu'elles soient européennes ou non (II).

1. 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 (règlement général sur la protection des données).
2. 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.
3. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1).
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.

I. LE CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES

A. Un règlement européen, une loi française

Dans les années 70, l'objectif était de reconnaître des droits nouveaux aux citoyens face aux grands systèmes centralisés d'informations dont se dotaient les administrations. En conséquence, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[5], fondatrice du système français et européen actuel de protection des données, vise le secteur public et privé, les traitements automatisés et pour certains fichiers les traitements manuels. Elle énonce le principe fondamental suivant : l'informatique doit être au service des citoyens[6].

Adaptée à plusieurs reprises pour tenir compte des évolutions technologiques et sociales, cette loi a fait preuve d'une extraordinaire longévité.

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique[7] (« loi Lemaire ») l'a complétée, par un chapitre sur la protection de la vie privée en ligne (articles 54 et suivants) qui introduit notamment le principe d'auto-détermination informationnelle. « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi »[8]. La loi Lemaire crée aussi un droit à l'oubli pour les mineurs et un droit à la maîtrise de ses données post-mortem (la « mort numérique »[9]), sujet absent du RGPD.

L'Assemblée nationale a adopté, après l'échec de la commission mixte paritaire le 6 avril dernier, le projet de loi adaptant le droit français au Règlement européen sur la protection des données personnelles (RGPD) le 14 mai 2018. Après un passage devant le Conseil Constitutionnel le 16 mai 2018, la loi a été promulguée par le président de la République le 21 juin 2018. Cette loi complète le Règlement européen[10] et modifie de nouveau la loi de 1978.

La loi sur la protection des données personnelles[11] qui adapte la loi Informatique et libertés[12] au Règlement général sur la protection des données (RGPD)[13] a été définitivement adoptée par l'Assemblée nationale mardi 14 mai et promulguée le 20 juin, mais pour des raisons d'économie légistique, la loi n'a pas

5. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
6. Article 1er de la loi.
7. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (1).
8. Article 54 de la loi.
9. Article 63 de la loi.
10. La loi permet d'exercer certaines des « marges de manœuvre nationales » autorisées par le RGPD.
11. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1).
12. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
13. 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 (règlement général sur la protection des données).

reproduit tout le règlement, affectant ainsi la lisibilité du droit positif[14]. Elle autorise le Gouvernement à adopter par voie d'ordonnance les mesures nécessaires à la réécriture de la loi Informatique et libertés afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence des règles de protection des données. Cette ordonnance, qui sera prise après avis de la Commission nationale de l'informatique et des libertés (« CNIL »), devra être adoptée dans un délai de 6 mois à compter de la promulgation de la loi et ratifiée dans un délai de 6 mois à compter de sa publication.

Après la transposition de la directive de 1995 relative à la protection des données personnelles, d'assez grandes divergences entre les législations des États membres ont subsisté : les autorités de régulation étaient dotées de pouvoirs différents, la concurrence était parfois faussée et les droits des personnes concernées différemment protégés selon les Etats membres. L'Europe a donc fait le choix, justifié, de réviser la Directive et de la transformer en règlement. Par sa nature même (un règlement, non une directive) le RGPD n'a pas à être transposé. Ce règlement est néanmoins « hybride » en ce qu'il laisse des espaces de liberté laissés aux États membres. Ainsi, le RGPD laisse aux Etats membres la possibilité d'apporter des précisions ou des limitations aux règles qu'il prévoit[15]. Cela joue notamment pour les données sensibles, le régime des sanctions pénales applicables en cas de violation des principes du règlement, les critères de déclenchement des sanctions administratives, les conditions de licéité des traitements, les conditions d'âge s'agissant de la protection des mineurs (question très débattue par le législateur français), l'encadrement du droit à l'effacement, etc. Le Secrétariat général des affaires européennes, responsable du suivi des négociations pour la France, a comptabilisé 56 marges de manœuvre renvoyant au droit national. Le chapitre IX du RGPD laisse encore aux Etats le pouvoir d'adopter des règles qui concilient cette protection et celle de la liberté d'expression et d'information, y compris le traitement à des fins journalistiques. Il permet aux Etats de prévoir certaines dérogations pour les traitements à des fins de recherche scientifique ou historique ou à des fins statistiques. La loi de 2018 ne prévoit pas de telles dérogations, ce qui paraît étonnant compte tenu de l'ambition française en matière de recherche, notamment dans le domaine de l'intelligence artificielle. Dans la mesure où certaines marges de manœuvre touchent des sujets pratiques importants (tels que l'âge ou les sanctions), certaines disparités, parfois difficiles à gérer pour les groupes qui ont différentes filiales dans plusieurs Etats membres, subsistent.

La loi française prévoit l'adoption de nombreux décrets en Conseil d'Etat et autorise le Gouvernement à adopter par voie d'ordonnance les mesures nécessaires à la réécriture de la loi Informatique et libertés afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence des règles de protection des données[16]. Cette ordonnance prise après avis de la CNIL devra être adoptée dans un délai de 6 mois à compter de la promulgation de la loi et ratifiée dans un délai de 6 mois à compter de sa publication.

14. La délibération n° 2017-299 du 30 novembre 2017 portant avis sur le projet de loi relatif à la protection des données personnelles de la CNIL relève que « le choix fait est d'autant plus dommageable que la loi du 6 janvier 1978 constitue, par son objet et par son rayonnement aux niveaux européen et international, l'un des grands marqueurs du droit français, connu et pris comme standard ». Elle regrette encore cette « occasion manquée de procéder à un réexamen global du droit de la protection des données en France ». Dans un contexte marqué par la reconnaissance de nouveaux droits aux citoyens et le renforcement de la responsabilité des opérateurs, la CNIL recommande que des dérogations nationales au règlement ne soient adoptées « que lorsque celles-ci sont réellement justifiées » (notamment en matière de données de santé).

15. Considérant n° 8, RGPD.

16. Article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

B. Une autorité de contrôle française, un réseau européen d'autorités, un comité européen de la protection des données

Les pouvoirs de la CNIL ont été adaptés pour respecter les dispositions du RGPD. Parce que les données circulent librement dans un monde ouvert, la mise en place d'une coopération européenne et internationale est un enjeu stratégique. Pour l'Europe, les choses se mettent en place. Non seulement le RGPD renforce les pouvoirs des autorités de contrôle nationales, mais un « comité européen de la protection des données », indépendant, est institué en tant qu'organe de l'Union[17]. Le système antérieur, qui résultait de la directive de 1995, avait conduit à la création dans chaque Etat membre d'une ou plusieurs autorités de contrôle aux pouvoirs inégaux, et le Groupe de l'Article 29[18], institué par l'article 29 de cette directive, n'avait pas assez de pouvoir pour uniformiser les pratiques. Les missions et pouvoirs du comité européen de la protection des données sont précisés aux articles 70 et 71 du RGPD. Ainsi, l'application de la réglementation européenne est assurée de manière coordonnée et décentralisée par les autorités de régulation nationale, avec toutefois un mécanisme de coopération inédit.

Cela a été relevé par le Conseil d'Etat, dans son Avis n°393836 du 7 décembre 2017 « sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés »[19]. L'Avis souligne qu'il s'agit là d'un système de coopération « sans précédent », qui va plus loin que la coopération souple entre autorités sans toutefois créer un modèle intégré où les autorités nationales exerceraient en commun une compétence de l'Union[20]. Non seulement leur compétence matérielle et territoriale est clarifiée, mais l'exercice de leurs pouvoirs est « articulé », ce qui permettra l'application uniforme du Règlement et garantira une plus grande sécurité juridique aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union. En cas de désaccord entre ces autorités, un comité les réunissant tranchera les différends, selon des règles de majorité qualifiée.

La coopération s'organise aussi, quoique de manière moins poussée, au niveau international, entre les différentes instances supranationales concernées (OCDE, Conseil de l'Europe, zone de Coopération Économique de l'Asie-Pacifique, etc.)...

Le régime juridique de la protection des données se développe à partir d'instruments de droit dur (le règlement, de la loi, mais aussi, même s'il n'en sera pas question dans ce bref article, les conventions internationales et la jurisprudence), mais aussi à partir du droit souple et des nouveaux outils de la mise en conformité.

17. Article 68, RGPD.
18. Le G29 est un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales de chaque état membre de l'Union Européenne.
19. Avis du Conseil d'État - Assemblée nationale n°393836 du 7 décembre 2017 « sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».
20. Paragraphe 2 de l'Avis.

II. D'UNE LOGIQUE DE DÉCLARATION À UN PROCESSUS DE MISE EN CONFORMITÉ GÉNÉRALISÉE

A. Le changement de logique

Contrairement à ce qui se dit souvent (avec un effet médiatique assuré), l'apport essentiel du règlement n'est pas tant d'avoir durci les sanctions, que d'avoir abandonné la logique des déclarations et ce, au profit d'une autre logique, fondée sur une mise en conformité généralisée et continue. Mise en conformité, *compliance,* responsabilisation des acteurs, documentation, corégulation, *privacy by design et by default* deviennent les maîtres-mots. Il en résulte que le rôle de la CNIL, s'il reste évidemment de contrôler (ses pouvoirs d'investigation et de sanctions sont même renforcés), devient prioritairement celui d'accompagner et de permettre la mise en conformité. Acteur majeur de la coopération entre les régulateurs, la CNIL, régulateur des données personnelles, « accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits ».[21] C'est même la première de ses missions.

Les « déclarations CNIL » sont remplacées par l'obligation pour le responsable de traitement de mettre en œuvre des « mesures techniques et organisationnelles appropriées » pour s'assurer et démontrer la conformité du traitement au Règlement[22]. En pratique ces mesures peuvent inclure des politiques internes de protection des données telles que la formation du personnel, des audits internes des activités de traitement ; les entreprises peuvent aussi adhérer aux codes de conduite et / ou aux systèmes de certification approuvés. Les autorités de contrôle (la CNIL en France) sont chargées de vérifier le respect de l'ensemble de ces obligations (logique de compliance). Cette nouvelle logique de contrôle *ex post* s'appuie sur l'essor des instruments de droit souple, destinés à « faciliter sa mise en œuvre ».[23]

Il n'est qu'à consulter le site de la CNIL (et des autres autorités nationales en la matière) pour découvrir, au-delà des traditionnelles « recommandations », toutes sortes d'autres outils : fiches pratiques, glossaire et lexique, guides (par exemple, le guide sur la sécurité des données), formulaires types de notification de violation des données personnelles. On y trouve aussi les versions françaises des lignes directrices du G29, telles celles sur la portabilité, les DPO, les études d'impact, la transparence, le consentement, le profilage. La CNIL propose également un logiciel open source qui facilite la conduite et la formalisation d'analyses d'impact et est traduit dans de nombreuses langues.

La CNIL diffuse encore des « packs de conformité » qui établissent dans un secteur donné et dans un document non contraignant, les bonnes pratiques « informatique et libertés » ou « RGPD » de nature à garantir le respect des textes et parfois même à être « mieux disant ». Elaborés en étroite association avec les professionnels, ils sont plus opérationnels que les recommandations. L'objectif est que se développent des pratiques conformes au droit dur.

La CNIL se tourne vers les mécanismes de certification en recourant à des tiers certificateurs. La certification est un outil de coré-

21. Site de la CNIL.

22. Article 70-10 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés consolidée.

23. I. Falque Pierrotin, « Le droit souple vu de la CNIL : un droit relais nécessaire à la crédibilité de la régulation des données personnelles », *in Le Droit souple*, Conseil d'Etat, Etude annuelle 2013, p. 239-245.

gulation qui permet de promouvoir le modèle européen et la certification des DPO sera l'un des grands chantiers à venir.

Depuis l'adoption de la loi de mai 2018, la Cnil peut certifier des personnes, des produits, des systèmes ou des procédures. Elle peut également agréer des organismes certificateurs sur la base de l'accréditation qui leur a été délivrée par le Cofrac[24] ou décider conjointement avec lui de lui déléguer cet agrément.

Tout ceci permet aux entreprises de répondre aux réglementations sur la protection des données personnelles, facilite la conformité des acteurs aux exigences réglementaires et donne aux pouvoirs publics des outils de présomption de respect des exigences réglementaires.

La première étape pour se mettre en conformité est d'établir une cartographie des traitements existants (afin de voir quelles actions engager en premier) et de tenir un registre des traitements. Ce registre est obligatoire pour les entreprises ou organismes, à l'exception de ceux de moins de 250 salariés (sauf exceptions si le traitement comporte des risques et n'est pas occasionnel, ou s'il porte sur des données sensibles ou des données personnelles relatives à des condamnations et infractions).[25] Si le traitement présente un risque élevé pour les droits et libertés des personnes, le responsable de traitement doit effectuer une analyse d'impact préalable.

24. Comité français d'accréditation (« Cofrac »).

25. Article 30, RGPD.

B. Le DPO, *acteur de la conformité*

Héritier du Correspondant Informatique et Libertés, le délégué à la protection des données voit sa fonction et ses missions en grande part définies par le règlement. Les structures dans lesquelles un Correspondant Informatique et Libertés (CIL) est déjà en place pourront confier ces nouvelles missions au DPD, tandis que les autres devront soit former un collaborateur, soit en recruter un ou s'attacher les services d'un professionnel externe.

Le règlement rend obligatoire la présence d'un DPO (« Data Protection Officer », délégué à la protection des données ou DPD) dans les cas énumérés par l'article 37[26]. Le premier cas envisagé par l'article 37 est celui du traitement « effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ».[27] La tâche est immense et le Sénat s'en est inquiété, particulièrement pour les collectivités territoriales, encore fort peu préparées au moment de l'adoption de la loi française. Ce fut d'ailleurs l'un des points de résistance du Sénat lors des débats parlementaires. Ainsi, le Conseil constitutionnel a été saisi le 16 mai 2018 par le Sénat afin de répondre à ces inquiétudes. Cependant, le Conseil Constitutionnel a validé la quasi intégralité des dispositions de la loi, avec pour seule objection, la censure des mots « sous le contrôle de l'autorité publique » figurant à l'article 13 de la loi, afin de fixer le régime des traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes.

Pour les années à venir, la formation des DPO sera un enjeu crucial. Curieusement, le RGPD se contente de préciser que le DPO « est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 ».[28] Face à l'importance pratique du sujet, des *Guidelines* du G29 sur les DPO[29] ont très vite été adoptées (dès le 13 décembre

26. Article 37 (1) à (3), RGPD.
Désignation du délégué à la protection des données

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :
a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

2. Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

3. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille. Sur la notion d' « activités de base » *(core activities),* v. sur les *Guidelines* du G 29 sur les DPO, adoptées le 13 décembre 2016, 16/EN WP 243 (ci-après G 29 WP 243).

27. Le règlement ne définit pas les termes « autorité publique » ou « organisme public », qui sont donc définis par chaque Etat membre. Les *Guidelines* mettent en exergue le fait que ce sont alors toutes les activités, et non seulement celles « de base » qui sont visées. Elles recommandent aux entreprises privées qui exercent une mission de nature publique de désigner un DPO pour toutes les activités, y compris celles non liées à cette mission (G 29 WP 243, 2.1.1).

28. Article 37 (5), RGPD.

29. CNIL, *Lignes directrices concernant la protection des données.*

2016), puis révisées 4 mois plus tard (en avril 2017)[30]. Elles précisent que si le niveau d'expertise requis n'est pas strictement défini, « il doit être proportionné à la sensibilité, à la complexité et au volume des données traitées par un organisme ». Il est essentiel que le DPO (ou son équipe) soit associé le plus en amont possible aux questions relatives à la protection des données car l'article 38 (1), relatif à la « Fonction du délégué à la protection des données », lui donne compétence pour « toutes les questions relatives à la protection des données à caractère personnel »[31].

L'article 38 précise que le responsable du traitement et le sous-traitant fournissent au DPO « les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement ». Les lignes directrices distinguent selon que « l'organisme transfère systématiquement des données à caractère personnel hors de l'Union européenne ou, au contraire, que les transferts de ce type sont occasionnels ». Elles insistent sur le fait que le DPO doit non seulement posséder une solide expertise, mais qu'il doit aussi avoir certaines qualités personnelles, notamment « l'intégrité et le haut niveau de déontologie ». Elles mentionnent son « rôle clé dans la promotion d'une culture de la protection des données au sein de l'organisme » et précise qu'il « contribue à mettre en œuvre des éléments essentiels du RGPD, tels que les principes relatifs au traitement des données, les droits des personnes concernées, la protection des données dès la conception et la protection des données par défaut, le registre des activités de traitement, la sécurité du traitement ainsi que la notification et la communication des violations de données ».

L'indépendance du DPO est cruciale. Le considérant 97 indique que les DPO « qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance » et l'article 38 (3) du RGPD la consacre en ces termes : « Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant »[32].

Cette disposition soulève diverses questions, en particulier quant à la possibilité pour

30. CNIL, *Lignes directrices concernant les délégués à la protection des données (DPD)*
31. Article 38 (1), RGPD.
32. Article 38 (3), RGPD.

le DPO d'exprimer son désaccord et aux conséquences qui s'ensuivront[33].

De nombreuses autres questions se posent, dont celle de l'absence de conflits d'intérêts[34] pour le DPO dont le devoir de loyauté s'exerce tout à la fois envers son employeur et envers l'autorité de contrôle qui peut lui ordonner de lui notifier les failles de sécurité[35], ou encore celle de l'obligation de confidentialité : dans quelle mesure le DPO peut-il, et doit-il, dénoncer les violations dont il est témoin ?

Le DPO assume une mission stratégique au sein de l'entreprise. Il est acteur d'une approche par les risques et l'analyse des risques pour la protection des données est au cœur du métier du DPO[36]. Cela signifie que, conformément à la nouvelle logique mise en place par le règlement, il doit adopter une approche « sélective » et « pragmatique », il doit traiter prioritairement des questions qui présentent les risques les plus élevés en matière de protection des données[37]. Pour développer et piloter la stratégie de gouvernance de l'entreprise en matière de données, le DPO a besoin du soutien d'un réseau de personnes sensibilisées aux risques prêtes à l'aider au sein des directions, notamment juridique, informatique et des ressources humaines. C'est pour accompagner les DPO ou les prestataires de services amenés à exercer cette fonction si elle est externalisée en un nouveau métier, que l'université Paris II Panthéon-Assas a créé le diplôme « Data Protection Officer »[38].

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental protégé par la Charte des droits fondamentaux de l'Union européenne[39] et cela justifie en partie le champ d'application territorial très étendu du RGPD. En effet, le règlement s'applique même si le responsable du traitement ou le sous-traitant n'est pas établi sur le territoire de l'Union lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paie-

33. Pour plus de précisions, voir les *Guidelines* préc., par. 3.3 : « dans l'exercice de leurs missions au titre de l'article 39, les DPO ne doivent pas recevoir d'instructions sur la façon de traiter une affaire, par exemple, quel résultat devrait être obtenu, comment enquêter sur une plainte ou s'il y a lieu de consulter l'autorité de contrôle. En outre, ils ne peuvent être tenus d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données, par exemple, une interprétation particulière du droit. L'autonomie des DPD ne signifie cependant pas qu'ils disposent de pouvoirs de décision allant au-delà des missions leur incombant conformément à l'article 39 ». Le responsable du traitement ou le sous-traitant reste responsable du respect de la législation sur la protection des données et doit être en mesure de démontrer ce respect.

    3.4 : Si le responsable du traitement ou le sous-traitant prend des décisions qui sont incompatibles avec le RGPD et l'avis du DPO, ce dernier devrait avoir la possibilité d'indiquer clairement son avis divergent au niveau le plus élevé de la direction et aux décideurs. À cet égard, l'article 38, paragraphe 3, dispose que le DPO « fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du soustraitant ». Une telle reddition de compte directe garantit que l'encadrement supérieur (par ex., le conseil d'administration) a connaissance des avis et recommandations du DPO qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant. L'élaboration d'un rapport annuel sur les activités du DPO destiné au niveau le plus élevé de la direction constitue un autre exemple de reddition de compte directe. V. aussi le par. 3.4 sur les sanctions ou le licenciement du DPO.

34. Article 38 (6), RGPD, pour plus de précisions, v. *les Guidelines* préc., par. 3.5.

35. Article 58 (1), RGPD.

36. Article. 39 (2), RGPD.

37. Prec., par. 4.4.

38. Pour répondre aux besoins de formation des DPD, l'université Paris II Panthéon-Assas vient de créer un diplôme d'université dont l'objectif est de permettre aux professionnels d'assumer pleinement ces nouvelles fonctions.

39. Charte des Droits Fondamentaux de l'Union Européenne, Article 8 (1).

ment soit exigé ou non desdites personnes[40] ; ou suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union[41]. Ce critère nouveau du « ciblage » de la personne, par l'offre de biens ou de services ou par le suivi du comportement permet de viser les entreprises établies hors de l'Union européenne. En pratique, le RGPD s'applique chaque fois qu'un résident européen est visé par un traitement de données ainsi qu'aux données de non-résidents européens traitées dans le contexte des activités d'un établissement en Europe. Le transfert international des données est une question particulièrement sensible à laquelle la CJUE apporte sa contribution[42], comme elle le fait et le fera pour tous les aspects du règlement.

Le RGPD s'applique donc bien au-delà des frontières de l'Europe, ce qui signifie aussi que des sociétés établies à l'étranger peuvent avoir besoin, pour se mettre en conformité, de recourir aux services d'un DPO ou d'un prestataire externe (il est recommandé d'avoir un DPO ou prestataire établi en Europe). Pour tous, cela nécessite un investissement humain et financier important, parfois même une réorganisation interne au sein du groupe.

Malgré les deux années laissées, depuis l'adoption du règlement, pour se mettre en conformité, rares sont les acteurs privés ou publics qui sont parfaitement organisés. Il est vrai que le RGPD, avec ses 173 considérants et ses 99 articles – est un instrument exigeant, complexe et anxiogène (ne serait-ce que parce que les sanctions peuvent atteindre des sommes considérables). Les régulateurs ont donc cherché à rassurer les acteurs économiques et à leur faire part de leur volonté de les accompagner dans cette transformation. Malgré certaines différences d'approche, les Etats membres partagent les mêmes valeurs, fondées sur la protection des données et de la personne. Cela a un coût économique direct. Toutefois, l'asymétrie existante en matière de flux de données entre les États-Unis et l'Union européenne le justifie. Plus fondamentalement encore, l'actualité révèle, presque quotidiennement, le coût, non seulement économique, mais aussi culturel et politique, qu'il y aurait à s'aligner sur le moins offrant.

40. Article 3 (2) (*a*), RGPD.

41. Article 3 (2) (*b*), RGPD .

42. Communication intitulée « Echange et protection de données à caractère personnel à l'ère de la mondialisation » (du 10.1.2017, COM(2017) 7 final), dans laquelle la Commission européenne explique comment elle procède pour promouvoir ses valeurs en matière de protection des données et faciliter les flux de données.

ET MAINTENANT. À QUOI NOUS ATTENDRE ?

Bruno RASLE,
Délégué général de l'AFCDP,
Chef de projet Informatique et Libertés dans l'une des branches de la sécurité sociale, Co-auteur des livres : *Halte au Spam* (Eyrolles, 2003), *Correspondant Informatique et Libertés : bien plus qu'un métier* (AFCDP, 2015), *Droit à l'oubli* (Larcier, 2015) et *Protection des données personnelles - Se mettre en conformité pour le 25 mai 2018* (Éditions législatives, 2017),
-
Bruno Rasle forme les DPO depuis 2007 au sein d'un Mastère spécialisé et a créé un « Kit de survie Technique pour DPO, avocats et juristes ».

Projetons-nous un an « l'après 25 mai 2018 ». Le RGPD[43] est entré en application, le décret qui l'accompagne a été publié ainsi que le décret-cadre qui définit les cas d'usage du numéro d'inscription au répertoire des personnes physiques (plus connu sous le nom de « Numéro de sécurité sociale »), le G29[44] a publié ses dernières lignes directrices avant de renaître en tant que Comité européen à la protection des données, la CNIL a publié son « Guide du DPO », dévoilé ses deux listes relatives aux analyses d'impact (celle donnant les finalités pour lesquelles une AIPD, ou en anglais « PIA », est obligatoire et celle donnant les finalités pour lesquelles l'exercice est superflu), revu son Règlement intérieur et recyclé ses autorisations uniques et autres normes simplifiées en référentiels. La loi « Informatique et Libertés »[45], promulguée dans l'urgence dans sa troisième version, a été revue dans sa forme – grâce à l'ordonnance *ad hoc* – et constitue désormais un véritable « Code de la donnée personnelle », et plus de 80 000 responsables de traitement français ont désigné leur Délégué à la protection des données, interne ou externe.

Tout cela est facile à prévoir. L'exercice est plus périlleux concernant la publication du décret d'application censé apporter des précisions sur la façon dont les responsables de traitement doivent traduire de façon opérationnelle la possibilité d'organiser le sort des données personnelles après la mort[46]). Ce décret verra-t-il le jour ?

Verrons-nous également la publication d'actes délégués censés compléter le RGPD ? La Commission européenne peut en adopter, comme cela est prévu dans le RGPD[47], sur des sujets tels que les informations à présenter sous la forme d'icônes normalisées ainsi que les procédures régissant la fourniture de ces icônes et les critères et exigences applicables aux mécanismes de certification.

43. 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 (règlement général sur la protection des données).
44. Le G29 est un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales de chaque état membre de l'Union Européenne.
45. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
46. Actuel article 40-1 de la loi Informatique et Libertés, créé par la loi pour une République numérique.
47. Considérant 166 et Article 92, RGPD.

Justement, quel sera l'avenir des labels et des certifications ? Comme l'indique Claire Levallois-Barth[48], la surutilisation de labels (pratique très américaine) ne risque-t-elle pas parfois de déresponsabiliser les individus en les déchargeant de toute analyse critique ?

Comment va évoluer le *Privacy Shield* dans le contexte de la récente adoption du *Clarifying Lawful Overseas Use of Data Act*[49] ? Rappelons que cette loi fédérale des États-Unis permet aux forces de l'ordre (fédérales ou locales, y compris municipales) de contraindre les fournisseurs de services américains à dévoiler les données demandées stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers… y compris en Europe. Cette loi permet notamment aux USA d'obtenir les données personnelles d'un individu sans que celui-ci en soit informé, ni que son pays de résidence ne le soit, ni que le pays où sont stockées ces données ne le soit, ni que le responsable de traitement ne le soit…

Et que dire du projet de règlement relatif à la vie privée et aux communications électroniques (*ePrivacy*)[50], qui entre en phase de trilogue sous la pression d'un intense *lobbying* ? Peut-on l'espérer pour 2019 ?

Revenons au RGPD. Quel responsable de traitement français notifiera le premier une violation de données ? Qui inaugurera l'obligation de communiquer avec les personnes concernées quand la violation sera « susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique afin qu'elle puisse prendre les précautions qui s'imposent » ? Et, au contraire, qui prendra le risque de ne pas notifier à la CNIL ni d'informer les personnes, alors qu'il s'agit d'une obligation de résultat ?

En matière de contrôle, quelle va être la politique de la CNIL (dont on peut rappeler que le changement de Président approche) ? Va-t-elle se déplacer à chaque notification de violation ? Va-t-elle vouloir venir vérifier la réalité des mesures prises pour réduire les risques, telles qu'elles lui auront été présentées dans les analyses d'impact transmises au titre de l'article 36 du RGPD[51] ? Va-t-elle se focaliser dans un premier temps sur les finalités qui étaient jusqu'au 25 mai 2018 soumises à son approbation préalable ? Va-t-elle vouloir s'assurer de la conformité des procédures de recueil du consentement des mineurs ? Va-t-elle, comme certaines déclarations faites par ses agents lors de conférences le laissent penser, réaliser des contrôles « à 360° » – c'est-à-dire mener moins de missions de contrôles de durée courte au profit de missions de plusieurs jours à l'occasion desquels tous les traitements d'un organisme seront passés au scanner ?

Quand aurons-nous les premières sanctions au titre du RGPD ? La réponse à cette question est cruciale, car il est à craindre que certains responsables de traitement – se basant à tort sur l'historique des sanctions infligées jusqu'alors par la CNIL – soient tentés de ne retenir que le volet « auto-responsabilisation » du texte, en oubliant le volet « contrôle

48. Claire Levallois-Barth, *Signes de confiance – L'impact des labels sur la gestion des données personnelles*, (Chaire Valeurs et Politique des Informations Personnelles de Telecom ParisTech, janvier 2018).

49. *CLOUD Act :* Le *Clarifying Lawful Overseas Use of Data Act* (H.R. 4943) est une loi fédérale des États-Unis de 2018 sur la surveillance des données personnelles, notamment dans le Cloud. Elle modifie principalement le Stored Communications Act (en) (SCA) de 1986 en permettant aux forces de l'ordre (fédérales ou locales, y compris municipales 1) de contraindre les fournisseurs de services américains, par mandat ou assignation, à fournir les données demandées stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers. Critiquée par certaines associations de défense de la vie privée, cette loi permet notamment aux forces de l'ordre américaines d'obtenir les données personnelles d'un individu sans que celui-ci en soit informé, ni que son pays de résidence ne le soit, ni que le pays où sont stockées ces données ne le soit (Wikipédia).

50. Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement vie privée et communications électroniques).

51. Article 36 (1) et (3), RGPD.

a posteriori ». Cette période sera donc délicate pour les Délégués à la protection des données désignés par ces responsables, qui devront veiller à documenter soigneusement leurs analyses et recommandations.

Les DPO devraient rappeler à leur entourage que, par un simple effet de « moyenne », le niveau des sanctions pécuniaires ne peut que mécaniquement augmenter en France, une même non-conformité devant être sanctionnée de façon équivalente en Europe. Plusieurs autorités de contrôle (comme celles de l'Espagne, de l'Italie et de Grande-Bretagne – dans l'attente du Brexit) ayant opté pour la politique du bâton plutôt que de la carotte, il serait sage de surveiller et d'analyser toutes les décisions prises au niveau européen… et plus seulement celles de la CNIL. Notre organisme présente-t-il la même non-conformité pour laquelle une entreprise polonaise, portugaise ou néerlandaise vient d'écoper d'une pénalité financière importante ?

Restons quelques instants encore sur ce volet répressif. Il est à parier que les premières sanctions impliquant un sous-traitant (et de la sous-traitance en cascade) vont être analysées en détail. Sur quelles têtes tombera la foudre ? La nouvelle responsabilité des sous-traitants créée par le RGPD permet désormais aux autorités de contrôle de « ventiler » leur sanction entre le responsable de traitement et ses prestataires, selon l'acteur responsable de la non-conformité, ce qui n'était pas possible sous l'empire de la loi Informatique et Libertés jusqu'au 24 mai 2018. On peut élargir la question aux premiers litiges qui ne manqueront pas de survenir entre coresponsables de traitement (au sens de l'article 26 du RGPD) qui n'auraient pas suffisamment défini leurs obligations respectives et se renverraient la balle suite à une sanction.

Il est également difficile d'estimer l'impact des actions de groupes en matière de données personnelles – surtout si celles-ci peuvent déboucher sur l'indemnisation des victimes. Une telle disposition pourrait impacter les autorités publiques, elles qui sont à l'abri des sanctions pécuniaires de la CNIL. Ainsi, après le 25 mai 2018, pourrions-nous voir des assujettis à l'impôt sur le revenu se regrouper pour ester contre la Dgfip quand elle impose une vidéo postée sur Youtube sur la page destinée à saisir ses revenus[52], vidéo accompagnée par une collecte de données personnelles et un flux transfrontière, sans aucune information ni moyen de s'y opposer ? On peut aussi s'étonner de voir des grandes administrations intégrer sans réflexion aucune le reCaptcha de Google dans leur site web… Ayons une pensée pour leur DPO, fraîchement désignés, qui ont devant eux un véritable travail de Sisyphe.

Et *quid* de la réalité de la grande nouveauté introduite par le RGPD, l'extraterritorialité ? Les acteurs américains et chinois – pour n'évoquer que ceux-là – se plieront-ils de bonne grâce à une sanction de plusieurs milliards d'euros que pourraient leur infliger les autorités de contrôle européennes ? Et surtout, ces sanctions seront-elles suffisantes ? Il est intéressant de noter que, dans le cas de Facebook, la sanction maximale prévue correspondrait à environ deux milliards de dollars, à comparer avec un bénéfice de seize milliards dégagé en 2017. On observera avec attention ce que va décider la Federal Trade Commission[53] dans l'affaire Cambridge Analytica[54], Facebook ayant été placé sous surveillance en 2011 par le gendarme du commerce pour vingt ans : le géant américain pourrait écoper d'une amende allant jusqu'à un milliard de dollars si la FTC concluait que l'entreprise n'a pas respecté ses promesses.

52. NetxInpact.fr, *Vidéo YouTube obligatoire : la DGFiP fait machine arrière*.

53. La Federal Trade Commission (FTC) (Commission fédérale du commerce) est une agence indépendante du gouvernement des États-Unis, créée en 1914 par le Federal Trade Commission Act (en). Elle agi en tant qu'autorité de contrôle de la protection des données non-officielle.

54. Site de la CNIL, *Affaire Cambridge Analytica / Facebook*.

Allons-nous observer une forte croissance – voire une explosion – du nombre de demandes d'exercice des droits de la part des personnes concernées ? Au-delà des chiffres hautement fantaisistes qui circulent actuellement, les CIL observent déjà depuis quelques mois une augmentation des demandes de droit d'accès, de rectification, de correction, de suppression, voire de verrouillage (préfigurateur du droit de limitation, créé par l'article 18 du RGPD). Sachant que le traitement d'une simple demande de droit d'accès nécessite *a minima* quatre jours/homme pour être traitée au sein d'une entreprise de taille moyenne, quelle charge cela va-t-il représenter pour les organismes sollicités ?

Quels « paris » pouvons-nous faire concernant plus particulièrement les Délégués à la protection des données ? Du fait de la pénurie de professionnels formés et répondant aux exigences, il est à craindre quelques « erreurs de casting », des responsables de traitement se rendant compte *a posteriori* de l'inadéquation du savoir, du savoir-faire et du savoir-être de la personne qu'ils ont désignée auprès de la CNIL. Des CIL « pionniers » - qui avaient pourtant créé le poste *ex nihilo* et n'ont jamais démérité - ont été écartés par des personnes alléchées par certaines caractéristiques de la fonction de DPD. Mais ces dernières sont-elles assez « équipées » pour tenir le job ? Du fait des risques encourus (qui peuvent aller jusqu'à 4 % du chiffre d'affaires mondial[55]), ce ne sont pas deux ou trois jours de formation ou un rapide QCM associé à une certification qui font un expert[56].

En symétrie, il ne serait pas surprenant que des DPO cherchent à changer d'employeurs si ceux-ci n'ont pas bien saisi le concept « d'indépendance » dont bénéficie le Délégué à la protection des données… ou si leurs conseils restent trop souvent lettre morte. Ajoutons à cela l'effet « allons-voir-ailleurs-si-l'herbe-est-plus-verte », et l'on peut prévoir, au moins durant les deux premières années après lentrée en application du RGPD, un fort taux de rotation chez les DPO français. Sans compter l'appel de pays voisins, qui offrent un niveau de salaire bien supérieur.

Mais surtout, la question qui doit venir à l'esprit porte sur l'adéquation du RGPD avec l'air du temps. La directive 95/46/CE[57] a tenu vingt-trois ans. Combien de temps tiendra le nouveau règlement ? Ne prenons qu'un seul exemple : le texte est-il (déjà) adapté aux traitements mettant en œuvre la *blockchain* ? La CNIL, indique qu'elle souhaite proposer des « solutions et lignes directrices concrètes et lisibles » pour les acteurs qui souhaiteraient utiliser cette technologie[58]. Nous sommes impatients d'en prendre connaissance.

Qui ose encore prétendre que le chemin sera couvert de pétales de roses une fois passé le 25 mai 2018 ?

55. Article 83 (5), RGPD.
56. L'AFCDP publie sur son site la liste des formations longues préparant au métier de DPO
57. 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.
58. Communiqué de presse de la CNIL accompagnant son dernier rapport annuel.

LES MESURES APPROPRIÉES ET ANALYSES DE RISQUES DANS LE RGPD

Winston MAXWELL,
-
Diane OUANDJI,

Le règlement général sur la protection des données à caractère personnel (RGPD)[59] impose aux responsables du traitement l'obligation de mettre en œuvre des « mesures techniques et organisationnelles appropriées ». Les « mesures appropriées » nécessitent une analyse du contexte du traitement et des risques y associés. Une mesure qui est appropriée dans un contexte ne le sera pas dans un autre. Le caractère approprié des mesures dépendra également des coûts engendrés par les mesures. Le présent article examine le concept de « mesures appropriées » dans le RGPD (I), avant d'examiner l'articulation entre les « mesures appropriées » et les analyses de risques (II). Enfin, l'article propose une approche économique pour déterminer si une mesure est « appropriée » (III).

I. LE RESPONSABLE DU TRAITEMENT DOIT APPLIQUER DES MESURES APPROPRIÉES EN FONCTION DU RISQUE

A. Les « mesures appropriées » à travers les dispositions du RGPD

En application de l'article 24 du RGPD, le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour « s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. » Des mesures tiennent compte « de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques[60] ».

L'article 25 du RGPD, dédié à la protection des données dès la conception, prévoit que « le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, qui sont desti-

59. Règlement (UE) 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, et abrogeant la directive 95/46/CE.

60. Article 24(1), RGPD.

nées à mettre en œuvre les principes relatifs à la protection des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ».

L'article 32 du RGPD, dédié à la sécurité du traitement, exige la mise en œuvre de mesures techniques et organisationnelles appropriées pour « garantir un niveau de sécurité adapté au risque ».

L'article 35 du RGPD impose l'élaboration d'une analyse d'impact en cas de traitement « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ». L'analyse d'impact de l'article 35 doit examiner les risques au regard des finalités du traitement, la nécessité et la proportionnalité du traitement par rapport à ces finalités, et les « mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées ».

Pour résumer, les mesures appropriées sont : I) des mesures « appropriées et effectives »… qui « devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques »[61] ; II) des mesures pour « s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement », et qui tiennent compte « de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques »[62] ; III) des mesures « destinées à mettre en œuvre les principes relatifs à la protection des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée »[63] ; IV) des mesures destinées à « garantir un niveau de sécurité adapté au risque » … « compte tenu 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 ainsi que des risques »[64] ; V) des mesures « pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées »[65].

Les finalités, le contexte et le risque sont les principaux paramètres pour juger si une mesure est « appropriée » ou non.

FIGURE 1 : ELÉMENTS À PRENDRE EN CONSIDÉRATION DANS L'ÉLABORATION DE MESURES APPROPRIÉES

61. Considérant 74, RGPD.
62. Article 24, RGPD.
63. Article 25, RGPD.
64. Article 32, RGPD.
65. Article 35, RGPD.

B. Appréciation des risques pour les droits et libertés

Pour définir les mesures appropriées, les articles 24 et 32 indiquent que le responsable du traitement doit tenir compte « de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ». Ces articles évoquent les risques « pour les droits et libertés des personnes physiques », et non seulement pour la protection des données à caractère personnel. Comme l'explique le groupe de travail de l'Article 29 (G29), « la référence au droits et libertés des personnes concernées concernent principalement les droits à la protection des données à caractère personnel, mais pourrait également impliquer d'autres droits fondamentaux tels que la liberté d'expression, la liberté de pensée, la liberté de mouvement, la prohibition de discrimination, le droit à la liberté, la liberté de conscience et de religion ».[66]

L'article 32 du RGPD indique que le responsable du traitement doit tenir compte de « l'état des connaissances et des coûts de mise en œuvre » alors que l'article 24 du RGPD ne fait aucune référence aux coûts des mesures et l'état des connaissances. Cette différence peut s'expliquer par le fait que les mesures de sécurité visées par l'article 32 ne seront jamais efficaces à 100 %, le risque zéro n'existant pas en matière de cyber sécurité. Ainsi, le coût des mesures et l'état des connaissances seront des facteurs à prendre en considération. En revanche, une mesure destinée à garantir à la personne concernée le respect d'un de ses droits au titre du RGPD sera en principe jugé sans prendre en considération l'état des connaissances et les coûts de mise en œuvre.

Selon le considérant 76 du RGPD, l'évaluation du risque doit être effectuée de manière objective. L'auteur de l'évaluation du risque doit donc évaluer les risques non seulement du point de vue de l'entreprise, mais du point de vue des personnes concernées.

C. Les risques à prendre en considération.

Les types de risques à prendre en considération sont énumérés au considérant 75 du RGPD. Cette liste est longue, soulignant la nature hétérogène des risques liés à la protection des données à caractère personnel. Le considérant 75 mentionne les risques suivants :

« les dommages physiques, matériels ou un préjudice moral, en particulier :

• lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important ;

• lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel ;

• lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'ap-

66. Groupe Article 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 October 2017, WP 248 rev.01, p. 6.

partenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes ;

• lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels ;

• lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants ; ou

• lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées. »[67]

Cette énumération ne vise que les risques liés à la protection des données à caractère personnel, alors que l'analyse des risques doit tenir compte de « tous les droits et libertés des personnes physiques », et notamment l'impact sur la liberté d'expression. L'énumération du considérant 75 démontre que le préjudice peut être financier – les conséquences d'un vol d'identité par exemple – ou bien moral – les risques liés aux données sensibles par exemple. Le simple fait de ne pas être en mesure d'exercer le contrôle de ses données constitue également un préjudice dont le risque devra être évalué.

Le considérant 76 du RGPD explique qu'il « convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé. »

L'analyse d'impact visée par les considérants 75 et 76 s'applique à chaque traitement. Elle est destinée à aider le responsable du traitement à définir les mesures appropriées compte tenu du contexte et des risques[68].

II. LES ANALYSES D'IMPACT AU SEIN DU RGPD

A. Analyse d'impact et la protection des données dès la conception

Le paragraphe 1 de l'article 25 du RGPD consacré à la protection des données dès la conception et par défaut fait clairement référence à une analyse d'impact.

Le règlement dit, concernant le privacy by design, que « le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées,[...] qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, [...] de façon effective et à assortir le traitement des

67. Considérant 75, RGPD.
68. Considérant 74, RGPD.

garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée »[69]. Le meilleur moyen d'identifier ces mesures techniques et organisationnelles est encore de réaliser une analyse d'impact.

L'analyse d'impact peut aider au respect des exigences liées au *privacy by design* en identifiant les risques pour les personnes concernées ainsi que les mesures à mettre en œuvre pour réduire ces risques à un niveau acceptable pour l'individu. Les bonnes pratiques en matière d'évaluation des risques et des contre-mesures à mettre en œuvre pour traiter ces risques veulent que le risque résiduel (risque après application de la contre-mesure) soit évalué ; les mesures ne seront retenues que si le risque résiduel est d'un niveau (suffisamment) inférieur au risque initial. La prise en compte du coût de mise en œuvre et l'état des connaissances est indispensable pour évaluer l'efficacité de la contre-mesure, ce qui correspond aux attentes en matière de *privacy by design.*

La notion d'état de l'art a tout son sens car le contexte évolue, ainsi que les technologies et les menaces. De ce fait, l'analyse d'impact doit être régulièrement revue tout au long de la vie du traitement, pour prendre en compte ces évolutions.

Cette analyse n'est pas différente des analyses conduites par la plupart des entreprises lors du lancement d'un nouveau produit sur le marché. La méthodologie de la Commission Européenne en matière d'analyse des risques pour les produits semble adaptée. Cette méthodologie prévoit notamment que : « Les fabricants devraient effectuer une analyse de risques exhaustive dans le cadre de sa procédure d'évaluation de la conformité des produits avant leur mise sur le marché (ou dans certains cas particuliers lorsque le produit est déjà dans la chaîne d'approvisionnement). L'évaluation des risques effectuée par le fabricant doit prendre en considération tous les risques pertinents liés au produit, et sera la base à partir de laquelle le risque sera réduit à un niveau acceptable lorsque le produit est conçu ou fabriqué. »[70]

Lorsqu'une entreprise dispose déjà d'un processus d'analyse de risques dans le cadre de la mise sur le marché de produits, cette méthodologie pourrait utilement être réutilisée pour l'analyse de risques visée par les considérants 75 et 76, et de l'article 25 du RGPD. La méthodologie est similaire.

B. Analyse d'impact pour « risque élevé »

Quand réaliser une analyse d'impact détaillée ?

L'article 35 du RGPD exige une analyse d'impact pour tout traitement « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ». Le règlement ainsi que les lignes directrices du G29 ne donnent pas de liste exhaustive et définitive des cas où une analyse d'impact est obligatoire. L'article 35 du règlement cite en particulier les cas suivants : « a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement

69. Article 25 (1), RGPD

70. EU general risk assessment methodology (Action 5 of Multi-Annual Action Plan for the surveillance of products in the EU (COM(2013)76), 2015-IMP-MSG-15, 16 October 2015, p. 4. https ://ec.europa.eu/docsroom/documents/17107/attachments/1/translations/en/renditions/native

automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ; b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou c) la surveillance systématique à grande échelle d'une zone accessible au public. »[71]

Le considérant 91 du règlement précise que « le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. Dans de tels cas, une analyse d'impact relative à la protection des données ne devrait pas être obligatoire ».[72]

L'avis du G29[73] cite également le cas de traitement de données qui ont été combinées ou corrélées, ou des traitements qui font appel à des technologies, organisations ou usages nouveaux ou innovants. Les traitements utilisant le *Big data* ou la *Blockchain* pourraient donc être concernés. Les traitements qui par nature ne permettent pas aux personnes concernées d'exercer leurs droits ou qui sont nécessaires pour l'utilisation d'un service ou la signature d'un contrat sont également concernés. L'exemple des banques qui contrôlent/vérifient les informations des clients pour décider d'accorder ou non un prêt est cité dans les lignes directrices. Ce cas particulier pourrait également s'appliquer aux traitements RH car le salarié ou le candidat au recrutement est très rarement libre de refuser les traitements qui sont réalisées sur ses données.

Cette liste est non exhaustive et n'inclut bien évidemment pas tous les cas. Le dilemme pour le responsable des traitements reste donc entier pour les autres cas. En effet, celui-ci est tenu de documenter les traitements et de prouver qu'il a mis en œuvre les mesures techniques et organisationnelles appropriées pour garantir le respect des droits et libertés des personnes. Comment faire cela si les risques n'ont pas été identifiés et évalués ?

La réalisation d'une pré-analyse d'impact (par opposition à l'analyse telle que demandée par l'article 35 du RGPD) s'avère nécessaire afin de démontrer le caractère adéquat des mesures.

Sans être aussi détaillée que l'analyse d'impact, cette pré-analyse doit permettre : I) d'identifier la nature, le périmètre, le contexte et les finalités du traitement, les données utilisées et supports utilisés ainsi que les personnes concernées ; II) de décrire le traitement et déterminer si un des cas pour lequel l'analyse d'impact « risque élevé » est applicable ; III) de prendre des mesures techniques et organisationnelles déjà prises en compte, y compris la conformité à des normes, standards, code de conduite ; IV) une évaluation des risques déjà identifiés compte-tenu du secteur d'activité de l'entreprise ou du contexte de réalisation du traitement. Ceci nécessite de disposer d'une base de risques (et de mesures) qui sera enrichie par les résultats des différentes pré-analyse.

Autant d'éléments qui au-delà de l'identification des traitements nécessitant une analyse d'impact, permettront d'enrichir le registre des traitements.

Point non négligeable, l'analyse d'impact doit être réalisée avant la mise en œuvre du

71. Article 35(3), RGPD.

72. Considérant 91, RGPD.

73. Groupe Article 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, 4 octobre 2017, WP 248 rev.01.

traitement, ceci bien entendu pour les nouveaux traitements. Mais l'état de l'art étant en perpétuelle évolution, cette analyse d'impact doit être régulièrement mise à jour au cours de la vie du traitement. Il ne s'agit donc pas de réaliser une analyse « one shot » avant la mise en œuvre du traitement, mais de la faire vivre tout au long de la durée du traitement.

C. Avis du délégué à la protection des données personnelles

L'article 35 paragraphe 2 du règlement précise que « Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné ».

Ainsi, l'analyse d'impact est réalisée par le responsable du traitement, mais celui-ci doit demander l'avis du délégué à la protection des données s'il existe. Ceci fait partie des critères d'acceptabilité d'une analyse d'impact décrit dans les lignes directrices du G29 relatives aux analyses d'impacts.

Doit-on tenir compte de cet avis ? Ni le règlement, ni les lignes directrices du G29 ne précisent explicitement s'il est obligatoire ou non de tenir compte de l'avis du délégué à la protection des données personnelles, dans quel cas cet avis peut être écarté et si des justifications sont nécessaires. Mais en consultant les différents outils d'analyse d'impact ou d'aide à la conformité mis à disposition par différentes autorités de contrôle, il est clair que le responsable de traitement doit prendre en compte cet avis et donc justifier les cas où cet avis serait écarté[74].

Ceci est en accord avec la logique de responsabilisation, documentation et preuve qui sous-tend le RGPD.

74. Voir l'outil d'aide à la conformité du CNPD : https ://cst.cnpd.lu/portal/

D. Comment réaliser une analyse d'impact ?

Les lignes directrices du G29[75] donnent une liste de critères permettant de savoir si une méthode d'analyse d'impacts est conforme aux exigences du règlement et cite des modèles existants par pays ou secteur d'activités. La norme ISO 29134[76] décrit également une méthode d'analyse d'impact sur la vie privée.

Il existe déjà de nombreuses méthodes d'analyses d'impact, que l'entreprise devra adapter à son contexte. Toutes ces méthodes, en cohérence avec le règlement et les lignes directrices du G29, conduiront à une cartographie des risques, selon leur probabilité et leur niveau de gravité :

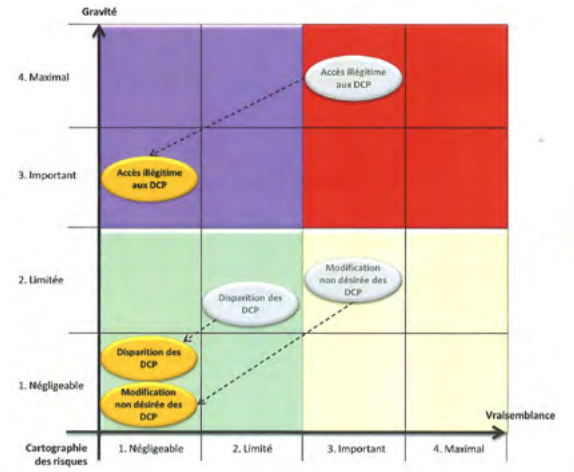


FIGURE 2 : CARTOGRAPHIE DES RISQUES[77]

Ces cartographies permettent d'identifier des risques manifestement intolérables (dans le quadrant en haut à droite), et de montrer l'évolution des risques en fonction des mesures mises en œuvre par le responsable du traitement. Grâce aux mesures, un risque situé dans le quadrant en haut à droite peut évoluer vers la gauche et vers le bas.

En revanche, une cartographie des risques ne permettra pas de déterminer s'il est possible d'accepter ou non un risque résiduel se trouvant dans un quadrant non rouge du tableau. Cette question dépend de la notion de « risque acceptable ».

75. Groupe Article 29, *WP 248,* 4 octobre 2017.
76. ISO/IEC 29134 :2017. *Information technology – Security techniques – Guidelines for privacy impact assessment*, juin 2017.
77. Source : CNIL, *PIA-2, L'Outillage : Modèles et bases de connaissances de l'étude d'impact sur la vie privée*, 2015.

E. Analyse d'impact, incidents de sécurité et violation de données

Les mesures sélectionnées devant être appropriées et à l'état de l'art, l'analyse d'impact devra être régulièrement mise à jour, notamment pour tenir compte de l'évolution de cet état de l'art.

En particulier, il conviendra de se poser la question de la nécessité de mettre à jour cette analyse d'impact à l'issue d'un incident de sécurité et/ou d'une violation de données. En effet, un incident de sécurité peut révéler une faille du système utilise pour traiter les données. Même si cet incident n'a pas conduit à une violation de données, il est impératif de se poser la question de l'exhaustivité des menaces et vulnérabilités identifiées lors de l'analyse d'impact, ainsi que de la pertinence des mesures sélectionnées.

Pour illustrer ce propos, prenons un exemple : vous utilisez un logiciel disponible en ligne pour réaliser des traitements de données personnelles. En faisant préalablement une analyse d'impact, vous avez décidé, entre autres mesures, que les mots de passe devraient avoir une complexité spécifique, que l'utilisateur devrait saisir son login/mot de passe à chaque connexion et que les données stockées dans l'applications devaient être chiffrées. Vous avez mené une campagne de sensibilisation pour éviter que les collaborateurs n'écrivent ces mots de passe sur des post-it et cette campagne a été efficace. Suite à une attaque informatique, le poste d'un collaborateur est infecté par un virus. Vous avez réussi à circonscrire l'attaque mais en investiguant, vous vous apercevez que cette attaque a été rendue possible parce que cet utilisateur se sert d'un navigateur qui n'est pas à jour. Vous vous apercevez également que cet utilisateur enregistre ces mots de passe dans le gestionnaire de mot de passe[78] disponible par défaut sur son poste. Il le fait pour tous ses mots de passe. En poussant l'investigation, vous constatez que c'est une pratique courante dans votre entreprise. Les collaborateurs s'échangent cette astuce et la transmette aux nouveaux embauchés.

Bien qu'il n'y ait pas eu de violation de données à caractère personnel, vous savez que ce gestionnaire de mot de passe présente une vulnérabilité qui permet à n'importe quel site web de voler les mots de passe enregistrés par ce gestionnaire[79].

Votre analyse d'impact doit donc être mise à jour pour prendre en compte cette vulnérabilité, ce scénario d'attaque (un utilisateur se connecte à un site web malveillant qui vole ces identifiants de connexion stockées dans le gestionnaire de mot de passe et peut ainsi se connecter à votre application) et identifier les mesures appropriées à mettre en œuvre.

78. Pour plus d'explication sur les gestionnaires de mots de passe, voir https ://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe.

79. Pour un exemple d'actualité, voir : https ://bugs.chromium.org/p/project-zero/issues/detail?id=1481&desc=3.

III. DES « MESURES APPROPRIÉES » SOUS L'ANGLE ÉCONOMIQUE

A. Une analyse d'impact aide à trouver le niveau de « mesures appropriées »

Les analyses d'impact aident à réduire le risque à un niveau suffisamment bas pour être acceptable. Dans son avis sur les analyses d'impact, le G29 précise seulement que les mesures doivent permettre de réduire le risque à un niveau acceptable, sans préciser ce qu'est un niveau acceptable[80]. La protection dépend du contexte. Une « mesure appropriée » ne correspond pas forcément à un niveau de protection de 100 %.

En droit, les termes « mesures appropriées » renvoient au concept de la personne raisonnable, concept qui remplace celui de « bon père de famille ». Ce sont des concepts malléables, qui permettent d'imposer à des personnes physiques et morales des niveaux de responsabilité différents en fonction des circonstances, et notamment du niveau de dangerosité de leur activité et les attentes légitimes des victimes. Le gestionnaire d'un central nucléaire aura des obligations de sécurité plus élevées que l'exploitant d'un vignoble compte tenu de la dangerosité de son activité. De même, un médecin aura des obligations plus élevées en matière de soins qu'un simple passant en raison de la formation et expertise du médecin. Le RGPD essaie de répliquer ce modèle souple : Plus une opération de traitement est risquée, plus le niveau de mesures appropriées sera élevé. D'où l'exigence au titre de l'article 35 d'effectuer une analyse d'impact pour les traitements présentant un « risque élevé ».

Souvent, les risques d'une activité ne peuvent être réduits à zéro. Pour éliminer les risques entièrement, il faudrait soit interdire l'activité, soit mettre en place des mesures de sécurité tellement couteuses que l'activité ne serait plus viable économiquement. Dans ce contexte, le niveau de mesures appropriées et adaptées aux risques pose question.

L'automobile est un bon exemple. Pour réduire à néant le niveau de risque, il faudrait soit interdire l'utilisation de la voiture, soit imposer des mesures de sécurité qui augmenteraient le poids et le coût de chaque véhicule, ce qui rendrait la voiture moins accessible aux individus. Au lieu d'interdire la voiture, ou d'imposer des obligations de sécurité qui rendraient la voiture inaccessible à la majorité de la population, nous acceptons des mesures moins drastiques. Ces mesures sont considérées comme appropriées dans le contexte de l'automobile, même si les risques de sécurité restent élevés.

En termes économiques, le niveau approprié des mesures de protection correspond au point où le coût marginal d'une unité supplémentaire de mesures de protection est égal au bénéfice marginal résultant de cette mesure[81]. Au-delà de ce point, les mesures de sécurité supplémentaires coûtent plus chères pour la société que le bénéfice qui en découle. Elles vont réduire le bien-être social dans son ensemble, au lieu de l'augmenter. Le niveau optimal théorique se situe au point où la somme de tous les coûts liés aux risques et de tous les coûts liés aux mesures de prévention sont minimisés. Le bien-être social trouve son niveau maximum à ce point, car l'ensemble des coûts est minimisé.

80. *WP 248*, p. 18.

81. Cette règle découle d'une décision de justice américaine rendu par le magistrat Learned Hand en 1947. Depuis, cette règle s'appelle la « Règle Hand ». Elle est utilisée pour définir un comportement fautif.

Les coûts liés aux mesures de prévention incluent non seulement les coûts techniques des mesures, mais les coûts pour la société d'une utilité réduite découlant des mesures de protection. Par exemple, une voiture serait plus sûre si sa vitesse était limitée à 30km/heure, mais cela conduirait à une réduction de l'utilité de la voiture pour la société, ce qui créerait un coût social à prendre en considération. Il en est de même pour une mesure d'anonymisation totale des données de santé, si cette mesure réduisait l'utilité d'une recherche médicale. Cette réduction d'utilité créerait un coût social à inclure dans le bilan.

Une mesure de protection peut également générer des coûts indirects. Par exemple, un système pour renforcer la collecte du consentement de l'individu peut créer un risque de sécurité dans une voiture connectée. Il en est de même pour une mesure de protection des données à caractère personnel qui créerait un impact négatif pour la liberté d'expression. Ces coûts indirects devraient être pris en considération dans le bilan coûts/avantages.

Sur le plan économique, le niveau optimal des mesures de prévention se situe au point C* dans la figure suivante :

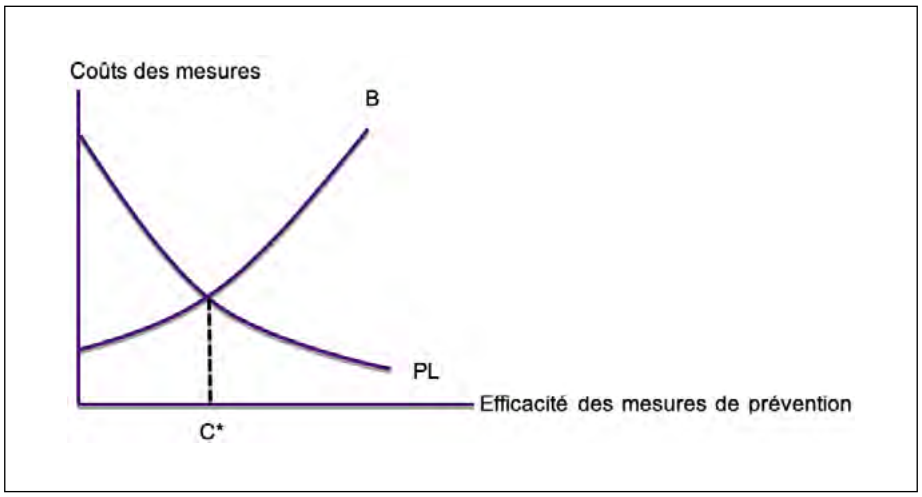


FIGURE 3 : ILLUSTRATION DE LA RÈGLE HAND[82]

Dans ce diagramme, la courbe PL représente les coûts liés au risque du préjudice, P étant la probabilité de l'occurrence du préjudice, et L étant le niveau de préjudice qui résulterait si le risque se réalisait. Par exemple, si le coût social (L) lié à la perte d'un million de numéros de cartes crédit est égal à 100 millions d'euros (soit 100 euros par carte), et la probabilité de cette perte (P) est de 0,1 % (une chance sur mille), le produit « PL » est égal à 100 000 euros. Cette courbe PL décroit lorsque l'on ajoute des mesures de sécurité, mais il n'atteint pas zéro. La courbe s'aplatit, ce qui signifie qu'au-delà d'un certain seuil, chaque mesure de sécurité supplémentaire contribue faiblement à la diminution du risque.

La courbe B représente les coûts liés aux mesures de prévention. Généralement, les premières mesures de prévention, peu onéreuses et très efficaces, ont un impact important sur le

82. Richard Posner, *Economic Analysis of Law*, Aspen Casebook Series, 8th Edition, 2011.

risque (diminution de la courbe PL). Mais au-delà d'un certain seuil, les mesures de prévention deviennent très chères pour un impact plus faible sur le risque. Par exemple, une mesure de prévention qui réduit la probabilité « P » de 100 % à 0,5 % pourrait coûter le même montant qu'une mesure supplémentaire qui réduirait la probabilité « P » de 0,5 % à 0,1 %, ou de 0,1 % à 0,08 %. Chaque incrément de protection devient plus cher lorsqu'on approche un niveau de risque zéro. La courbe B grimpe de manière exponentielle.

Une autre façon de présenter le niveau optimal de mesures de prévention est un graphique montrant le point où le bien-être social atteint son niveau maximum :

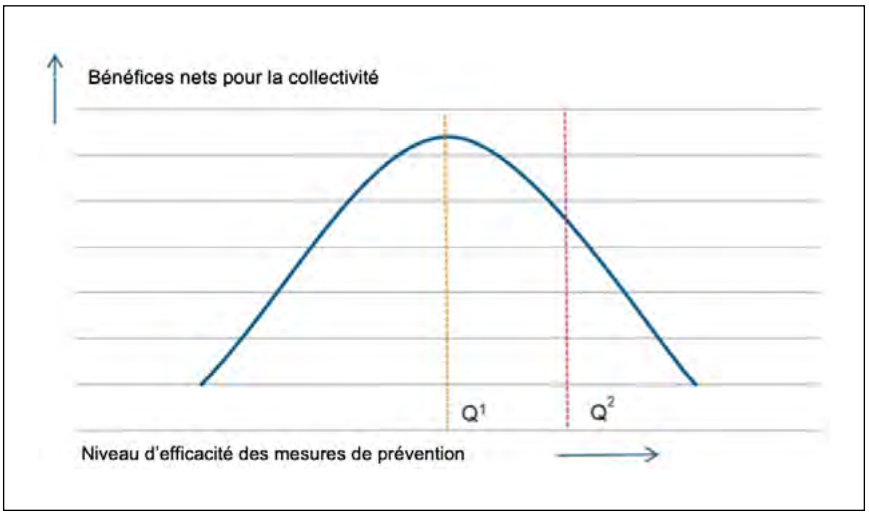


FIGURE 4 : MAXIMISATION DU BIEN-ÊTRE SOCIAL SELON LE NIVEAU D'EFFICACITÉ DES MESURES DE PRÉVENTION[83]

Même si la mesure de prévention Q^2 fournit un niveau de protection supérieur à la mesure Q^1, le niveau optimal se trouve au point Q^1, car le bien-être social trouve son maximum à ce point.

B. Les bénéfices du traitement pour la société doivent être pris en considération

En termes économiques, le caractère approprié d'une mesure de protection dépendra en partie des bénéfices attendus du traitement, et de la réduction de ces bénéfices causés par la mesure de protection. Cette analyse « risques/bénéfices » n'est pas explicitement prévue par le RGPD, mais elle y figure de manière implicite, puisque le règlement se réfère au caractère « approprié » des mesures, compte tenu du contexte. Le caractère approprié s'apprécie au moins en partie par rapport à l'utilité sociale du traitement, et la diminution de cette utilité provoquée par les mesures de prévention.

La norme ISO en matière d'analyses d'impact de données à caractère personnel recon-

83. Winston Maxwell, *Smarter Internet Regulation Through Cost-Benefit Analysis*, Presses des Mines, 2017.

naît les relations entre l'utilité sociale du traitement et les mesures de prévention : « Il peut avoir des situations où les mesures de diminution des risques ont un impact sur les bénéfices que les parties prenantes peuvent réaliser du traitement des informations concernées. Dans ce cas, la personne rédigeant l'analyse d'impact devrait effectuer une analyse coûts/bénéfices pour déterminer si les risques pèsent plus lourds que les bénéfices ou vice versa. Dans le premier cas, l'entreprise devrait adopter les mesures de diminution des risques en cause. Dans le deuxième cas, l'entreprise devrait décider d'accepter les risques, dans les limites permises par la réglementation. »[84]

Un traitement générant un bénéfice important pour la collectivité pourrait justifier un niveau de risques plus élevé qu'un traitement contribuant faiblement au bien-être social. Une analyse d'impact devra donc évaluer les bénéfices du traitement pour l'ensemble des parties impactées : le responsable du traitement, les individus concernés, et la société dans son ensemble. Une analyse risques/bénéfices serait particulièrement utile dans le cadre de projets du type « Big data », où les contraintes liées à l'anonymisation de données peuvent réduire l'utilité des traitements.[85]

Conclusion

Le RGPD impose une responsabilisation des acteurs économiques. Dans la plupart des cas, ceux-ci devront définir eux-mêmes les « mesures appropriées » à mettre en œuvre pour assurer une conformité aux règles générales du règlement. De plus, le RGPD impose une obligation de « démontrer » sa conformité. Cette démonstration passera par la tenue d'un registre (article 30) et la conduite d'analyses d'impact pour des traitements présentant un risque élevé. Cette analyse d'impact permettra au responsable de traitement de justifier ses choix en matière de mesures appropriées, en mettant en évidence les facteurs que le responsable du traitement a mis en balance pour arriver à sa décision.

84. ISO 29134, p. 20.

85. Jules Polonetsky, Omer Tene and Joseph Jerome, *Benefit-Risk Analysis for Big Data Projects*, Future of Privacy Forum, september 2014.

METTRE EN PLACE DES RELATIONS ÉQUILIBRÉES ENTRE RESPONSABLES DE TRAITEMENT ET SOUS-TRAITANTS DANS LE CADRE DU RGPD

Anne BAUDEQUIN,
Avocat, Squire Patton Boggs
-
Rachel BOGE KNITTEL,
Juriste Conformité Données Personnelles, Imprimerie Nationale SA
-
Nathalie LANERET,
Group DPO, Capgemini, Enseignant DU DPO Panthéon Assas

Un des principaux objectifs du Règlement Européen sur la Protection des Données Personnelles[86] ou « RGPD », applicable depuis le 25 mai 2018 est d'assurer une protection accrue des droits des personnes dont les données personnelles sont traitées. A l'heure où la digitalisation croissante de toutes les activités et fonctions de l'entreprise engendre des traitements de données personnelles de plus en plus importants et sophistiqués par une chaîne croissante d'acteurs, le RGPD vient responsabiliser davantage à la fois les responsables de traitement[87] mais également leurs sous-traitants[88].

Cette démarche passe par l'instauration du principe d' « accountability » qui impose aux entreprises de démontrer leur conformité à la réglementation[89], une augmentation substantielle du montant des amendes administratives en cas de non-respect de la réglementation[90], l'introduction de la notion de « responsables conjoints de traitement » et encore le renforcement du formalisme contractuel en cas de recours à la sous-traitance[91]. Le RGPD impose également des obligations directes au sous-traitant et permet aux autorités compétentes de le sanctionner directement pour ses propres défaillances. Enfin, le RGPD instaure une responsabilité conjointe et solidaire des organisations ayant participé au traitement

86. 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 (règlement général sur la protection des données) – JOCE du 4 mai 2016 – L119/1.

87. L'article 4 (7) du RGDP définit le responsable du traitement comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

88. L'article 4 (8) du RGPD définit le sous-traitant comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

89. Articles 5 (2) et 24 (1), RGPD.

90. Article 83, RGPD.

91. Article 28, RGPD.

des données personnelles en permettant aux personnes ayant subi un dommage de demander réparation intégrale à l'une quelconque de celles-ci et ce afin de garantir à la personne une réparation effective[92].

Ces derniers points établissent un changement notable de paradigme par rapport à la réglementation applicable jusqu'à l'entrée en vigueur du RGPD[93] qui limitait les engagements du sous-traitant à des obligations contractuelles envers le responsable de traitement. Le RGDP permet donc de rééquilibrer les relations entre les acteurs de la « chaîne digitale logistique » qui doivent chacun assumer leurs obligations, sauf à devoir en répondre directement au régulateur et aux individus en cas de difficulté.

Si les règles du RGPD semblent claires à première vue[94], il n'en est pas toujours de même en ce qui concerne la mise en application concrète de celles-ci par les parties concernées qui peuvent bien souvent, dans le cadre d'un rapport de force, être tentées d'interpréter les règles en leur faveur afin d'échapper à leurs obligations ou aux nouvelles responsabilités. Ceci peut même aller parfois jusqu'à mépriser les grands principes et la philosophie du RGPD et aboutir alors à remettre en cause le nouvel équilibre mis en place.

L'objectif de cet article est de clarifier les rôles et responsabilités du responsable de traitement et du sous-traitant afin de promouvoir une approche équilibrée de leurs relations. Ainsi, les nouvelles obligations du sous-traitant doivent nécessairement s'inscrire dans le cadre de l'accountability qui interdit une prise en charge intégrale de celles de son client (I). La même logique doit prévaloir en termes de responsabilité afin d'éviter que le jeu de la négociation contractuelle n'aboutisse à faire porter l'intégralité du risque par le sous-traitant au mépris des règles du droit commun de la responsabilité civile (II).

I. LE NOUVEAU CADRE D'ACTION DU SOUS-TRAITANT

Les modalités de la sous-traitance étaient déjà encadrées par la loi de 1978[95]. Cependant, jusqu'alors, seul le responsable de traitement se voyait imposer des obligations légales (encadrer contractuellement la relation avec le sous-traitant, choisir un sous-traitant présentant des garanties suffisantes, garantir le respect des mesures de sécurité et de confidentialité). Le RGPD reconnait dorénavant le sous-traitant comme l'un des acteurs du traitement de données personnelles en lui imposant de nouvelles obligations (A), dont il répond devant le responsable de traitement (B).

92. Article 82, RGPD.

93. 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 – *JOCE n°L 281 du 23 novembre 1995 p.0031-0050.*

94. La CNIL a publié à ce titre un guide sur le sous-traitant afin d'assister ces derniers dans la compréhension de leurs nouvelles obligations. CNIL, Règlement Européen sur la protection des données personnelles - *Guide du Sous-traitant*, édition septembre 2017.
https ://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf.

95. Loi n°78/17 du 6 janvier 1978 modifiée, dite Loi Informatique et Libertés.

A. La responsabilisation de tous les acteurs du traitement

Afin de protéger les personnes concernées, le RGPD responsabilise l'ensemble des acteurs du traitement (1). A ce titre, tout comme le responsable de traitement, le sous-traitant est dorénavant tenu à certaines obligations (2).

1. Le principe d'*accountability*

Bien que la mise en œuvre du principe d'*accountability*[96] repose sur le responsable de traitement[97], le sous-traitant participe à la conformité et doit en justifier au responsable de traitement. Il devra mettre en œuvre tous les mécanismes et procédures internes permettant de démontrer le respect des règles relatives à la protection des données. En effet, le RGPD impose au responsable de traitement de ne faire appel qu'à des sous-traitants présentant des « garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées… »[98]. Cette obligation doit être calibrée en fonction du traitement, de sa nature, de son contexte et des risques, dont le degré de probabilité et de gravité varie[99].

Ainsi, le sous-traitant devra pouvoir justifier au responsable du traitement du respect des règles, telle que la mise en place d'une gouvernance, la déclinaison d'une documentation afférente (au travers de politiques, de chartes, de procédures), la sensibilisation de ses personnels, la mise en place de procédures de contrôle[100].

2. Des obligations en propre pour le sous-traitant

Le RGPD place le sous-traitant dans un rôle actif au service de la protection des données personnelles, au même titre que le responsable de traitement. Le sous-traitant se voit donc tenu au respect de nouvelles obligations en propre au titre desquelles il pourra voir sa responsabilité engagée.

Le RGPD étend au sous-traitant l'obligation de tenue d'un registre des activités de traitement en en précisant le contenu[101].

Le sous-traitant devra également vérifier s'il doit désigner un délégué à la protection des données, chargé de piloter la conformité au RGPD. En effet, les critères de

96. Au titre des articles 5 et 24 du RGPD, le responsable de traitement doit être en mesure de démontrer qu'il a mis en œuvre au sein de son organisation les principes relatifs au traitement des données à caractère personnel. En tenant compte du contexte et du risque, il doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de démontrer la conformité du traitement au RGPD.

97. Article 5 (2), RGPD

98. Article 28, RGPD : « … de manière à ce que le traitement réponde aux exigences du présent règlement européen et garantisse la protection des droits de la personne concernée ». A noter que cette obligation n'est pas vraiment une nouveauté puisque la Directive 95/46/CE imposait déjà au responsable de traitement de « … choisir un sous-traitant qui apporte les garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives au traitement à effectue ». Voir Directive 95/46/CE, article 17.

99. Article 24 (1), RGPD

100. Articles 40 à 43, RGPD

101. Le sous-traitant aura certainement deux registres à tenir : l'un pour les traitements dont il est responsable (au titre de la gestion de son personnel par exemple) et l'autre pour les traitements dont il est sous-traitant et qu'il opère pour le compte du responsable de traitement.

désignation posés par le RGPD s'appliquent, que l'organisme soit responsable du traitement ou sous-traitant[102].

Enfin, le sous-traitant non établi sur le territoire de l'Union européenne devra désigner un représentant au sein de l'Union européenne[103] s'il procède à un traitement de données relatives à des personnes se trouvant sur le territoire européen et si ces opérations de traitement sont liées à une offre de biens ou services, ou impliquent un suivi de comportement de ces personnes.

Ces obligations viennent s'ajouter aux obligations auxquelles le sous-traitant est soumis dans la mesure où il aurait lui-même à traiter des données à caractère personnel (données RH par exemple). Ainsi, il pourrait être amené à tenir un registre en sa qualité de sous-traitant en plus du registre en qualité de responsable du traitement.

B. Des obligations vis-à-vis du responsable de traitement

Le sous-traitant ne peut agir que sur instruction du responsable de traitement[104] et sous son autorité[105] et ne bénéficie donc d'aucune autonomie dans l'exercice de ses missions[106]. Ces obligations doivent être prévues par un contrat (1) qui devra préciser l'étendue de l'obligation de collaboration (2).

1. L'encadrement contractuel du champ d'intervention du sous-traitant

L'article 28.3 du RGPD liste des points à définir entre le responsable de traitement et le sous-traitant ainsi que les engagements du sous-traitant vis-à-vis du traitement et des données à caractère personnel auxquelles il a accès à l'occasion des opérations de traitement.

Ainsi, doivent notamment être décrits les missions précises du sous-traitant, l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, les obligations et droits du responsable de traitement[107]. En plus de ces éléments descriptifs – qui doivent permettre au sous-traitant de tenir son registre – les relations entre le sous-traitant et le responsable de traitement doivent être explicitées.

Le contrat doit exposer les obligations du sous-traitant vis-à-vis du responsable de traitement : le sous-traitant ne peut traiter les données que pour les seules finalités qui font l'objet de la sous-traitance et conformément aux instructions – documentées – du responsable de traitement.

La sous-traitance de second rang doit être impérativement autorisée (de façon spécifique ou générale) préalablement par écrit par le responsable de traitement[108]. Elle doit correspondre en tous points aux conditions de la

102. Article 37, RGPD
103. Article 27, RGPD
104. Article 28 (3) (a), RGPD
105. Article 29, RGPD
106. L'article 4.8° du RGPD rappelle cette hiérarchisation des rôles dans la définition même de la notion de sous-traitant : «la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement».
107. Article 28, RGPD
108. Article 28 (2), RGPD.

sous-traitance de premier rang. Le sous-traitant de premier rang reste pleinement responsable devant le responsable de traitement de l'exécution par le sous-traitant de second rang de ses obligations[109].

Le contrat doit mentionner les mesures de sécurité techniques et organisationnelles appropriées que les parties doivent mettre en œuvre pour garantir au traitement un niveau de sécurité adapté au risque[110]. Cette obligation incombant tant au responsable de traitement qu'au sous-traitant, le contrat devra clairement organiser les rôles et responsabilités de chacune des parties au regard des mesures à mettre en œuvre[111]. L'information devant être communiquée par le sous-traitant au responsable de données en cas notamment d'incident devra être précisée (nature, délais) sachant qu'en la matière les nouvelles obligations imposées au responsable de traitement sont lourdes.

Le sous-traitant pourra être requalifié en responsable de traitement s'il ne respecte pas les instructions du responsable de traitement telles que formulées dans le contrat. Cela confirme que les deux rôles sont distincts mais n'empêchent pas une collaboration entre les parties.

2. Les obligations de collaboration entre le sous-traitant et le responsable de traitement

En plus des nouvelles obligations spécifiques au sous-traitant, le RGPD impose une obligation d'assistance par le sous-traitant au responsable de traitement dans le respect de ses propres obligations. L'objectif affiché est de favoriser la coopération entre les acteurs du traitement au profit de la sécurité du traitement et de la garantie des droits des personnes concernées. Cette obligation d'assistance se décline dans toutes les dimensions du traitement :

Le sous-traitant aide le responsable de traitement dans la réalisation de l'analyse d'impact selon les modalités qui auront été définies au contrat[112]. Il informe le responsable de traitement si une instruction constitue une violation du RGPD[113]. Il apporte son conseil au responsable de traitement pour l'aider à garantir le respect de ses propres obligations prévues aux articles 32 à 36[114].

Les modalités de cette assistance devront être définies dans le contrat : réponse aux demandes du responsable de traitement ou véritable obligation de coopération ; conditions financières ; et délais.

Le RGPD ne se contente pas de mettre en place des nouvelles obligations pour le sous-traitant. Il instaure également un régime de responsabilité du sous-traitant au titre des obligations qui lui incombent, dans le cadre du droit commun de la responsabilité.

109. Article 28 (4), RGPD.

110. Article 32 (1), RGPD.

111. Le contrat prévoit également le sort des données à l'issue de la prestation relative au traitement : soit une destruction de toutes les données à caractère personnel, soit un renvoi des données à caractère personnel au responsable de traitement ou au sous-traitant désigné par lui. Voir RGPD, Article 28.3 g).

112. Article 28 (3) (f), RGPD et voir le guide du sous-traitant de la CNIL les lignes directrices du G29 relatives à l'analyse d'impact.

113. Article 28 (3) (h), RGPD Cet aspect des obligations du sous-traitant fait actuellement l'objet de nombreuses polémiques notamment car il fait du sous-traitant le conseil juridique de son client, responsable de traitement.

114. Cf note 27 : notamment à «*assurer la sécurité du traitement, à notifier les violations de données à caractère personnel à l'autorité de contrôle et aux personnes concernées, à procéder aux analyses d'impact et à la consultation préalable de l'autorité de contrôle*».

II. LA RESPONSABILITÉ DU SOUS-TRAITANT INSCRITE DANS LE DROIT COMMUN DE LA RESPONSABILITÉ

Jusqu'alors uniquement responsable vis-à-vis du responsable de traitement au titre de ses obligations contractuelles, le sous-traitant peut désormais être responsable directement du fait de ses propres manquements (A). En parallèle, le sous-traitant peut engager sa responsabilité contractuelle vis-à-vis du responsable de traitement (B).

A. La responsabilité autonome du sous-traitant

Le RGPD introduit un nouveau régime de responsabilité du sous-traitant vis-à-vis des personnes concernées (1), mais également vis-à-vis du régulateur (2).

1. La responsabilité du sous-traitant vis-à-vis des personnes concernées

L'article 82 du RGPD prévoit que « toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable de traitement ou du sous-traitant réparation du préjudice subi » [115]. Cette disposition a pour objectif d'assurer la protection des personnes concernées et permettre qu'elles puissent obtenir une réparation effective de l'un quelconque des acteurs impliqués dans le traitement. Partant de ce postulat, le RGPD établit un régime de responsabilité équilibré entre responsable de traitement et sous-traitant.

Ainsi la responsabilité du sous-traitant pourra directement être mise en jeu par une personne concernée[116] et celui-ci pourra être tenu d'indemniser l'intégralité du dommage subi même s'il n'en est pas le seul responsable mais qu'il y a néanmoins contribué[117]. Néanmoins le sous-traitant ne supportera pas intégralement la responsabilité de la conformité du traitement et pourra engager un recours contre les autres acteurs du traitement pour récupérer le montant des indemnités versées[118].

La responsabilité du sous-traitant est cependant strictement encadrée puisque ce dernier ne pourra voir sa responsabilité engagée que s'il n'a pas respecté les obligations du RGPD qui lui incombent spécifiquement ou s'il a enfreint les instructions

115. Article 82 (1), RGPD.

116. A noter qu'en droit français, sous l'empire de la réglementation actuelle, il est possible pour la personne concernée de mettre en jeu la responsabilité du sous-traitant sous le régime délictuel.

117. Article 82 (4), RGPD.

118. Article 82 (4), RGPD.

du responsable du traitement[119]. La mise en jeu de la responsabilité du sous-traitant est donc conditionnée à la démonstration d'une faute de celui-ci.

Ainsi, le sous-traitant pourra voir sa responsabilité exonérée s'il apporte la preuve « que le fait qui a provoqué le dommage ne lui est nullement imputable »[120].

2. La responsabilité administrative autonome du sous-traitant

Le RGPD permet au régulateur d'imposer des sanctions administratives directement au sous-traitant en cas de manquement à ses obligations pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial[121].

Ces amendes, appliquées au sous-traitant, bien qu'identiques à celles encourues par le responsable de traitement, sanctionneront spécifiquement les manquements à ses obligations.

Dans les cas où le responsable de traitement et le sous-traitant se voient tous deux infliger une amende, la sanction du sous-traitant devra concerner des faits distincts de ceux ayant généré la sanction du responsable de traitement. Chaque acteur restera responsable de ses propres faits et aucune des parties ne se verra imposer de sanction du fait des agissements de l'autre. D'ailleurs, pour décider s'il y a lieu d'imposer une sanction ou pour décider de son montant, il devra être tenu compte du degré de responsabilité du responsable de traitement et du sous-traitant[122].

Néanmoins il ne faudrait pas que ce régime de responsabilité équilibré soit remis en cause par le jeu de la négociation contractuelle.

119. Article 82 (2), RGPD. Ainsi, comme le souligne le guide de la CNIL, le sous-traitant sera responsable s'il agit en dehors ou contrairement aux instructions licites du responsable de traitement, ou s'il n'aide pas le responsable de traitement à respecter ses obligations, par exemple en ne lui notifiant pas une violation de données, ou s'il ne l'aide pas à la réalisation d'une analyse d'impact, ou encore s'il fait appel à un sous-sous-traitant ne présentant pas de garanties suffisantes.

120. Article 82, RGPD.

121. Article 83 (4) et (5), RGPD.

122. Article 83 (2) (d), RGPD.

B. La responsabilité contractuelle du sous-traitant

1. Les possibles dérives de l'aménagement contractuel de la responsabilité du sous-traitant

Avec les nouveaux principes et obligations introduits par le RGPD, notamment le principe d'accountability,[123] il était légitime de penser que les acteurs des traitements de données personnelles n'auront pas à négocier des aménagements contractuels à leur responsabilité légale puisque une répartition est déjà prévue.

Toutefois, le RGPD exigeant que le sous-traitant et le responsable du traitement concluent un contrat définissant les missions du sous-traitant[124], certains responsables de traitement chercheront nécessairement à imposer des clauses limitatives ou exonératoires de responsabilité ou encore d'indemnisation à leur avantage.

La présence de telles clauses a pour effet de bouleverser l'équilibre des responsabilités respectives mises en place par le RGPD, en transférant contractuellement certaines responsabilités du responsable de traitement au sous-traitant ou vice versa, selon le degré de dépendance économique entre les parties. Cela pourrait même aller jusqu'à faire porter la charge financière de la sanction administrative au sous-traitant[125]en réduisant à néant l'action du régulateur, et ce, alors même que ces sanctions administratives ayant un caractère quasi-pénal, ne sont généralement pas assurables. Le responsable de traitement pourrait également imposer des clauses de responsabilité et d'indemnisation déplafonnées en faisant porter à son sous-traitant l'intégralité des conséquences financières du dommage, lui faisant ainsi jouer le rôle d'un assureur[126].

Afin de limiter ce type de pratiques et au vu de l'importance des sanctions prévues par le RGPD, il est essentiel de rappeler les règles du droit commun dans lesquelles cette responsabilité doit s'inscrire afin que ce ne soit pas le sous-traitant qui supporte l'intégralité du risque.

2. Les limites à l'aménagement contractuel de la responsabilité du sous-traitant

Si le sous-traitant et le responsable de traitement demeurent libres de prévoir des clauses de responsabilité dans leur contrat, cette liberté devra s'exercer dans les limites fixées par la loi[127] notamment aux vues des conditions posées par le droit commun des contrats. En effet, le Code civil dispose : « les contrats obligent non seulement à ce qui y est exprimé, mais encore à toutes les suites que leur donnent l'équité, l'usage et la loi. » [128]

123. Considérant 85 et Article 5 (2), RGPD : principe qui requiert du responsable du traitement de prendre des mesures efficaces et appropriées afin de se conformer au règlement européen et d'en apporter la preuve, sur demande de l'autorité de contrôle.

124. Cf I.B.

125. Cette situation est d'autant plus inacceptable que le sous-traitant pourra faire l'objet d'une sanction administrative autonome pour les faits qui lui sont propres.

126. Ces pratiques pourraient avoir un effet désastreux sur l'écosystème numérique et en particulier sur les petites structures qui ne pourront pas supporter financièrement une telle prise de risque.

127. Article 1102, Code Civil.

128. Article 1194, Code Civil.

Ainsi le Code Civil sanctionne « toute clause qui prive de sa substance l'obligation essentielle du débiteur est réputée non écrite »[129]. Il n'existe pas à ce jour de liste des clauses prohibées et il sera donc nécessaire de dégager un faisceau d'indices afin de démontrer que la clause de responsabilité contredit la portée des obligations essentielles prévues au contrat, qui sont elles-mêmes clairement prévues par la réglementation.

Les clauses de responsabilité pourront également être sanctionnées lorsqu'elles génèrent un « déséquilibre significatif » sur le fondement du droit spécial[130] ou du droit commun[131]. La notion de déséquilibre significatif entre droits et obligations des parties a vocation à appréhender toute situation et est appréciée au regard des effets de l'application de la convention entre les parties. Elle pourra donc venir rééquilibrer les relations entre responsable de traitement et sous-traitant.

La sanction de ces dispositions déséquilibrées engendre la nullité des clauses qui sont réputées non-écrites : non seulement les clauses sont privées d'effets, mais encore elles disparaissent du contrat. La conséquence en est un retour immédiat au droit applicable à la situation juridique.

Il est donc fort probable que les autorités verront d'un mauvais œil les clauses contractuelles limitatives ou déplafonnées de responsabilité, dès lors que celles-ci viendront priver d'effet certaines dispositions du RGPD ou encore de générer un déséquilibre significatif en contradiction avec le principe d'*accountability.*

Ainsi, dans le guide du sous-traitant publié par la CNIL, les clauses contractuelles de sous-traitance proposées ne traitent pas la question des responsabilités respectives du sous-traitant et du responsable de traitement, invitant les parties à se limiter à ce qui est prévu par le RGPD[132].

Alors que la tentation est forte de faire du sous-traitant le « gardien des données personnelles », force est de constater que bien au contraire, le RGPD met en place un nouveau cadre équilibré entre le responsable de traitement et le sous-traitant[133]tant au niveau de leurs obligations que de leur responsabilité avec pour objectif ultime de responsabiliser chacun des acteurs et de renforcer leur coopération au profit de la protection des données personnelles.

Mais il faudra veiller à l'application des principes d'équilibre et de bonne foi lors de la négociation des contrats entre responsable de traitement et sous-traitant. Devront notamment guider la définition des rôles et missions de chaque partie : la sensibilité des données personnelles, le coût du traitement, les couvertures d'assurances et leur coût, les risques potentiels et leur probabilité d'occurrence et les pratiques du marché.

129. Article 1170, Code Civil, consacrant la jurisprudence Chronopost (Cass Com, 22 Oct 1996 ; Cass Com 9 juillet 2002 ; Cass Mixte, 22 avril 2005 ; Cass Com, 30 mai 2006 ; Cass Com 13 juin 2006) et Faurecia (Cass Com 13 février 2007 ; Cass Com 29 juin 2010) ; A noter que Cette disposition génère à ce jour certaines incertitudes, notamment sur les concepts de « substance » et d'« obligation essentielle ».

130. Article L. 442-6 I. alinéa 2° du Code de Commerce et article L. 212-1 du Code de la Consommation : qui sanctionnent les obligations créant un déséquilibre significatif dans les droits et obligations des parties.

131. Article 1171, Code Civil.

132. CNIL, *Guide du sous-traitant*, Edition Septembre 2017.

133. Considérant 13, RGPD : « [...] un règlement est nécessaire [...] pour offrir aux personnes physiques de tous les États membres un même niveau de [...] responsabilités pour les responsables du traitement et les sous-traitants [...] ».

LE RGPD PERMET-IL DE TRANSFÉRER PLUS LIBREMENT LES DONNÉES HORS DE L'UNION EUROPÉENNE SUR LA BASE DU CONSENTEMENT ?

Stéphanie FABER,
Avocat Of Counsel, Responsable des pratiques droit commercial / IT et données personnelles / cyber-sécurité, Squire Patton Boggs, Paris

Le G29[134] avait interprété de façon très restrictive la possibilité offerte par la directive 95/46 de transférer des données hors de l'Union européenne sur la seule base du consentement de la personne concernée. Les nouvelles dispositions du règlement européen 2016/679 dit « RGPD »[135] sont-elles plus libérales sur ce point et notamment sur la condition que le transfert ne soit pas massif, répété ou structurel ?

Par le passé de nombreux responsables de traitements étaient tenté d'utiliser le consentement des personnes concernées pour le transfert des données vers des pays en dehors de l'Espace économique européen comme cela était prévu à l'article 26 (1) de la directive 95/46/CE du 24 octobre 1995 sur la protection des données personnelles (« directive 95/46 »).

Or, le G29 avait donné en 2005 une interprétation très restrictive des cas dans lesquels le consentement pouvait être utilisé pour un transfert international dans un document relatif à l'article 26 (1) de la directive 95/46 (« WP 114 »)[136].

En quoi le RGPD a-t-il pu modifier les règles s'appliquant à l'utilisation du consentement ?

134. Le Groupe de travail « article 29 » (« G 29 ») rassemble les représentants de chaque autorité de protection des données nationale et sera remplacé par le Comité européen de la protection des données « CEPD ». Certains des documents cités ci-après n'ont pas été traduits en français à la date de l'article

135. Le règlement européen 2016/679 dit « Règlement Général sur la Protection des Données » (« RGPD »).

136. « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 » du 25 novembre 2005 (« WP 114 »). La position de la CNIL avait suivi cette interprétation pour l'application de l'article 69 de la loi dite « Informatique et Libertés ».

I. LE FONDEMENT JURIDIQUE DE L'UTILISATION DU CONSENTEMENT POUR LES TRANSFERTS INTERNATIONAUX

A. Les dispositions du RGPD sur le transfert international de données personnelles

Le chapitre V du RGPD offre différentes bases juridiques pour le transfert de données personnelles vers des pays tiers ou à des organisations internationales :

Le caractère adéquat du destinataire : à savoir, le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou encore l'organisation internationale (« OI ») en question ; le caractère adéquat est établi, comme par le passé, sur la base d'une décision d'adéquation de la Commission européenne[137].

La mise en place de « garanties appropriés » par le destinataire ou avec lui. Les garanties[138] sont celles qui sont déjà utilisées aujourd'hui (comme les clauses contractuelles types adoptées par la Commission européenne ou les règles contraignantes d'entreprises dites « BCR ») ainsi que de nouveaux instruments (un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics, des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission, un code de conduite approuvé et un mécanisme de certification).

Les « dérogations » prévues par l'article 49 (1) du RGPD. Celui-ci prévoit que des transferts de données à caractère personnel vers un pays tiers ou une OI n'assurant pas un niveau de protection adéquat peuvent être effectués si l'une des conditions listées est remplie ; cette liste étant presque identique à celle de la directive 95/46.

B. Les dérogations incluant le consentement

Les transferts de données à caractère personnel vers un pays tiers ou une OI n'assurant pas un niveau de protection adéquat peuvent être effectués dans les cas suivants[139] :

Article 49 (1) premier alinéa, (a) à (g) :

La personne concernée a consenti explicitement au transfert (c'est le cas qui nous intéresse principalement).

- Le transfert est nécessaire :

- à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée ;

- à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;

137. Article 45, RGPD.

138. Article 46, RGPD.

139. Certaines de ces dérogations ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

- pour la sauvegarde des motifs importants d'intérêt public ;

- à la constatation, l'exercice ou la défense de droits en justice ;

- la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.

• Le transfert intervient au départ d'un registre qui, conformément au droit national ou de l'UE est destiné à l'information du public et est ouvert à la consultation par celui-ci ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

L'article 49 (1) deuxième alinéa prévoit une dérogation supplémentaire et nouvelle, assortie de nombreuses restrictions et conditions :

• Le transfert est « nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée ».

II. LE RÉGIME DES DÉROGATIONS

Comme pour la directive 95/46 « La juxtaposition de ces différentes règles relatives aux transferts de données personnelles peut donner une impression paradoxale et être aisément source de malentendus »[140]. D'une part, une première série de dispositions[141] visent à garantir que les données qui sont transférées continuent à bénéficier d'une protection adéquate après leur transfert vers le pays de destination, et d'autre part l'article 49 (1) permet des transferts vers des pays où il n'y a pas de protection adéquate en l'absence de garanties appropriées.

A. Une interprétation restrictive et un caractère exceptionnel

Des « Lignes directrices 2/2018 sur les dérogations de l'article 49 sous le règlement 2016/976 » (« Lignes Directrices »)[142] ont été adoptées le 25 mai 2018 par le Comité Européen de la Protection des Données « CEPD » (qui a remplacé le G29 le même jour), et qui font notamment référence au WP 114. Dans ce document, le G29 a donné une interprétation très restrictive de l'article 49 (1) RGPD : « Les dérogations doivent [...] être interprétées restrictivement afin qu'elles ne puissent pas devenir la règle » et met en avant le fait que le titre même de l'article 49 « Dérogations pour des situations particulières » reflète leur caractère exceptionnel.

140. WP114 visé ci-avant.

141. Articles 45 et 46, RGPD.

142. EDPB, *Guidelines 2/2018 on dérogations of Article 49 under Regulation 2016/679*, 25 mai 2018. En anglais et non traduit à la date de l'article.

B. L'absence de décision d'adéquation ou de garanties appropriées

En premier lieu, l'article 49 (1) prévoit qu'il n'est applicable qu'en « l'absence de décision d'adéquation, ou de garanties appropriées en vertu de l'article 46, y compris les [BCR] ». Cette disposition semble à première vue constituer une lapalissade. En effet, les dérogations ne sont pas nécessaires si le destinataire est considéré comme offrant une protection adéquate ou si des garanties appropriées sont en place.

Cependant, le G29 rappelle qu'il a depuis longtemps recommandé « une approche par étapes fondée sur les meilleures pratiques ». A savoir, « Si le niveau de protection dans le pays tiers n'est pas adéquat eu égard à toutes les circonstances, le responsable du traitement des données devrait considérer apporter des garanties adéquates. De ce fait, les sociétés exportatrices devraient d'abord s'efforcer de protéger les transferts par le biais de l'un des mécanismes des article 45 ou 46, et seulement, en leur absence, avoir recours aux dérogations de l'article 49 (1) ».[143]

Selon cette interprétation, il ne serait donc possible de recourir aux dérogations qu'après s'être « efforcé » de mettre en place des garanties appropriées.

C. Garantie du droit des personnes concernées

L'article 44 du RGPD « Principe général applicable aux transferts » encadre les transferts internationaux de façon générale et, de ce fait, aussi les transferts effectués en application de l'article 49 (1) du RGPD. Il dispose que le transfert s'effectue « sous réserve des autres dispositions du présent règlement ».

En cela, il fait référence à l'obligation de respecter, de façon générale, les droits des personnes concernées (information, droit d'accès, droit d'opposition etc.) et les obligations imposées aux responsables de traitement et sous-traitants dans la collecte et le traitement des données, le transfert n'étant qu'un aspect du traitement. Ces autres dispositions peuvent, le cas échéant, amener des contraintes supplémentaires à l'utilisation de ces dérogations. Ce principe est aussi évoqué dans les Lignes Directrices.

L'article 44 dispose par ailleurs, que « Toutes les dispositions du présent chapitre [V] sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis ». Cela signifierait que, même en l'absence de mise en place de garanties appropriées, il faut que, par d'autres moyens, le niveau de protection soit garanti.

Est-ce que cette disposition pourrait servir à étendre plus généralement certaines des obligations appliquées à la dérogation des « intérêts légitimes impérieux poursuivis par le responsable du traitement »[144], à savoir, que le responsable de traitement ait évalué toutes les circonstances entourant le transfert de données et qu'il offre, sur la base de cette évaluation, des garanties appropriées ?

143. Contrairement au WP114 de 2005, le texte des Lignes Directrices ne fait plus mention de ce que « [...] les dérogations [...] s'appliquent de préférence aux cas dans lesquels il serait vraiment inapproprié voire impossible que le transfert s'effectue sur la base [des garanties adéquates] ».

144. Article 49 (1) al.2, RGPD.

Cela n'est pas la position prise par le CEPD dans les Lignes Directrices. En se référant à l'article 44 du RGPD, il considère « que le recours aux dérogations [..], ne doit jamais conduire à une situation dans laquelle il pourrait y avoir violation des droits fondamentaux »[145]. Pour autant il n'en tire pas d'autre conclusion que le caractère exceptionnel des dérogations de l'article 49 (1). Pour lui, tout en faisant référence au considérant (144)[146], les dérogations de l'article 49 (1) constituent des « exemptions au principe général que les données personnelles ne doivent être transférées que vers des pays offrant un niveau de protection adéquat ou si des garanties adéquates sont offertes et que les personnes concernées bénéficient de droits opposables de façon à ce que lesdites personnes continuent de bénéficier des droits fondamentaux et des garanties ».

D. La condition d'absence de transferts massifs, répétés ou structurels

Dans le WP 114 de 2005, le G29 avait introduit une condition supplémentaire pour le recours aux modes exceptionnels de transferts, en recommandant : « que les transferts de données personnelles qui pourraient être qualifiés de répétés, massifs ou structurels soient, dans toute la mesure du possible et justement en raison de ces caractéristiques, effectués dans un cadre juridique spécifique (c'est-à-dire des contrats ou des [BCR]) ».

En ce qui concerne le RGPD, alors que le législateur avait largement l'occasion de reprendre une telle limitation, cette interprétation ne se retrouve pas de façon généralisée dans le texte. Ceci représente donc un changement par rapport à la position passée du G29.

La seule référence, dans les articles du RGPD, à la condition du caractère non répétitif et non massif des transferts, est faite pour le transfert nécessaire aux fins des « intérêts légitimes impérieux poursuivis par le responsable du traitement »[147]. De plus, la mise en œuvre de cette dérogation est accompagnées de conditions supplémentaires puisqu'elle ne s'applique que si (I) les autres dérogations ne peuvent pas s'appliquer, (II) que le responsable de traitement a évalué toutes les circonstances entourant le transfert de données et (III) a offert, sur la base de cette évaluation, des garanties appropriées (l'évaluation et les garanties devant être documentées au registre), (IV) informe l'autorité de contrôle et (V) informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

On peut donc supposer, a contrario, que ces conditions ne sont pas applicables aux autres dérogations, y compris le transfert sur la base du consentement.

Il y a cependant une référence plus large à ce type de limitation dans les considérants. En effet, en plus du considérant 113 qui reprend ce qui est prévu l'article 49 (1) deuxième alinéa concernant le transfert pour « motifs légitimes impérieux du responsable de traitement », le considérant 111 restreint les transferts nécessaires dans le cadre d'un contrat ou

145. La même considération apparaissait déjà dans le WP114.

146. Considérant 144, RGPD : « En tout état de cause, lorsque la Commission ne s'est pas prononcée sur le caractère adéquat du niveau de protection des données dans un pays tiers, le responsable du traitement ou le sous-traitant devrait adopter des solutions qui garantissent aux personnes concernées des droits opposables et effectifs en ce qui concerne le traitement de leurs données dans l'Union une fois que ces données ont été transférées, de façon à ce que lesdites personnes continuent de bénéficier des droits fondamentaux et des garanties ».

147. Article 49 (1) al.2, RGPD.

d'une action en justice à des cas où ce transfert est « occasionnel ».

Par conséquent, même après l'examen des considérants, il semblerait que, par un raisonnement a contrario, la restriction du caractère non massif, non répété ou non structurel ne s'applique plus au transfert sur la base du consentement des personnes concernées.

Le CEPB relève ce point dans les Lignes Directrices, mais tient à « souligner que même les dérogations qui ne sont pas expressément limités au transferts « occasionnels » ou « non répétitifs » doivent être interprétées dans un sens qui ne contredit pas la nature même des dérogations, à savoir quelles sont une exception à la règle [...] ». Ceci semble donc constituer une libéralisation potentiellement très importante pour les transferts sur la base du consentement.

Cependant, si le RGPD ne prévoit pas directement cette restriction, c'est peut-être parce que le régime du consentement crée indirectement une contrainte d'un effet identique.

III. LE CONSENTEMENT POUR LE TRANSFERT INTERNATIONAL

De nombreux groupes étrangers, et notamment américains, sont tentés d'utiliser le consentement des personnes concernées pour le transfert des données. Après tout, un des principes sous tendant le RGPD est de donner à la personne concernée le contrôle de ses données personnelles. Pour autant, l'utilisation du consentement est assortie de contraintes qui limitent sa flexibilité.

A titre liminaire, notons que le RGPD prévoit que le consentement ne peut pas être utilisé pour légitimer un transfert international dans le cadre d'activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique[148].

A. Conditions de validité du consentement

En application des articles 4 (11), 7 et 49 (1) a) du RGDP, pour être valable, le consentement doit, quelles que soient les circonstances dans lesquelles il est donné, respecter certaines conditions qui sont ont aussi donné lieu à des lignes directrices sur le consentement « WP 253 rev. 01 » par le G29 du 28 novembre 2017 et révisée le 10 avril 2018[149]. A ce titre le consentement doit être libre, spécifique, éclairé, univoque, et donné de façon explicite.

148. Article 49 (3), RGPD.

149. Le Groupe de travail « article 29 » (« G 29 »), *Guidelines on consent under Regulation 2016/679* . En anglais et non traduit à la date de l'article

1. Un consentement libre

La personne concernée doit disposer d'une véritable liberté de choix ou être en mesure de refuser ou de retirer son consentement sans subir de préjudice[150]. Le consentement ne peut pas être utilisé lorsqu'il existe un « déséquilibre manifeste entre la personne concernée et le responsable de traitement [...] et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière »[151]. A titre d'exemple cela peut généralement s'appliquer lorsque le responsable du traitement est une autorité publique ou encore dans les relations entre employeur et employés selon le WP 253 ainsi que l'avis 2/2017 sur le traitement des données au travail[152] (reprenant un avis de 2001[153]).

2. Un consentement spécifique

Le consentement vaut pour une finalité précise, qui doit être déterminée et définie. En cas de finalité ultérieure, un nouveau consentement de la personne concernée est nécessaire, à moins que cette finalité supplémentaire soit compatible avec la finalité initiale[154]. Selon les Lignes Directrices il doit donc être « spécifiquement donné pour le transfert ou la catégorie de transferts dont il s'agit » et le consentement ne peut pas être obtenu à l'avance « si le transfert n'est pas envisagé au moment où le consentement est demandé ».

150. Considérant 42, RGPD.
151. Considérant 43, RGPD.
152. Groupe Article 29, *Opinion 2/2017 on data processing at work (WP249)*,8 juin 2017.
153. Groupe Article 29 sur la protection des données, *Avis 08/2001 sur le traitement des données à caractère personnel (WP 48)*, 13 septembre 2001
154. Article 5 (b), RGPD.

3. Un consentement éclairé notamment sur les risques

Les articles 13 et 14 du RGPD prévoient qu'il faut informer la personne de l'absence de décision d'adéquation protégeant le transfert. Si l'on s'en réfère au WP sur le consentement, section 3.3.1, et aux Lignes Directrices page 7, les informations minimum requises pour le consentement éclairé couvrent : l'identité du responsable de traitement, les finalités du transfert, les catégories de données transférées, les catégories de destinataires, le fait que le consentement est la base juridique du transfert, le droit de retrait du consentement et ce qui suit. L'article 49 (1) du RGPD prévoit expressément que la personne doit avoir préalablement été informée « des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées ». Les Lignes Directrices envisagent que les informations, « qui pourraient être standardisées », puissent inclure des mentions que « le pays tiers ne dispose pas d'une autorité de protection des données et/ou de principes de protections des données personnelles et/ou que les personnes concernées ne bénéficient pas des mêmes droits [que sous le RGPD]. » Le CEPD ajoute à ces informations « tous les pays vers lesquels les données sont transférés ». Ce qui confirme la position adoptée par le G29 dans les lignes directrices « WP 260 rev. 01 » sur la transparence[155] « en application du principe de loyauté, l'information [...] doit être la plus utile possible [...] ce qui signifie généralement que les pays soient désignés nommément »[156].

4. Un consentement univoque

A savoir son interprétation ne doit pas dépendre du contexte dans lequel le consentement a été donné.

5. Un consentement donné de façon explicite

Ceci semble être une exigence encore plus forte que l'exigence plus générale d'une « déclaration » ou d'un « acte positif clair ». Le consentement ne peut pas être implicite. Le considérant 32 du RGPD précise « Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité ».

155. Groupe Article 29, Guidelines on transparency under Regulation 216/679 « WP 260 rev. 01 », adopted on 29 November 2017 and last revised on April 2017 non traduite en français à la date de l'article.

156. Ibid, tableau pages 37 et 38.

B. Les conséquences de l'utilisation du consentement

En application de l'article 7 (3) du RGPD « Le consentement doit pouvoir être retiré à tout moment ». Or, comme le relève le WP 114 « [...] le groupe de travail estime que le consentement n'est pas susceptible de fournir un cadre adéquat à long terme pour les responsables du traitement, en cas de transferts répétitifs ou même structurels pour le traitement en question. De fait, et en particulier si le transfert fait partie intrinsèque du traitement principal (par exemple, la centralisation d'une base de données mondiale de ressources humaines, dont le fonctionnement nécessite des transferts de données permanents et systématiques), les responsables du traitement risqueraient de se trouver eux-mêmes dans des situations insolubles si ne fût-ce qu'une personne concernée par le transfert décidait ultérieurement de retirer son consentement [...] Le recours au consentement peut donc se révéler être une « fausse bonne solution », simple de prime abord, mais en réalité complexe et lourde à gérer ».

Conclusion

Le consentement de la personne concernée ne pourra être utilisé que de façon limitée pour les transferts internationaux en général et pour des transferts massifs, répétés ou structurés en particulier (malgré l'absence de restriction expresse à cet effet dans le RGPD), en raison non seulement du régime applicable à l'ensemble des dérogations de l'article 49 (1), mais aussi, en pratique, des conditions accompagnant l'utilisation du consentement.

CRÉER UN « DATA LAKE » AU SEIN D'UNE BANQUE

Bleiz TOURAILLE
-
Martin PAILHES

Les exigences en matière réglementaire, la valeur croissante de la donnée à caractère personnel et la forte inflation des projets impliquant un traitement massif de données sont autant de raisons qui appellent la création de *Data Lakes* mutualisés au sein des établissements bancaires et placent le sujet de la valorisation et la protection des données au cœur des enjeux pour la banque.

La donnée est devenue un enjeu métier crucial, au cœur de la relation client qui constitue l'une des priorités stratégiques pour le secteur bancaire et financier.

La banque dispose assurément d'un capital confiance important, et son positionnement doit reposer sur la sécurisation des échanges et la protection des données *(security and privacy by design)* ainsi que sur la clarté de ses pratiques en matière d'utilisation des données de ses clients.

Le *Data Lake* associé aux technologies de *Big Data* est essentiel pour la transformation digitale de la banque en ce qu'il permet de répondre aux exigences d'un environnement réglementaire en constante évolution, mais aussi parce qu'il offre une grande capacité de stockage, facilite le traitement rapide et agile des données et fait apparaître de nouveaux usages.

Le terme *Data Lake* n'en reste pas moins un de ces concepts à la mode aujourd'hui au même titre que le *Big Data,* la cybersécurité, les robots, l'intelligence artificielle ou le *machine learning.* Mais que recouvre précisément ce terme, d'un point de vue opérationnel et commercial, quel en est l'intérêt pour les banques (I) et quels sont les risques ainsi que les contraintes juridiques associés à la mise en place d'un *Data Lake* au sein d'une banque en France (II).

I. LE CONCEPT DE *DATA LAKE*

A. Qu'est-ce qu'un *Data Lake* ?

1. Une tentative de définition

Pour Vincent Heuschling, expert en données, « le *Data Lake,* ou lac de données, est un concept (...) lié à la mouvance Big Data. L'idée générale est de pouvoir fournir un stockage global des informations présentes dans l'entreprise. Il s'agit de le faire avec suffisamment de flexibilité pour interagir avec les données, qu'elles soient brutes ou très raffinées »[157].

Autrement dit et, comme son nom l'indique bien, le Data Lake est un vaste réceptacle dans lequel viennent se déverser des données de l'entreprise, données qui peuvent être de types très variés : « Le Data Lake regroupe les données structurées en provenance de bases de données relationnelles en couloir ou en colonne, les données semi-structurées telles que les CSV, les logs, les XML, les JSON, et les données non structurées telles que les emails, les documents et les PDF. On y trouve même des données binaires telles que des images, des fichiers audios ou des vidéos »[158].

Le stockage en un même endroit des données de l'entreprise permet ainsi de réduire, voire d'éliminer les silos de données, en rendant ces données directement accessibles à partir d'un endroit unique et en temps réel.

2. Mise en place technique d'un Data Lake

Ce vaste réceptacle à données est rendu possible technologiquement par le Cloud Computing, ou informatique en nuage, qui offre des capacités de stockage quasi-illimitée pour des coûts pouvant être très faibles en fonction du modèle choisi : ex. Cloud Computing public c'est-à-dire une solution informatique en nuage mutualisée pour de nombreux clients et maintenue par un prestataire spécialisé du type Amazon Web Services, Microsoft Azur or Google Cloud.

Au sein de grands groupes bancaires comportant de nombreuses sociétés aux activités souvent variées (banque de détail, banque d'investissement, banque privée, leasing, assurance, « asset management », gestionnaire de flottes de véhicules,...) un Data Lake pourrait se concevoir techniquement sous deux formes :

- une forme décentralisée : dans ce modèle chaque société du groupe serait responsable de mettre en place son propre Data Lake. Les différents Data Lakes ainsi créés pourraient être amenés à communiquer entre eux sous réserve des différentes contraintes mentionnées ci-après. Ainsi cela pourrait permettre d'enrichir les données sur un client contenues dans un Data Lake, par des données additionnelles

157. http ://www.journaldunet.com/solutions/dsi/1165409-qu-est-ce-que-le-datalake-le-nouveau-concept-big-data-en-vogue/, *Qu'est-ce que le Data Lake, le nouveau concept « Big Data » en vogue*.

158. http ://www.lebigdata.fr/data-lake-definition, *Data Lake : définition, avantages et inconvénients pour l'entreprise.*

sur ce même client contenues dans d'autres Data Lakes du groupe.

• une forme centralisée : dans ce modèle une société du groupe servirait de réceptacle technologique et juridique pour le stockage des données des autres sociétés du groupe. Ces données seraient ainsi stockées en un point unique et accessible par les sociétés du groupe en fonction d'autorisations qui leur seraient données découlant notamment de contraintes de sécurité et réglementaires, voir ci-après.

B. L'intérêt du *Data Lake* pour une banque

1. Un intérêt opérationnel et de conformité

Afin de répondre aux exigences de conformité réglementaire en pleine expansion pour l'activité bancaire (BCBS 239[159], Bâle III[160]), la création de Data Lake au sein des établissements bancaires permet de satisfaire à des impératifs de traçabilité, de rapprochement et de disponibilité de données de source hétérogène et dispersée en les agrégeant et en les stockant au sein d'un entrepôt unique pour en faciliter l'accès, la consultation et la transmission. A titre d'illustration, la banque doit être en mesure de répondre dans les délais impartis à des demandes de communication d'informations ou de données formulées par les autorités de supervision ou judiciaires. L'impossibilité de fournir les données exigées pourrait exposer la banque à un risque de sanction.

Le *Data Lake,* en réconciliant et en traçant des données de source et de nature diverses, va également permettre d'assurer la conformité aux réglementations DSP2[161]et RGPD[162] lors de l'exercice de certains droits ou de certaines obligations. La recherche et l'identification de données personnelles attachées à des individus par exemple seront ainsi facilitées pour répondre aux demandes de droit d'accès, de rectification, de droit à l'effacement ou encore pour satisfaire au nouveau droit à la portabilité[163].

Quel que soit le système d'information utilisé ou l'environnement applicatif, souvent très hétérogène, le *Data Lake* contribue à satisfaire aux enjeux de disponibilité des données et augmente l'efficacité opérationnelle de la banque et la gestion de ses risques tout en assurant la sécurité et la protection de ses données.

159. BCBS 239 désigne une norme issue des travaux du Comité de Bâle et applicable dès janvier 2016, visant essentiellement à renforcer la qualité des données remontées par la banque depuis les clients jusqu'au régulateur, pour mieux évaluer les risques des banques à risque systémique.

160. Bâle III désigne les Accords de Bâle III publiés le 16 décembre 2010 et ayant pour objectif d›imposer aux banques des règles de solvabilité et de contrôle prudentiel harmonisés au niveau mondial.

161. DSP2 désigne la Directive concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n o 1093/2010, et abrogeant la directive 2007/64/CE.

162. GDPR ou RGPD en Français désigne le Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

163. Cf RGPD articles 15 à 22 concernant ls droit des personnes concernées.

2. Un intérêt commercial

Mieux gérer techniquement et opérationnellement les données au sein d'un Data Lake va également permettre, par l'organisation de données disponibles et de qualité, une amélioration de la connaissance client et par là même des services rendus au client.

Ces technologies nouvelles améliorent les capacités de calculs et de stockage, accroissent la qualité de production et l'agilité du système d'information de la banque, mais aussi permettent d'analyser, d'organiser et donner du sens à la vaste quantité de données générée par l'activité bancaire, cela pour mieux identifier les besoins et attentes de ses clients et leur offrir des services personnalisés au plus proche de leur situation avec une tarification plus appropriée.

Leur intérêt est double : à la fois pour les clients et les institutions financières comme le résume l'*European Banking Association* (EBA) : « les utilisations innovantes de la donnée peuvent avoir des bénéficies pour les clients en améliorant la qualité des produits et leur offrant des services plus personnalisés et adaptés à leurs besoins ainsi qu'une meilleure vision de leur situation financière. Ils peuvent également amener à des économies pour les clients (...) par exemple au travers d'offres ciblées pour avec des partenaires commerciaux spécifiques. Dans l'autre sens, les institutions financières peuvent également bénéficier d'un meilleur ratio coût/revenu, d'une meilleure gestion du risque et conformité réglementaire »[164].

Le *Data Lake* facilite enfin la réalisation d'expérimentations ou « Proof of Concept »[165] sur de nouveaux cas d'usages innovants qui seront, demain, à l'origine du développement de nouveaux services à forte valeur ajoutée aux clients, comme par exemple une capacité de détection et de lutte contre la fraude en temps quasi-réel pour protéger le client et ses avoirs.

164. European Banking Association, Report on innovative uses of consumer data by financial institutions , § 22, https ://www.eba.europa.eu/documents/10180/1720738/Report+on+Innovative+uses+of+data+2017.pdf (traduction par les auteurs).

165. « Proof of Concept » ou POC désigne une réalisation expérimentale préliminaire visant à démontrer la faisabilité d'un projet.

II. CONTRAINTES À LA MISE EN PLACE D'UN *DATA LAKE* AU SEIN D'UNE BANQUE EN FRANCE

A. Contraintes de sécurité

1. Menaces sur les données : cybercrime

Internet et les mutations technologiques tels que le Cloud Computing, les objets connectés, les tablettes et mobiles ont marqué un coup d'arrêt aux modèles de sécurité fermée et, en offrant une proximité et une immédiateté entre la banque et ses clients, ont également considérablement accru les risques de cyber-attaques. La banque est désormais interconnectée avec ses clients, ses prospects, ses candidats, ses partenaires, ses fournisseurs, ou encore ses régulateurs, représentant autant d'accès de son système d'information ouverts vers l'extérieur.

La vision centralisée de son patrimoine informationnel au sein d'un Data Lake est n'en doutons pas de nature à susciter des convoitises et des intentions malveillantes visant à s'introduire, à capter les données, les altérer ou les corrompre, ou bien les rendre indisponibles pour chercher à couvrir une fraude ou encore provoquer la paralysie des services proposés. Dans une forme centralisée de Data Lake telle qu'évoquée ci-dessus où les données d'un groupe bancaire seraient stockées au sein d'un réceptacle unique, l'effet d'un ransomware[166], tel que Wannacry ou Petya, qui ont sévit au premier semestre 2017, visant à crypter les données, serait désastreux !

La création d'un Data Lake doit ainsi répondre à cette image de coffre-fort électronique garantissant la confidentialité, la sécurité et protection des données de la banque et de ses clients. Les mesures techniques et organisationnelles de sécurité doivent ainsi être à la hauteur des enjeux. Les données stockées ou traitées dans un Data Lake doivent en permanence demeurer intègres, disponibles, être régulièrement sauvegardées et facilement récupérables par la banque. Elles seront chiffrées en fonction de leur niveau de confidentialité et soumises à des plans de continuité d'activité.

166. Logiciel malveillant cryptant les données, ne les décryptant que contre rançon financière. Dans le cas de Petya l'objectif aurait été de rendre les données inutilisables indépendamment du paiement d'une rançon

2. Des exigences de sécurité renforcées pour certaines banques :

Le cadre juridique applicable aux failles de sécurité et violations de données, pouvant survenir à l'occasion d'une cyber-attaque ou d'un incident de sécurité informatique, a connu une inflation de textes applicables, en particulier au secteur bancaire en France et en Europe.

La Directive NIS[167] en Europe, et plus spécifiquement la Loi de programmation militaire[168] (LPM) en France comportent un volet s'adressant directement aux opérateurs d'importance vitale (OIV) fournissant des services indispensables à la survie de la Nation. A ce titre certaines banques sont directement concernées par des dispositions relatives à la sécurité des systèmes d'information (SI) des opérateurs d'importance vitale. Afin de prévenir les risques d'atteintes à leurs installations informatiques, ces opérateurs se voient imposer la mise en place de mesures de sécurité particulières telles que des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité des SI, des notifications aux autorités de tout événement susceptible d'affecter la sécurité des SI, ou encore des contrôles et audits de ces mêmes autorités visant à vérifier le niveau de sécurité des SI de la banque.

Citons également le RGPD[169] qui étend une obligation de notification des violations de données, qui ne concernait à l'origine que les seuls opérateurs de réseaux de communication au public, à l'ensemble des responsables de traitements dès lors que la violation entraîne une atteinte à la disponibilité, l'intégrité ou la confidentialité de données à caractère personnel faisant l'objet d'un traitement. L'obligation de notification à la CNIL devra intervenir sans délai et au plus tard dans les 72 heures suivant la découverte par le responsable de traitement de la violation, et le responsable de traitement pourra également être tenu d'informer les personnes concernées lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés des individus.

La 2e Directive relative aux services de paiement (DSP2)[170] prévoit aussi que les Prestataires de Services de Paiement (PSP) doivent depuis janvier 2018 informer sans retard injustifié l'autorité compétente en cas d'incident opérationnel ou de sécurité majeur. Et lorsque l'incident a ou est susceptible d'avoir des répercussions sur les intérêts financiers des utilisateurs, le PSP devra également informer les utilisateurs de l'incident ainsi que des mesures qu'ils peuvent prendre pour atténuer les effets dommageables de l'incident.

Enfin en ce qui concerne la réglementation bancaire, la Banque Centrale Européenne (BCE) a décidé que toute entité soumise à la surveillance prudentielle a l'obligation de lui déclarer les incidents significatifs liés à la sécurité de l'information. L'objectif de la BCE est de contribuer à la sécurité et à la solidité des établissements de crédit ainsi qu'à la stabilité du système financier au sein de l'Union et dans chaque État membre.

167. La Directive NIS pour « Network and Information Security », adoptée le 6 juillet 2016, définit des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Européenne.

168. La Loi de programmation militaire (LPM), adoptée le 18 décembre 2013, ayant vocation à couvrir les années 2014 à 2019, comporte un volet s'adressant directement aux opérateurs d'importance vitale (OIV) fournissant des services indispensables à la survie de la Nation, dont certaines banques.

169. Articles 33 et 34 RGPD.

170. La DSP2 désigne la Directive de Services de Paiement, publiée le 23 février 2017 et visant à réguler de nouveaux acteurs financiers et à améliorer la sécurité de leurs échanges.

B. Contraintes juridiques au partage des données à des fins business et marketing

1. La Propriété intellectuelle

Lors de l'alimentation du Data Lake en données il conviendra de porter une attention toute particulière aux données en provenance de sources tierces. En effet la tentation peut être grande de considérer que toutes données consultables et disponibles sur Internet et présentant a priori un caractère public sont libres de droits et donc « aspirables » sans contraintes ni autorisations préalables pour alimenter le Data Lake en données toujours plus riches, larges et précises.

Dans une délibération du 21 septembre 2011, la CNIL a d'ailleurs adressé un avertissement public à un éditeur d'annuaires qui avait indexé et diffusé sans consentement préalable des données personnelles de plusieurs millions d'internautes présents sur des réseaux sociaux. L'activité de « webcrawling » permettant d'aspirer les données personnelles figurant dans les profils de réseaux sociaux, en l'absence d'autorisation des personnes concernées, est un traitement « déloyal » contraire à la réglementation sur la protection des données.

Des bases de données externes à celles générées par l'activité bancaire peuvent bien évidemment être fournies par des prestataires et dans ce cas, c'est le contrat qui permettra de garantir que celles-ci ont bien été acquises ou collectées régulièrement. Le prestataire doit contractuellement déclarer et certifier à son client qu'il est bien autorisé à en disposer et qu'il n'enfreint pas par là même le droit d'un tiers, comme un droit de propriété intellectuelle par exemple, ou le droit des personnes dans le cas de données à caractère personnel. En cas d'atteinte portée aux droits de tiers, c'est encore le contrat qui permettra à la banque d'appeler son prestataire en garantie pour l'éviction subie et d'engager le cas échéant sa responsabilité contractuelle du fait des manquements du prestataire.

2. la Protection des données à caractère personnel : le RGPD

Une autre contrainte significative à la mise en place d'un Data Lake découle du nouveau cadre en matière de protection des données à caractère personnel dans l'Union Européenne posé par le RGPD.

Comme expliqué ci-avant, l'intérêt d'un Data Lake est de pouvoir partager de la donnée entre entités d'un même groupe bancaire et l'utiliser notamment à des fins potentiellement autres que pour celles initialement prévues (traitement ultérieur). Or ces deux objectifs, partage et usage, sont fortement impactés par le RGPD lorsque des données à caractère personnel sont concernées.

a. Partage de données à caractère personnel entre entités

Le RGPD fait obligation à tout responsable de traitement de fournir un certain nombre d'informations obligatoires aux personnes dont il collecte directement des données à caractère personnel[171].

Cela inclut notamment d'informer sur « les destinataires ou les catégories de destinataires des données à caractère personnel »[172] c'est-à-dire les autres sociétés ou organismes à qui seraient transférées ces données : ex. des sociétés du groupe bancaire auquel appartient le responsable du traitement.

De plus, pour être licite, tout traitement de données à caractère personnel, en plus de respecter les principes relatifs au traitement de l'article 5 du RGPD, doit reposer sur l'une (au moins) des conditions limitativement énumérées à l'article 6 du RGPD. La plus connue de ces conditions étant le consentement : « la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques »[173].

Or sous le régime du RGPD, obtenir un consentement conforme à la loi est rendu plus contraignant : cf nouvelle définition du « consentement »[174] avec en gras les ajouts par rapport à la Directive de 95[175] : « 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 ».

Le fait pour un client de savoir que ses données seront partagées avec d'autres sociétés, fussent-elles des sociétés d'un même groupe bancaire, pourrait le conduire à ne pas consentir à ce traitement voire, après y avoir consenti, à retirer aisément son consentement comme le RGPD le lui permet[176].

b. Traitement ultérieur de données à caractère personnel pour des finalités autres que la finalité initiale

Comme présenté ci-avant, « le Data Lake, ou lac de données, est un concept (…) lié à la mouvance Big Data ». L'essence même du Big Data est de 'faire parler' les données en croisant différentes données afin d'en dégager de nouvelles informations qui pourraient avoir une utilité commerciale.

Or l'un des six principes clés de tout traitement de données à caractère personnel énoncés par le RGPD est que les données caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités »[177].

Cela semble donc incompatible avec la logique du Big Data de collecter maintenant pour voir plus tard ce qu'il pourrait en être tiré en termes d'informations : ex. quelles informa-

171. Article 13, RGPD.

172. Article 13 (1) (e), RGPD.

173. Article 6 (1) (a), RGPD.

174. Article 4 (11), RGPD.

175. Le Directive de 95 désigne la 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.

176. Article 7 (3), RGPD.

177. Article 5 (1) (b), RGPD.

tions pourraient être tirées de données collectées à de strictes fins d'effectuer des paiements.

C'est ce que confirme le Groupe de l'Article 29 (G29) dans son Opinion 03/2013 sur la « limitation des finalités » et plus particulièrement dans l'annexe 2 de ladite opinion consacrée au Big Data[178]. Tout en posant une analyse concernant ce qu'est un traitement ultérieur, le G29[179] détaille des conditions qui pourraient faire que ledit traitement soit tout de même valide.

3) le secret bancaire et le consentement

La création d'un Data Lake au sein d'un groupe bancaire impliquera nécessairement que soit analysé en amont la faisabilité juridique et la conformité du projet au regard de chacune des réglementations potentiellement applicables dont bien entendu les règlementations bancaires. En effet le transfert des données en provenance de chacune des entités composant un groupe international vers un *Data Lake* mutualisé appelle non seulement le respect des règles de protection des données à caractère personnel mais également celles relevant du secret professionnel et des règles spécifiques de chaque pays d'origine en matière de transfert de données couvertes par le secret bancaire vers un pays tiers.

Ainsi dans certains pays il conviendra de présenter un dossier d'information à destination du ou des régulateurs, dans d'autres obtenir l'autorisation préalable des autorités de supervision, ou encore se voire confronter à un principe d'interdiction de transfert de ce type de données vers des pays tiers au pays d'origine.

Vis-à-vis du client lui-même il conviendra en fonction des juridictions en cause, de recueillir individuellement l'accord express et spécifique du client pour obtenir la levée du secret bancaire, ou de l'en informer au titre d'un courrier ad hoc ou de la documentation contractuelle de ce flux de données. Or à l'occasion de la mise en œuvre de tels projets, certains clients pourraient s'opposer à ce que leurs données soient transmises à l'étranger dans le cadre d'un traitement de leurs données centralisé et ainsi soit mettre en cause la viabilité économique du projet ou encore remettre en cause leur relation contractuelle avec l'établissement bancaire engendrant ainsi un risque de perte de clientèle.

Enfin, certaines réglementations bancaires peuvent imposer de compartimenter les données bancaires et ainsi exiger la mise en place de pré requis techniques de type « muraille de Chine » afin de garantir que la solution de Data Lake envisagée intègre bien dès sa conception une ségrégation logique entre les données provenant de différents pays voire de différentes entités, avec des règles strictes de droits d'accès et de consultation.

178. Groupe de Travail « Article 29 » sur la protection des données, *Avis 03/2013 sur la Limitation des fnalités*, 2 avril 2013.

179. Le G29 ou Groupe de travail Article 29 sur la protection des données désigne la réunion des autorités de protection des données européennes au sein d'un organe consultatif indépendant sur la protection des données et de la vie privée. Son organisation et ses missions sont définies par les articles 29 et 30 de la Directive 95/46/CE.

Conclusion

Si l'idée d'un Data Lake, vaste réceptacle de données, au sein d'un groupe bancaire est séduisante, sa mise en place tant technologiquement que juridiquement s'avère un véritable défi.

D'autres risques liés à la qualité des sources, données déversées dans le lac sans gouvernance ni contrôle qualité, peuvent transformer un Data Lake en Data Swamp (marais à données!) et rendre très faible voire nulle son utilité.

Toutefois et pour rebondir sur les conclusions de l'EBA citées ci-avant : les utilisations innovantes de la donnée (dont le *Data Lake* fait partie à notre sens) peuvent avoir des bénéficies pour les clients et les institutions financières.

Dès lors la mise en place valide de *Data Lakes* pourrait passer notamment par :

- de plus grands efforts « d'éducation » et de transparence des banques à destination des clients comme le suggère l'EBA dans son rapport[180] afin de mieux les éclairer quant aux « opportunités et risques » de ces utilisation innovantes, et

- une meilleure appréhension par les banques des principales réglementations impactant la mise en place d'un *Data Lake* afin d'en cartographier les contraintes et donc les limites à l'utilisation qui peut être faite des données.

Ces limites pourraient être amenées à évoluer dans un sens moins contraignant au fur et à mesure que I) les clients seraient mieux informés sur ces nouveaux usages et y trouveraient un bénéfice grandissant et II) les régulateurs apprécieraient que cela ne se fasse pas au détriment des droits desdits clients.

180. European Banking Association, *Report on innovative uses of consumer data by financial institutions* , § 71, https ://www.eba.europa.eu/documents/10180/1720738/Report+on+Innovative+uses+of+data+2017.pdf (traduction par les auteurs).

ACTIONS DE GROUPE EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN EUROPE

Christine GATEAU,
Avocate associée Contentieux, Cabinet Hogan Lovells - Paris

Les actions de groupe sont courantes aux États-Unis mais relativement rares en Europe. L'Union européenne (UE) a souhaité faire évoluer ce constat en facilitant les actions de groupe en cas de violations de masse de la vie privée et des données à caractère personnel.

Avec le développement du Big Data l'étendue et l'impact de potentielles violations ou pertes de données se sont en effet considérablement accrus. Chaque jour, quelque part dans le monde, les médias relayent que les données à caractère personnel d'un très grand nombre d'individus, souvent des millions de personnes, ont été violées. Dès lors, les autorités publiques considèrent les actions de groupe comme une mesure corrective éventuelle pour ces violations, voire un moyen de les empêcher.

A première vue, rien n'est plus rationnel : les violations de données à caractère personnel causent à chaque personne un préjudice très limité, si ce n'est aucun préjudice. Il est souvent peu probable que ce préjudice suffise à motiver les individus à demander réparation (ou même à rechercher la personne responsable de cette violation). Or, un groupe entier de personnes concernées par la violation pourrait avoir un intérêt à demander réparation du préjudice global, d'où l'idée de permettre les actions de groupe.

Mais est-ce si simple ? Cet article a pour objet de prendre du recul et d'analyser ce sujet plus en détail en :

- mettant en perspective l'expérience acquise aux États-Unis au cours des dernières années,
- examinant le choix fait par l'UE d'ouvrir timidement la porte aux actions de groupe en matière de protection des données à caractère personnel,
- partageant quatre principaux enseignements à garder en tête face aux actions de groupe en matière de protection des données à caractère personnel en Europe.

I. ACTIONS DE GROUPE EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL AUX ÉTATS-UNIS

A. Le premier obstacle : la condition relative à la qualité pour agir et le besoin d'un « préjudice en fait »

Au cours des dernières années, les américains ont assisté à une hausse du nombre d'actions de groupe contre les pratiques de sociétés en matière de respect de la vie privée et de sécurité des données. Tandis que le nombre d'actions de groupe ne cesse d'augmenter, les procès font face à

des défis majeurs. Ils n'ont permis aux consommateurs d'obtenir qu'une réparation limitée et n'ont pas dégagé de normes cohérentes en matière de respect de la vie privée aux ÉtatsUnis. En comparaison, l'agence indépendante du gouvernement fédéral aux États-Unis, la Commission fédérale du commerce (Federal Trade Commission - FTC), s'est avérée bien plus efficace dans la mise en œuvre des pratiques en matière de respect de la vie privée et de sécurité des données.

Les actions de groupe ne se sont pas avérées être un mécanisme efficace pour les demandeurs aux États-Unis souhaitant obtenir réparation de prétendues violations de leur vie privée. Ceci résulte de la difficulté, en droit américain, de retenir un préjudice indemnisable causé par une violation d'un droit lié au respect de la vie privée. En effet, les demandeurs doivent démontrer leur qualité pour agir afin d'être en mesure de faire valoir leurs droits devant une cour fédérale. La qualité pour agir a été interprétée comme exigeant des demandeurs qu'ils établissent, entre autres, qu'ils aient subi un « préjudice en fait » *(injury in fact)* qui soit concret et réel ou imminent et non hypothétique ou incertain. De nombreuses actions de groupe ont échoué car les demandeurs n'avaient pas suffisamment démontré l'existence d'un « préjudice en fait » permettant de leur conférer la qualité pour agir[181].

Les défis auxquels les demandeurs font face pour prouver leur qualité pour agir se retrouvent également dans le contexte des actions de groupe pour violation de données à caractère personnel. De nombreuses juridictions américaines ont rejeté des demandes liées à des cyber-attaques sur le fondement d'une absence de qualité pour agir. Par exemple en retenant que les allégations des demandeurs quant à une menace de préjudice futur à laquelle ils feraient face du fait d'un potentiel détournement de leurs données à caractère personnel, ne permettent pas d'établir leur qualité pour agir. Ces juridictions retiennent que ce qui pourrait ou non être fait avec les données à caractère personnel d'une victime d'une cyber-attaque est trop spéculatif et ne constitue pas un préjudice concret, immédiat et suffisant pour leur conférer la qualité pour agir[182]. Lorsque les demandeurs allèguent que leurs données à caractère personnel ont été détournées par des criminels, les juridictions sont en revanche plus susceptibles de considérer que ces allégations d'activités frauduleuses sont suffisantes pour établir un « préjudice en fait »[183]. Cependant, de manière générale, le simple risque d'un détournement futur des données par des criminels ne vient pas appuyer la thèse d'un préjudice viable[184]. Néanmoins, la condition relative à la qualité pour agir résultant du concept de « préjudice en fait » de la Constitution américaine reste un obstacle souvent difficile à franchir pour les demandeurs.

La Cour suprême des États-Unis a rappelé aux tribunaux de première instance qu'un demandeur doit alléguer un préjudice qui soit à la fois « personnalisé », c'est-à-dire que le demandeur principal a été personnellement affecté par le comportement du défendeur, et « concret », ce qui signifie qu'un « préjudice en fait » est nécessaire. Alléguer simplement qu'une loi a été violée n'est pas suffisant.

181. *Facebook Internet Tracking Litig.*, N° 5 :12-md-02314-EJD, 2015 WL 6438744 (N.D. Cal. 23 Oct. 2015) ; *LaCourt c/ Specific Media, Inc.*, N° SACV 10-1256-GW(JCGx), 2011 WL 1661532 (C.D. Cal. 28 Avr. 2011).

182. Voir, par exemple, *Reilly c/ Ceridian Corp.*, 664 F.3d 28 (3d Cir. 2011) ; *Whalen c/ Michael Stores Inc.*, N° 14-CV_7006 (JS)(ARL), 2015 WL 9462108 (E.D.N.Y. 28 déc. 2015) ; *Storm c/ Paytime, Inc.*, N° 14-cv-1138, 2015 WL 1119724 (M.D. Pa. 13 mars 2015) ; *Peters c/ St. Joseph Servs. Corp.*, N° 4 :14-cv-2872, 2015 WL 589561 (S.D. Tex. 11 fév. 2015).

183. Voir, par exemple, *Remijas c/ Neiman Marcus Grp., Inc.*, 794F.3d 688 (7th Cir. 2015).

184. Voir, par exemple, *Scientific Applications International Corp.* 45 F.Supp.3d 14 (D. D.C. 2014).

B. Le second obstacle : les fondements de l'action

Même lorsque les consommateurs sont en mesure de franchir la question préliminaire de savoir s'ils ont subi un préjudice indemnisable lié à la violation de leur vie privée, il est en outre difficile de trouver des fondements juridiques viables par le biais desquels les demandeurs peuvent obtenir réparation. Ceci s'avère déjà difficile du fait des lois fédérales, la plupart des demandes liées au respect de la vie privée ne cadrant pas parfaitement au régime statutaire fédéral existant. Aucune loi actuelle ne prévoit de fondement exprès afin d'obtenir réparation pour les individus ayant prétendument subi un préjudice lié à la violation de leur vie privée.

Les demandeurs ont par conséquent essayé de fonder leurs demandes sur diverses autres lois fédérales, y compris celles conçues en premier lieu pour protéger les systèmes et communications des hackers et pirates. Par exemple, la loi sur les fraudes et infractions dans le domaine informatique (« Computer Fraud and Abuse Act ») vise de nombreuses activités liées à l'informatique, mais afin d'être en mesure d'intenter une action au titre de ses dispositions, un demandeur doit alléguer un préjudice réel d'au moins 5.000 dollars. Cependant, puisqu'elles sont fondées sur un ensemble de lois étatiques différentes, ces demandes ne permettent que très rarement une réparation au niveau national et ne créent pas de normes nationales que les sociétés peuvent suivre et sur lesquelles les consommateurs peuvent s'appuyer.

C. Exemples récents d'actions de groupe en matière de respect de la vie privée et de sécurité

Malgré ces défis, les avocats aux États-Unis ont continué à intenter de nombreuses actions de groupe. Ce déluge de contentieux s'explique en partie par les honoraires relativement importants que les avocats des demandeurs espèrent obtenir. De nombreuses actions de groupe liées à la protection de la vie privée ont été résolues par le biais de protocoles transactionnels rapportant peu aux consommateurs mais gros à leurs avocats.

Par exemple, dans une affaire à l'encontre de LinkedIn, 5.000 dollars ont été octroyés au demandeur principal, laissant moins d'un dollar à chacun des autres membres de l'action tandis que les avocats ont reçu plus de 321.000 dollars.

L'octroi de moins d'un dollar de dommages et intérêts au total ou même parfois de quelques centimes aux membres de l'action est probablement généreux, car certaines transactions relatives à des actions de groupe en matière de protection de la vie privée exigent uniquement des défendeurs qu'ils versent le montant des dommages et intérêts à des associations caritatives qui soutiennent des actions bénéficiant indirectement au groupe et à l'intérêt public.

Dans d'autres cas, les transactions en matière de violation de données à caractère personnel ont créé des fonds d'indemnisation ayant pour objet notamment de rembourser les membres du groupe pour les dommages dont ils peuvent justifier. Cependant, la plupart de ces transactions ne fournissent aucune indemnisation financière aux membres du groupe dont les informations personnelles ont été violées.

D. Les actions coercitives du FTC, une contribution plus efficace aux normes en matière de protection de la vie privée

Parce que de nombreuses actions de groupe sont résolues par le biais de transactions ou sont rejetées, elles n'ont pas permis d'établir des normes cohérentes et complètes en matière de respect de la vie privée. En revanche, l'action réglementaire par le biais du FTC s'est avérée être une force pour l'application de ces normes.

Le FTC a rendu de nombreuses ordonnances transactionnelles de grande importance dans des contentieux impliquant des sociétés défenderesses, qui requièrent que des changements de fond soient apportés à la politique de ces sociétés et ont établi certaines normes en matière de respect de la vie privée. Typiquement, ces ordonnances transactionnelles : I) interdisent les activités qui ont fait l'objet d'une plainte de l'agence ; II) imposent des sanctions financières ; III) exigent des sociétés qu'elles suppriment ou n'utilisent pas les données à caractère personnel indûment collectées ; IV) exigent la tenue de registres et rapports de conformité pour faciliter la mise à exécution de l'ordonnance par le FTC ; et V) exigent des sociétés qu'elles notifient au FTC tous changements importants qui pourraient avoir un impact sur leur obligation de se conformer.

Les juridictions fédérales ont confirmé l'autorité et la compétence du FTC en matière de respect de la vie privée et protection des données[185]

II. LE RGPD[186] OUVRE TIMIDEMENT LA PORTE AUX ACTIONS DE GROUPE EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN EUROPE

Plus de 15 ans après l'adoption de la Directive sur la protection de données[187], la Commission européenne a observé que le cadre juridique actuel en matière de protection des données à caractère personnel ne répondait pas de manière satisfaisante aux risques associés aux activités en ligne et nouvelles technologies[188].

185. Federal Trade Comm'n c/ Wyndham Worldwide Corp., N° 14-3514, 2015 WL 4998121 (3d Cir. 24 août 2015).

186. 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 (règlement général sur la protection des données).

187. Directive 95/46/CE 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 (la « Directive sur la protection des données »).

188. Exposé des motifs de la proposition de règlement 2012/0011 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), publiée par la Commission Européenne le 25 janvier 2012.

Dans ce contexte, le RGPD a finalement été adopté par le Parlement européen le 14 avril 2016 et est entré en vigueur en mai 2016. Il est directement applicable dans tous les États membres depuis le 25 mai 2018.

Le RGPD vise le responsable de traitement ou son sous-traitant et prévoit un ensemble de règles relatives au traitement des données à caractère personnel par lesdites entités. Il fournit également les moyens de mettre en œuvre ces dispositions. Plus particulièrement, le RGPD introduit partout en Europe des actions collectives qui peuvent être initiées par des organismes à but non lucratif dédiés à la protection des données à caractère personnel grâce à des mécanismes de consolidation.

A. Actions individuelles

1. Une action devant les juridictions nationales contre un responsable de traitement ou un sous-traitant

Sans préjudice de tout recours administratif ou extrajudiciaire qui leur est ouvert, le RGPD permet aux personnes concernées d'intenter une action à l'encontre d'un responsable de traitement ou d'un sous-traitant devant les juridictions nationales lorsqu'elles considèrent que les droits que le RGPD leur confère ont été violés du fait d'un traitement[189].

A cet égard, le RGPD offre aux personnes concernées une option de compétence leur permettant d'intenter leur action devant différentes juridictions[190]et prévoit également une exception de litispendance exigeant que les juridictions suspendent l'action ou se dessaisissent si une action identique est pendante devant une autre juridiction d'un autre État membre[191].

2. Droit à réparation et responsabilité

Le RGPD permet aux personnes concernées d'obtenir réparation du responsable de traitement ou du sous-traitant pour tout dommage matériel ou moral du fait d'une violation des droits que le RGPD leur confère devant les juridictions nationales[192].

L'aperçu ci-dessous décrit les conditions de la responsabilité telles qu'exigées par l'article 82(1) du RGPD :

• Demandeurs : toute personne ayant subi un dommage du fait d'une violation de la protection des données à caractère personnel a le droit d'obtenir réparation pour les dommages subis. Ceci s'applique en premier lieu aux personnes concernées. En outre, d'autres personnes ont également le droit de demander réparation sous certaines conditions. Cela peut être le cas si un membre de la famille de la personne concernée subit des atteintes à son intégrité psychique ou autres dommages matériels

189. Article 79, RGPD.
190. Article 79, RGPD.
191. Article 81, RGPD.
192. Articles 79 et 82 (1), RGPD.

ou moraux du fait de la violation des données à caractère personnel.

• Le défendeur : les responsables de traitement et les sous-traitants peuvent être condamnés à payer des dommages et intérêts. Cela signifie que toutes les sociétés traitant des données à caractère personnel feront face à des risques de responsabilité accrus.

• Violation fautive du RGPD : pour engager leur responsabilité civile au titre du RGPD, le responsable de traitement et le sous-traitant doivent violer les dispositions du RGPD de manière fautive. A cet égard, le RGPD prévoit un renversement de la charge de la preuve : dès lors qu'une violation est constatée, la réparation sera automatique, à moins que le responsable de traitement ou le soustraitant ne prouve qu'il n'est pas responsable du non-respect de la règlementation[193].

Le texte prévoit également le principe de la réparation intégrale des préjudices, principe très protecteur des droits des personnes concernées. Ainsi, le responsable de traitement et le sous-traitant ont l'obligation d'indemniser intégralement la personne concernée pour tous les dommages matériels et moraux. Par ailleurs, le RGPD prévoit la responsabilité solidaire : lorsque plusieurs soustraitants/responsables de traitement participent au même traitement et sont responsables d'un dommage causé par ce traitement, chacun est tenu responsable du dommage dans sa totalité[194].

Le RGPD ne prévoit pas expressément de mécanisme d'actions de groupe mais son article 80 permet que les actions soient intentées par des tiers au nom des personnes concernées et de les transformer en des demandes collectives via un mécanisme de consolidation.

B. Mécanisme de consolidation des demandes

Bien que le RGPD s'étende sur plus de 88 pages et presque 100 articles, le mécanisme tant attendu d'actions de groupe se trouve dans un seul article intitulé « Représentation des personnes concernées » [195].

En premier lieu, cet article définit le type d'entité légale qui sera en droit d'exercer les droits des personnes concernées en leur nom : les organismes ou associations dont les objectifs statutaires sont d'intérêt public et qui sont actifs dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel.

En second lieu, cet article crée trois différents types d'actions :

• une action représentative conjointe : les personnes concernées auront le droit de mandater l'entité autorisée à introduire une réclamation en leur nom et exercer les droits visés aux articles 77, 78 et 79 du RGPD ;

• une action représentative conjointe en réparation limitée : les personnes concernées auront le droit de mandater l'entité autorisée à exercer, en leur nom, leur droit à réparation uniquement si le droit de l'État membre le prévoit ;

• une action de groupe limitée : les entités autorisées auront le droit, indépendamment de tout mandat, d'introduire une réclamation et d'exercer un recours juridictionnel en cas de violation des droits des personnes concernées, à condition que l'État membre ait prévu une telle possibilité. Les demandes de réparation sont exclues de ce mécanisme.

193. Articles 82(2) et (3), RGPD.

194. Article 82 (4), RGPD.

195. Article 80, RGPD.

C. A quoi s'exposent réellement les soustraitants / responsables de traitement ?

Rien de nouveau sous le soleil ? En réalité, le RGPD ne prévoit pas de mécanisme d'action de groupe cohérent ni même un cadre procédural pour l'exercice d'une action représentative conjointe efficace. A cet égard, il n'apporte rien de nouveau et formalise simplement une pratique déjà établie dans les États membres. En France, par exemple, il est possible depuis longtemps pour une personne d'obtenir des mandats avant d'intenter une action, ce qui aboutit ainsi à une action collective. L'action représentative conjointe pourrait cependant mettre en lumière les problèmes en matière de protection des données à caractère personnel en Europe et éliminer l'obstacle habituel au développement des actions représentatives, notamment en France, que constituent l'exposition et la publicité limitées, ainsi que la difficulté d'obtenir un nombre suffisant de mandats pour que l'action collective atteigne la taille minimale. Combiné aux nouvelles méthodes de diffusion des informations liées aux actions collectives sur internet[196], l'impact médiatique du RGPD est susceptible de sensibiliser les consommateurs aux actions collectives en matière de protection des données à caractère personnel.

Enfin, le mécanisme d'action de groupe étant uniquement optionnel, sa mise en œuvre dépend de la position des États membres et peut donc être limitée.

1. Un droit européen à 28 actions collectives nationales ?

Le RGPD ne crée pas de mécanisme européen d'action de groupe mais plutôt un droit européen aux actions collectives. En effet, le RGPD dispose uniquement que la personne concernée «a le droit» d'intenter une action mais ne lui fournit pas un outil concret et laisse aux États membres le soin de fournir un tel outil.

Par conséquent, il pourrait bientôt y avoir autant d'actions collectives en matière de protection des données à caractère personnel qu'il y a d'États membres, ce qui serait contraire à l'objectif d'uniformité et de cohérence du règlement.

2. Des actions de groupe paneuropéennes et transnationales sont-elles possibles ?

Les soustraitants qui traitent des données à caractère personnel à travers le monde peuvent légitimement se demander si le RGPD pourrait donner lieu à des actions collectives multi juridictionnelles impliquant des citoyens européens et provenant d'États tiers (telle que «l'action de groupe» à l'encontre de Facebook Ireland Ltd en Autriche, qui réunit des demandeurs domiciliés dans de nombreux pays).

A cet égard, le premier problème a trait au champ d'application du RGPD : I) le RGPD ne limite pas son application aux citoyens / résidents européens[197] ; et II) bien qu'il ne

196. En Autriche par exemple, Maximilian Schrems a utilisé le site internet fbclaim.com afin d'accroître l'impact médiatique de sa démarche.

197. Article 1, RGPD

soit pas illimité, le champ d'application territorial du RGPD[198] est très large et pourrait mener à l'application du RGPD hors des frontières européennes.

La combinaison d'un large champ d'application du RGPD et de l'option de compétence qu'il fournit aux personnes concernées pourrait, en théorie, donner naissance à des actions collectives paneuropéennes en matière de protection des données à caractère personnel, qui pourraient inclure des ressortissants d'États tiers sous certaines conditions.

En tout état de cause, le système européen d'actions de groupe en matière de protection des données reste vague à ce stade. Son cadre procédural et son applicabilité devront être précisés et améliorés. A cet égard, certaines réponses pourraient venir du Comité européen de la protection des données qui a reçu pour mission de publier des lignes directrices, des recommandations et des bonnes pratiques[199].

APPLICABILITÉ DU RGPD SELON L'ORIGINE DU SOUS-TRAITANT / RESPONSABLE DE TRAITEMENT ET DE LA PERSONNE CONCERNÉE

	Sous-traitant / responsable de traitement européen (établissement principal au sein de l'UE)	Sous-traitant / responsable de traitement non-européen (établissement principal hors de l›UE) avec une filiale exerçant une activité au sein de l'UE	Sous-traitant / responsable de traitement non-européen (établissement principal hors de l›UE) avec aucune filiale exerçant une activité au sein de l'UE
Personne concernée européenne	Applicable	Applicable *	Applicable **
Personne concernée non européenne	Applicable	Applicable *	Non Applicable

* *à condition que le traitement des données à caractère personnel ait été effectué dans le contexte des activités de l'établissement situé au sein de l'UE, indépendamment du fait que le traitement ait lieu ou non au sein de l'Union*

** *à condition que l'activité de traitement soit liée à la fourniture de biens ou de services ou au suivi du comportement de la personne concernée*

198. Article 3, RGPD

199. Considérants n°77 et 124, Article 70, RGPD

III. LES QUATRE PRINCIPAUX ENSEIGNEMENTS FACE AUX ACTIONS DE GROUPE EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN EUROPE

A. Dommages et intérêts

Aux États-Unis, de nombreuses actions de groupe sont rejetées pour défaut de qualité pour agir, c'est-à-dire parce que les demandeurs ne démontrent pas avoir subi un « préjudice en fait » qui soit concret et réel ou imminent. Est-ce que la notion américaine de « préjudice en fait » s'applique aux actions de groupe en matière de protection des données à caractère personnel en Europe ?

Au titre du RGPD, les personnes concernées ont le droit d'obtenir réparation aussi bien pour les dommages matériels que moraux[200]. De fait, en cas de responsabilité, tous les dommages ayant été causés par une violation de la protection des données à caractère personnel doivent être réparés. Cette responsabilité étendue est très différente de la situation légale actuelle au titre des lois relatives à la protection des données à caractère personnel de nombreux États membres.

1. Rapide coup d'œil en France

Les actions de groupe en matière de protection des données à caractère personnel[201] peuvent être utilisées pour mettre fin à une violation des dispositions gouvernant la protection des données à caractère personnel. La loi dispose expressément que cette action de groupe ne peut donner lieu à réparation sous forme de dommages et intérêts. Il s'agit uniquement d'une forme de recours collectif par voie d'injonction. Cependant, cette position a évolué avec la loi du 20 juin 2018, qui prévoit la création d'une action de groupe en réparation en matière de protection des données à caractère personnel[202]. L'article 25, 3° dispose que cette action peut être exercée en vue soit de faire cesser un manquement aux obligations en matière de protection des données personnelles, soit d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis, soit de ces deux fins. Toutefois, la responsabilité de la personne ayant causé le dommage ne peut être engagée que si le fait générateur du dommage est postérieur au 24 mai 2018.

200. Article 82, RGPD.

201. Article 43 ter, paragraphe III de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (la « Loi Informatique et Libertés »).

202. Article 25, loi 2018-493 du 20 juin 2018 relative à la protection dès données à caractère personnel.

2. Rapide coup d'œil en Allemagne

Le 24 février 2016, une nouvelle loi allemande est entrée en vigueur ayant pour objet de renforcer les règles en matière de confidentialité des données des consommateurs[203]. Entre autres, elle a adopté le mécanisme appelé "Verbandsklage". Il s'agit d'une action représentative permettant à des entités qualifiées, par exemple des associations de défense des consommateurs, d'intenter des actions à l'encontre de sociétés et d'individus violant les lois en matière de confidentialité des données. Elle permet uniquement aux associations de réclamer la cessation du manquement (injonctions). Par conséquent, les demandes de dommages et intérêts doivent être intentées par les personnes physiques. Ce mécanisme connu sous le nom de "Verbandsklage" ne prévoit pas de réparation collective.

Le RGPD n'établit pas de critères d'évaluation du dommage indemnisable et en laisse la responsabilité aux droits nationaux applicables. De fait, les États membres disposent de leurs propres critères nationaux pour déterminer si les demandeurs ont qualité pour agir et si un préjudice hypothétique, futur ou même d'anxiété peut être indemnisable.

L'article 82 du RGPD a pour objectif d'être dissuasif, rendant les violations de la protection des données à caractère personnel peu attrayantes d'un point de vue financier. En particulier, la jurisprudence de la Cour de justice de l'Union européenne concernant les préjudices moraux doit être prise en compte. Selon la jurisprudence, le montant alloué doit avoir un effet dissuasif. Cet objectif peut uniquement être atteint si le montant des dommages et intérêts alloués atteint un niveau suffisamment élevé.

B. Charge de la preuve

Au titre du RGPD, le responsable de traitement doit s'assurer et démontrer que ses activités de traitement sont conformes aux dispositions du RGPD ainsi qu'aux lois des États membres prises en application dudit règlement. Le responsable de traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD[204].

Le responsable de traitement doit tenir un registre par écrit, y compris sous forme électronique, des activités de traitement effectuées et mettre le registre à la disposition de l'autorité de contrôle sur demande[205].

Le responsable de traitement doit enregistrer et documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. Cette documentation doit être transmise à l'autorité de contrôle sur demande[206].

Le RGPD impose un régime strict de responsabilité aux responsables de traitement : dès lors qu'une violation est constatée, sa réparation sera automatique. Les personnes concernées peuvent intenter une action sans avoir à prouver une faute ou une négligence de la part du responsable de traitement. La charge

203. Loi pour une meilleure application des dispositions visant à protéger les consommateurs de la loi sur la confidentialité des données du 17 février 2016, BGBl I 2016, 233.

204. Article 24, RGPD.

205. Article 30, RGPD.

206. Article 33, RGPD.

de la preuve que « le fait qui a provoqué le dommage ne lui est nullement imputable » (à savoir que le traitement de données à caractère personnel est réalisé conformément au RGPD et aux droits nationaux transposant le RGPD) pèse sur le responsable de traitement défendeur[207].

Les responsables de traitement doivent répondre aux nouvelles exigences en matière de protection des données à caractère personnel et être en mesure de démontrer que le traitement de ces données est réalisé conformément au RGPD et aux lois des États membres. De fait, il est extrêmement important que le responsable de traitement tienne un registre et conserve la preuve de toutes les mesures, actions et éléments susceptibles de démontrer qu'il a respecté le RGPD.

Les responsables de traitement doivent considérer la logique de responsabilisation du RGPD comme une stratégie précontentieuse, conçue pour créer des documents permettant de démontrer que le défendeur a appliqué les mesures techniques et organisationnelles appropriées.

C. Territorialité

Le champ d'application territorial étendu du RGPD et l'option de compétence qu'il fournit aux personnes concernées pourrait donner lieu à des cas de *forum shopping* et à des actions collectives multi-juridictionnelles impliquant des personnes concernées européennes et non européennes.

Le RGPD s'applique : aux entreprises établies sur le territoire de l'UE et qui traitent des données à caractère personnel[208] ; ainsi qu' aux entreprises qui sont établies hors de l'UE si elles traitent les données à caractère personnel de résidents européens dans le cadre de la fourniture de biens ou de services ou du suivi du comportement des résidents européens (dans la mesure où ledit comportement a lieu au sein de l'UE)[209].

Les entreprises qui n'étaient pas soumises à la Directive sur la protection des données pourraient être soumises au RGPD si elles offrent des biens ou des services aux résidents européens ou suivent leur comportement.

Une action contre un responsable de traitement ou un sous-traitant peut être intentée par la personne concernée devant : I) les juridictions de l'État membre dans lequel le responsable de traitement ou le sous-traitant a son établissement ; ou II) les juridictions de l'État membre dans lequel la personne concernée réside[210].

L'option de compétence peut inciter les personnes concernées à intenter des actions individuelles et des actions de groupe dans un État membre spécifique pour bénéficier des différences des droits nationaux (par exemple, le préjudice en fait, les actions en réparation, la réparation de préjudices matériels et moraux).

207. Article 82, RGPD.
208. Article 3 (1), RGPD.
209. Article 3 (2), RGPD.
210. Article 79 (2), RGPD.

Rapide coup d'œil en Autriche

Le 1er août 2014, un étudiant en droit autrichien, Maximilian Schrems, a intenté un procès contre Facebook Ireland Ltd devant le tribunal de Vienne alléguant que les pratiques de Facebook violeraient les lois relatives au respect de la vie privée de nombreuses manières. Afin d'intenter une « action de groupe », Maximilian Schrems a créé un site internet invitant toute personne ayant subi les mêmes prétendues violations de leurs droits à rejoindre l'action. Le 12 septembre 2016, la Cour Suprême autrichienne a posé deux questions préjudicielles à la Cour de justice de l'Union européenne. Le 25 janvier 2018, (affaire C-498/16), la CJUE a jugé que l'article 16(1) du règlement 44/2001 « doit être interprété en ce sens qu'il ne s'applique pas à l'action d'un consommateur visant à faire valoir, devant le tribunal du lieu où il est domicilié, non seulement ses propres droits, mais également des droits cédés par d'autres consommateurs domiciliés dans le même État membre, dans d'autres États membres ou dans des États tiers ». La CJUE a expliqué que l'exclusion des droits cédés est nécessaire pour que les règles de compétence présentent un haut degré de prévisibilité, ce qui constitue l'un des objectifs du RGPD.

D. Procédure de *discovery*

Le RGPD ne crée pas de procédure de *discovery* précontentieuse. Cependant, il prévoit certaines dispositions exigeant que les responsables de traitement communiquent les preuves qu'ils respectent le RGPD. Ceci peut permettre aux personnes concernées de monter leur dossier avant de déposer une demande.

Le RGPD donne aux personnes concernée un droit général d'accès à leurs propres données à caractère personnel par le biais d'une demande de droit d'accès[211]. Le responsable de traitement doit répondre à la demande de droit d'accès dans un délai d'un mois à compter de la réception de la demande[212] et transmettre à la personne concernée une copie de toutes les données à caractère personnel que celle-ci lui a fournies.

Le RGPD développe les catégories obligatoires d'informations qui doivent être fournies en lien avec la demande de droit d'accès (par exemple les informations sur les finalités du traitement, les catégories de données traitées, la durée de conservation des données envisagée)[213]. Ceci permet aux personnes concernées de vérifier la légitimité du traitement de leurs données à caractère personnel.

Le responsable de traitement peut refuser de donner suite à la demande de droit d'accès d'une personne concernée si celle-ci est manifestement infondée ou excessive, mais il devra apporter la preuve que tel est le cas[214].

Les sociétés devraient être préparées à ce que les personnes concernées exercent leur droit d'introduire une réclamation auprès d'une autorité de contrôle pour avoir accès aux conclusions d'une enquête administrative[215]. Il est probable que les personnes concernées utiliseront ces informations dans le cadre de procédures civiles.

Du fait de cette approche, les personnes concernées peuvent facilement créer une pré-

211. Article 15, RGPD.
212. Article 12, RGPD.
213. Article 13, RGPD.
214. Article 12, RGPD.
215. Article 77, RGPD.

somption de violation de la protection des données à caractère personnel entrainant une charge de la preuve encore plus lourde pèse sur les responsables de traitement.

Les sociétés doivent être en mesure de démontrer que le traitement est effectué conformément au RGPD[216]. Cette preuve doit faire référence aux efforts généraux que font les sociétés pour mettre le RGPD en œuvre conformément à la loi. En outre, la société doit apporter la preuve des mesures que la société a prises à l'égard du demandeur en question. A cette fin, les sociétés devraient établir un système de consignation des opérations de traitement individuel pour être en mesure de prouver qui a eu accès aux données à caractère personnel d'un individu donné et quelles actions ont été prises à l'égard de ses données.

Conclusion

Du fait de la diversité des règles procédurales au sein des États membres de l'Union européenne et du champ d'application territorial étendu du RGPD, nous pouvons nous attendre à ce que les demandeurs recourent au forum shopping afin de trouver les juridictions nationales les plus favorables pour initier des actions de groupe en matière de protection des données à caractère personnel.

Les dispositions de responsabilisation du RGPD exigent des défendeurs qu'ils prouvent qu'ils ont mis en œuvre les « mesures techniques et organisationnelles appropriées ». Les registres de traitement de données à caractère personnel devraient être conçus dans un esprit de stratégie précontentieuse.

Les demandeurs pourront utiliser les demandes de droit d'accès aux données et les réclamations auprès des autorités de contrôle pour constituer un dossier de contentieux.

216. Article 24, RGPD.

DROIT À LA PORTABILITÉ DES DONNÉES À CARACTÈRE PERSONNEL

Hajar MALEKIAN,
Docteur en droit, université Paris II Panthéon-Assas,
Titulaire d'une maitrise en génie informatique,
Étudiante « Promotion DU *Data Protection Officer* Paris II – 2017 ».

Le droit à la portabilité est le nouveau droit introduit au sein du règlement général sur la protection des données à caractère personnel (ci-après le « RGPD »)[217]. Il s'agit de l'une des innovations majeures du RGPD en termes de droits des individus qui implique des évolutions substantielles notamment dans les métiers de la banque et de l'assurance[218] ainsi que dans ceux des opérateurs de téléphonie mobile. Les personnes concernées ont ainsi le droit de « recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine, et le droit de transmettre ces données à un autre responsable de traitement sans que le responsable de traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle »[219]. À titre d'exemple, lorsqu'un utilisateur a utilisé pendant des années un compte email, lors du changement de prestataire de messagerie, il lui serait difficile, sans l'existence du droit à la portabilité, d'avoir accès à l'historique de ses emails à travers le nouveau prestataire d'email. À cet égard, comme il a été remarqué dans les contributions en ligne du public concernant le projet de loi pour la République numérique, « la perspective de perdre ses données ou de devoir se lancer dans une fastidieuse récupération manuelle de celles-ci peut en effet inciter l'utilisateur à renoncer à changer d'opérateur, quand bien même il ne serait plus satisfait de ses services. Ce droit à la portabilité permettra de lever cette barrière et d'améliorer ainsi le fonctionnement du marché tout en offrant à l'utilisateur (particulier ou professionnel) une mobilité numérique accrue »[220].

L'objectif du droit à la portabilité est double. L'objectif premier est de faciliter la libre circulation des données[221] par une transmission directe[222] des données d'un responsable de traitement à un autre. Cette libre circulation est en faveur de l'intérêt économique du responsable de traitement destinataire des données. Cela permet d'équilibrer le rapport de concurrence entre différents fournisseurs de service dans le cadre du marché unique numérique[223], notamment en faveur des fournisseurs émer-

217. 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 (règlement général sur la protection des données).

218. Rapport du CGREF, *Entreprise : clé d'application réussite du GDPR*, http ://www.cigref.fr/entreprise-cle-application-reussie-gdpr-livrable-cigref-afai-tech-in-France.

219. Article 20 (1), RGPD.

220. Contribution en ligne concernant le projet de loi « pour la République numérique », https ://www.republique-numerique.fr/.

221. Groupe de l'Article 29, WP 242, Guide sur *le droit à la portabilité*, 13 décembre 2016, *op. cit.,* p. 4.

222. Article 20 (2) et Considérant 68, RGPD, sous réserve que cette transmission soit techniquement possible.

223. Groupe de l'Article 29, WP 242, Guide *sur le droit à la portabilité*, *op. cit.,* p. 3.

gents. Le deuxième objectif est de fournir à la personne concernée plus de contrôle[224] sur ses données à caractère personnel (ci-après « DCP ») lorsqu'elle a consenti à ce que ses DCP fassent l'objet d'un traitement, ou lorsqu'elle est l'utilisateur d'un service en ligne. Dans ce dernier cas, la personne concernée (le demandeur), exerce également plus de contrôle sur son choix de service en tant qu'utilisateur. Ainsi, ce droit à la portabilité tout en renforçant le droit à l'autodétermination informationnelle au niveau européen promeut la libre circulation des DCP sous contrôle de la personne concernée. Le droit à la portabilité peut ainsi être considéré comme un nouveau mécanisme allant dans le sens d'un équilibre entre la libre circulation et la protection des DCP en facilitant un partage sécurisé des données.

I. CADRE JURIDIQUE

A. Condition d'application du droit à la portabilité

Le droit à la portabilité s'exerce sur les DCP qui font l'objet d'un traitement automatisé[225]. En outre, selon l'article 20 (1) du RGPD, le droit à la portabilité peut être exercé par la personne concernée uniquement lorsque la condition de licéité du traitement initial est fondée sur son consentement[226]ou sur un contrat-[227]dont elle est la partie contractante. Ce droit « ne devrait pas s'appliquer lorsque le traitement est fondé sur un motif légal autre que le consentement ou l'exécution d'un contrat »[228]. En outre, le traitement doit être effectué à l'aide de procédés automatisés[229].

Pour les besoins de l'exercice du droit à la portabilité par la personne concernée, les responsables du traitement peuvent adopter certaines bonnes pratiques. Selon le guide du G29 sur le droit à la portabilité, ils peuvent commencer à mettre en place des infrastructures techniques et pratiques comme des interfaces permettant l'exercice du droit à la portabilité[230]. L'exercice de ce droit doit pouvoir être assuré le plus rapidement possible, sans jamais excéder deux mois tout en respectant l'exigence en matière de la vérification de l'identité des demandeurs[231]. Les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais[232]. Il convient de s'assurer que l'identité des demandeurs et que la légitimité de la portabilité demandée soient vérifiées.

Pour bien assurer la transmission des données, le format des données joue un rôle important. Les responsables de traitement

224. *Idem*., considérant 68 du RGPD.
225. Considérant 68, RGPD.
226. Article 6(1) (*a*), article 9(2) (*a*), RGPD.
227. Article 6(1) (*b*), RGPD.
228. Considérant 68, RGPD.
229. Article 20(1) (b), RGPD.
230. API (*application programming interfaces),* G29, WP 242, *Guide sur le droit à la portabilité,* 13 décembre 2016, *op. cit.,* p. 3.
231. Rapport du CGREF, « Entreprise : clé d'application réussite du GDPR », http ://www.cigref.fr/entreprise-cle-application-reussie-gdpr-livrable-cigref-afai-tech-in-france, p. 59.
232. *Idem*.

sont tenus de prévoir des mesures nécessaires pour un format structuré, couramment utilisé et lisible par machine[233]. « Il y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données »[234]. En outre, la personne concernée doit être informée de l'existence de ce droit, tant lorsque les données sont directement[235] collectées auprès d'elle que lorsque ce n'est pas le cas[236]. Selon l'article 20 (2) du RGPD, la personne concernée a le « droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable de traitement à un autre, lorsque cela est techniquement possible »[237]. Le format a un rôle important dans la réutilisation des données à la fois par les autres responsables de traitement et pour la personne concernée. Le format le plus approprié peut ainsi différer selon les secteurs d'activité. Selon la CNIL, « sur des jeux de données plus spécifiques, où il n'existe pas de standard de fait pour leur fourniture, les organismes peuvent fournir les données personnelles dans un format ouvert (XML, JSON, CSV, etc.), complété par toute métadonnée utile à leur interprétation, et documenté »[238]. Selon l'avis du G29, les acteurs de l'industrie et les associations professionnelles peuvent travailler sur un ensemble de standards et formats interopérables pour respecter ces pré requis du droit à la portabilité. Concernant le format, un haut niveau d'abstraction s'avère nécessaire. En outre, les métadonnées doivent être les plus précises possibles[239]. Selon le G29, « lorsque les données collectées auprès du consommateur ne peuvent pas être récupérées dans un standard ouvert et aisément réutilisable, le fournisseur de service de communication au public en ligne en informe le consommateur de façon claire et transparente. Le cas échéant, il l'informe des modalités alternatives de récupération de ces données et précise les caractéristiques techniques du format du fichier de récupération, notamment son caractère ouvert et interopérable ».

233. Article 20 (1), RGPD.
234. Considérant 68, RGPD.
235. Article 13 (2) (b), RGPD.
236. Article 14 (2) (c), RGPD. Il s'agit du cas où les données sont obtenues indirectement auprès de la personne concernée.
237. Article 20 (2), RGPD.
238. https ://www.cnil.fr/fr/le-droit-la-portabilite-en-questions.
239. http ://blog.businessdecision.com/bigdata/2017/04/gdpr-droit-portabilite-des-donnees.

B. Portée et limite du droit à la portabilité : un droit non-absolu.

1. Interprétation du terme « fourni »

Différentes questions se posent quant à la portée du concept « fournies par la personne concernée » : est-ce que ces données comprennent aussi les données collectées de manière automatique ? Qu'en est-il des données issues de traitements complémentaires donnant une valeur ajoutée aux données? Les lignes directrices du G29 sur le droit à la portabilité répondent à la première question par l'affirmative, et par la négative à la deuxième question. Selon ces lignes directrices, compte tenu des objectifs politiques[240] liés au droit à la portabilité des données, l'expression « fournies par la personne concernée » doit être interprétée de manière large et exclure uniquement les « données inférées » et les « données dérivées ». Ces données comprennent les DCP générées par l'activité de la personne concernée à travers un fournisseur de services (responsable de traitement). Un exemple selon le G29 vise des résultats à l'issue des algorithmes de traitement des données.

Ainsi, il est expressément précisé dans les lignes directrices du G29 sur le droit à la portabilité que les données dérivées et les données inférées sont exclues du champ d'application du droit à la portabilité par le fait qu'elles ne sont pas fournies par la personne concernée, et qu'elles sont le résultat d'analyses complémentaires faites par le responsable de traitement (ex. le crédit, l'état de santé). Ces exemples concernent le profilage défini comme l'évaluation des aspects de la vie de la personne concernée. Ainsi, les données fournies peuvent comprendre les DCP relatives à l'activité de la personne concernée, ou celles résultant de l'observation du comportement d'un individu lors de l'utilisation d'un service en ligne[241]. À titre d'exemple, nous pouvons citer l'historique des transactions ou Access log.

L'exercice de ce droit à la portabilité n'a aucune incidence sur les principes relatifs au traitement des DCP. Selon l'article 20 (3) du RGPD, « l'exercice du droit, visé au paragraphe 1 du présent article s'entend sans préjudice de l'article 17. Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ». Une condition importante visée par l'article 20 (4) du RGPD est que le droit à la portabilité ne doit pas porter atteinte aux droits et libertés de tiers. En outre, ce droit ne porte pas atteinte à l'exercice des autres droits de la personne concernée. Le nouveau responsable de traitement destinataire des données est tenu de procéder au traitement des données a priori pour la même finalité qu'initialement prévu, sauf si la personne concernée a consenti à d'autres finalités.

240. *Policy objectives*.

241. G29, WP 242, *Guide sur le droit à la portabilité*, 13 décembre 2016, *op. cit.*, p. 8-9.

2. Quel lien avec le droit d'accès aux données ?

Le droit à la portabilité est en lien étroit avec le droit d'accès de la personne concernée à ses DCP[242]. Comme nous l'avons constaté ci-dessus, alors que dans le cadre du droit d'accès, la personne concernée peut avoir accès à toutes ses DCP y compris celles dites dérivées, l'accès aux données dans le cadre du droit à la portabilité, en vertu du RGPD, se limite aux données fournies par la personne concernée, et cela lorsque les conditions de licéité du traitement se bornent juste au consentement de la personne concernée et au traitement dans le cadre d'un contrat dont la personne concernée constitue l'une des parties contractante. Cependant, le droit à la portabilité reste plus exigeant en matière du format des données fournies à la personne concernée. Ainsi, ces deux droits restent complémentaires.

II. ENJEUX CONCERNANT L'APPLICATION DU DROIT À LA PORTABILITÉ.

A. Droit des tiers

L'application du droit à la portabilité peut avoir des effets indésirables notamment sur des tiers[243]. Les données faisant l'objet de l'exercice du droit à la portabilité peuvent comprendre des données de tiers. Cela concerne notamment les données de communication que ce soit par le service de messagerie ou de téléphone, données de transactions bancaires, etc. Dans ce cas, se pose la question concernant le droit des tiers. Certes, la présence des données de tiers ne peut pas justifier un rejet de la demande. Néanmoins, ces données de tiers doivent faire l'objet d'une protection spécifique. A défaut, cela engendrerait un climat d'insécurité et de manque de contrôle de ses données, ressenti par le tiers concerné dans le cadre d'une demande de communication. Selon le guide du G29 sur le droit à la portabilité, et afin de prévenir le risque sur les tiers, le nouveau responsable de traitement ne doit traiter ces données que dans la mesure où elles sont gardées sous le seul contrôle de la personne concernée à l'origine de la demande de portabilité, et qu'elles ne soient gérées que pour des besoins purement personnels. Ainsi, le nouveau responsable de traitement ne peut utiliser ces données pour d'autres finalités, comme la publicité ciblée. Un tel traitement serait susceptible d'être considéré comme illégal et injuste, en particulier si les tiers concernés ne sont pas informés et ne peuvent exercer leurs droits en tant que personnes concernées[244]. Il est préconisé par ce guide sur la portabilité que tous les responsables de traitement (les parties « expéditrice » et « réceptrice ») devront mettre en place des outils permettant aux personnes concernées de sélectionner les données pertinentes. En outre, ils devraient mettre en œuvre des mécanismes de consentement pour d'autres personnes concernées, afin de faciliter la transmission des données dans les cas où ces parties sont disposées à consentir[245].

242. *Ibid.*, p. 3.

243. *Ibid.*, p. 10.

244. *Ibid.*

245. *Ibid.*

À cet égard, selon le guide du G29, le responsable de traitement destinataire des données doit faire en sorte que les données reçues soient en conformité avec les principes concernant le traitement des DCP, notamment, à ce que les données soient pertinentes et non excessives à l'égard du nouveau traitement en cours[246]. Selon le RGPD, « ce droit ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles »[247] mais interopérables.

B. Articulation avec les dispositions françaises.

En droit français, l'article L.224-42-1 à L.224-42-4 du Code de la consommation concerne le droit à la portabilité. À cet égard, « le consommateur dispose en toutes circonstances d'un droit de récupération de l'ensemble de ses données »[248] auprès des fournisseurs d'un service de communication au public en ligne. « Cette récupération s'exerce conformément aux conditions prévues à l'article 20 du RGPD »[249]. Selon l'article L224-42-3, « sans préjudice des dispositions protégeant le secret en matière commerciale et industrielle et des droits de propriété intellectuelle, tout fournisseur d'un service de communication au public en ligne propose au consommateur une fonctionnalité gratuite permettant la récupération : 1° De tous les fichiers mis en ligne par le consommateur ; 2° De toutes les données résultant de l'utilisation du compte d'utilisateur du consommateur et consultables en ligne par celui-ci, à l'exception de celles ayant fait l'objet d'un enrichissement significatif par le fournisseur en cause. Ces données sont récupérées dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé ; 3° D'autres données associées au compte utilisateur du consommateur et répondant aux conditions suivantes : a) Ces données facilitent le changement de fournisseur de service ou permettent d'accéder à d'autres services ; b) L'identification des données prend en compte l'importance économique des services concernés, l'intensité de la concurrence entre les fournisseurs, l'utilité pour le consommateur, la fréquence et les enjeux financiers de l'usage de ces services »[250]. Une consultation publique sur les modalités de mise en œuvre de cette mesure a été lancée avec les différents acteurs économiques. Le décret attendu sur la portabilité des données clarifierait l'articulation entre l'article L.224-42-1 à L.224-42-4 du Code de la consommation qui dépasse le simple cadre des DCP[251] et la disposition du règlement.

246. G29, WP 242, *Guide sur le droit à la portabilité*, 13 décembre 2016, *op. cit*.

247. Considérant 68, RGPD.

248. Article L.224 (42) (1), Code de la consommation, https ://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069565.

249. *Ibid*.

250. Article L.224 (42) (3), Code de la consommation, https ://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069565.

251. Cette disposition prend en compte de « tous les fichiers mis en ligne par le consommateur » et « toutes les données résultant de l'utilisation du compte utilisateur du consommateur ».

Conclusion

Comme nous l'avons déjà indiqué, le droit à la portabilité tel qu'introduit dans le RGPD est un droit à double intérêt. Il présente un bénéfice à la fois pour les personnes concernées et à la fois pour le développement de l'économie numérique (la personne concernée peut récupérer une partie de ses données grâce au droit à la portabilité). Il permet également plus de contrôle à la personne concernée sur ses DCP, ainsi que la possibilité qu'elle puisse bénéficier à tout moment d'un meilleur service. En effet, ce droit conforte, pour la personne concernée, la possibilité de son libre choix du responsable de traitement en fonction des critères qu'elle souhaite mettre en avant tels que la qualité, la confidentialité, le coût de service. Ce droit contribue également au développement de l'économie numérique dans un cadre de concurrence loyale via la libre circulation, et en quelques sortes, une décentralisation des données, ce qui donne lieu à plus de concurrence entre les fournisseurs de service. C'est ainsi que ce droit présente globalement une occasion de réinstaurer l'équilibre dans le rapport existant entre la personne concernée et le responsable de traitement[252]. Cependant, un certain nombre de questions se pose lors de l'application de ce droit notamment quant au format des données, au droit des tiers, ainsi qu'à l'articulation avec la disposition française introduite dans le code de la consommation.

252. G29, WP 242, *Guide sur le droit à la portabilité,* 13 décembre 2016,op. cit., p. 4.

PROTECTION DES DONNÉES PERSONNELLES : QUAND LE DROIT DE LA CONCURRENCE S'EN MÊLE...

Rachel BOGE KNITTEL,
Juriste Conformité Données Personnelles, Imprimerie Nationale SA
-
Nathalie LANERET,
Group DPO, Capgemini, Enseignant DU DPO Panthéon Assas

La mise en conformité avec la réglementation applicable à la protection des données personnelles[253] est un sujet prioritaire pour toutes les entreprises. Celles dont le cœur de métier consiste dans le traitement de données personnelles, mais aussi plus généralement du fait de la digitalisation croissante de toutes les fonctions de l'entreprise qui mènent à une collecte toujours plus importante de données sur les clients, prospects, salariés, candidats, visiteurs ou utilisateurs.

Au-delà de ces évolutions réglementaires, les phénomènes de collecte massive de données personnelles dans tous les secteurs d'activité, la reconnaissance de leur valeur économique et de l'avantage concurrentiel qu'elles peuvent procurer à son détenteur pourraient obliger certaines entreprises à intégrer, en sus de la définition de la base légale du traitement[254] , des modalités de l'information de l'individu[255] ou des analyses d'impact sur la vie privée[256], une analyse économique afin de vérifier que les effets du traitement des données personnelles n'entrent pas en contradiction avec le droit de la concurrence, « invité surprise » dans ce domaine.

Cette analyse apparaît en premier lieu inappropriée : les données personnelles, dont la protection relève d'un droit fondamental[257] ne sont pas un bien commercialisable et ne peuvent donc faire l'objet d'une analyse économique. En second lieu, les objectifs respectifs du droit de la concurrence (protéger la concurrence sur le marché) et du droit de la protection des données personnelles (protéger le traitement des données personnelles de l'individu de façon à protéger les droits et libertés fondamentaux) sont clairement différents.

Néanmoins, on voit poindre un début de rapprochement de ces deux domaines dans le règlement général sur la protection des données (RGPD) lui-même qui définit les infractions à la réglementation sur la protection des données

253. 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 (règlement général sur la protection des données) – JOCE du 4 mai 2016 – L119/1, dit « RGPD » ; Proposition de Règlement du Parlement Européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE - COM(2017) 10 final 2017/0003 (COD).

254. Article 6 du RGPD sur les conditions de la licéité du traitement.

255. Articles 13 et 14 du RGPD sur l'information des personnes.

256. Articles 35 et 36 du RGPD sur les analyses d'impact relatives à la protection des données.

257. Article 8 de la Charte des droits fondamentaux de l'Union Européenne – JOCE du 26 Octobre 2012 - C 326/391.

personnelles en pourcentage du chiffre d'affaires du contrevenant afin de créer une corrélation entre la sanction et le gain indûment généré suite à une infraction à la réglementation, ce qui s'inscrit dans la logique suivie depuis longtemps par le droit de la concurrence[258].

Il est dès lors pertinent d'analyser les points de recoupement entre protection des données personnelles et droit de la concurrence. N'y-a-t-il pas des situations dans lesquelles, même si l'entreprise traite des données personnelles et les réutilise en stricte conformité avec les conditions prévues par la réglementation sur la protection des données personnelles, le droit de la concurrence pourra l'empêcher de procéder en ce sens ?

L'objectif de cet article est de mettre en évidence les situations dans lesquelles les entreprises devront, au-delà de la simple question de conformité de leurs pratiques à la réglementation sur la protection des données personnelles, également intégrer l'analyse économique permettant d'identifier les risques d'infraction de leurs pratiques au droit de la concurrence. Cette interaction se situe à deux niveaux : tout d'abord, sur la façon dont l'accumulation, la détention et le traitement de données personnelles peuvent contribuer au « pouvoir de marché » de l'entreprise, critère central dans toute analyse de concurrence (I) et ensuite comment le traitement des données personnelles en tant que tel peut potentiellement – sur la base de ce pouvoir de marché - constituer une infraction au droit de la concurrence (II).

I. LE TRAITEMENT DES DONNÉES PERSONNELLES, FACTEUR DE POUVOIR DE MARCHÉ

L'accumulation et le traitement intensif de grandes quantités de données personnelles ne constituent pas en tant que tels des infractions au droit de la concurrence[259]. Néanmoins, ils peuvent avoir une incidence importante puisque celles-ci sont susceptibles d'avoir un impact sur le pouvoir de marché de l'entreprise et donc d'influer sur le caractère concurrentiel du marché. Ces pratiques sont susceptibles de concerner potentiellement tous les marchés (A) avec des problématiques spécifiques dans le secteur numérique (B).

A. La détention de la donnée comme facteur de pouvoir de marché

Le pouvoir de marché d'une entreprise définit sa latitude à fixer les prix de vente sur un marché donné au-dessus de ses coûts de production sans tenir compte de ses concurrents. Cette détermination comprend plusieurs éléments dont l'analyse du nombre de concurrents, la disponibilité de produits substituables ou encore l'existence de barrières à l'entrée.

258. Le droit de la protection personnelles vient également au secours du droit de la concurrence en imposant un droit à la portabilité (voir l'article 20 du RGPD) des individus sur leurs données personnelles leur permettant de changer plus facilement de prestataire de service, ce qui va favoriser la concurrence entre ces derniers.

259. L'accumulation et le traitement intensif de grandes quantités de données personnelles ne constituent pas non plus en tant que tels une infraction au droit de la protection des données personnelles, lequel ne fixant aucune limite quantitative. Seuls les traitements « à grande échelle » pourront générer le respect d'obligations spécifiques, comme l'obligation de nommer un DPO ou la réalisation d'une analyse d'impact.

Transposée au secteur de la donnée, cette analyse couvre également l'existence de facteurs spécifiques tels que la non-réplicabilité des bases de données personnelles, l'accès à un large volume de données ou à une importante variété de données qui peut constituer un véritable facteur de compétitivité sur le marché.

Ainsi, les ressources à mettre en œuvre pour collecter ces données peuvent constituer une barrière à l'entrée d'un marché, si certains opérateurs ne sont pas en mesure de collecter ou d'acheter le même type de données, en termes de volume et/ou de variété que les entreprises déjà en place, tel que cela a pu être sanctionné par l'Autorité de la concurrence[260]. Cela a pour effet d'accroître le pouvoir de marché de l'entreprise qui en est détentrice.

Ce pouvoir de marché est préjudiciable au consommateur puisqu'il limite son choix tout en ayant pour effet d'augmenter les prix[261].

Bien que chaque entreprise peut en théorie acquérir des données (auprès de tierces parties) et rattraper l'avantage des entreprises déjà établies, en pratique cela s'avère impossible au regard de la quantité et de la qualité des données détenues par ces entreprises déjà en place, lorsqu'elles disposent d'une base clientèle et d'informations tellement large que la question se pose de savoir si un nouvel acteur est en mesure de reproduire le même volume et la même qualité de données.

Cette situation est courante pour les entreprises ayant une partie de leurs activités en situation de monopole et qui souhaitent développer des activités concurrentielles : elles se voient obligées de justifier que l'utilisation des données ne résulte pas du monopole et que les concurrents demeurent en mesure d'atteindre les clients potentiels[262].

Cette notion de pouvoir de marché explique par ailleurs que certaines analyses au titre du contrôle des concentrations intègrent une analyse sur les effets sur le marché de la détention de données personnelles dans le cas où l'acquisition pourrait résulter dans une concentration des données personnelles dans les mains d'une seule entreprise conduisant à enrichir une base de données ou offrant des possibilités de croisement et de combinaison uniques, inaccessible aux concurrents de l'entreprise[263].

260. Décision de l'Autorité de la Concurrence n°09-D-24 du 28 juillet 2009 « France Telecom » : sanction de 27,6 millions d'euros d'amende pour mise en œuvre un ensemble de comportements dont le but était d'affaiblir ses principaux concurrents en élevant leurs coûts de pénétration du marché. « *France Télécom a utilisé sa position dominante résultant notamment de son ancien monopole pour s'octroyer, de manière* déloyale, des avantages sur ses concurrents ». Décision de l'Autorité de la Concurrence n°12-D-25 du 18 décembre 2012 « SNCF » : sanction de 60,7 millions d'euros d'amende pour abus de position dominante résultant de l'utilisation à des fins commerciales par la SNCF d'informations confidentielles obtenues dans le cadre de sa mission publique de gestion des infrastructures et de la mise en œuvre d'obstacles à l'accès des concurrents aux capacités ferroviaires. « *Cette pratique, qui ne relève pas d'une concurrence par les mérites, a entravé artificiellement le développement de ses concurrents et porté atteinte au fonctionnement concurrentiel du secteur* ». Décision de l'Autorité de la Concurrence n° 14-D-06 du 8 juillet 2014 « Cegedim » : sanction de 5.7 millions d'euros d'amende pour abus de position dominante résultant du refus discriminatoire et abusif de vendre d'une base de données commerciale à un concurrent. L'Autorité de la concurrence a retenu que « *Cegedim a abusé de sa position dominante en raison de son refus de vendre sa base de données OneKey aux laboratoires recourant au logiciel commercialisé par Euris (son concurrent direct), alors qu'elle acceptait de la vendre à des entreprises ayant recours à des logiciels d'éditeurs tiers* ».

261. Voir avis 10-A-13 du 14 juin 2010 de l'autorité de la concurrence relatif à l'utilisation croisée de bases de données de clientèle.

262. Arrêté du 4 juillet 2013 autorisant la mise en œuvre par les collectivités territoriales, les établissements publics de coopération intercommunale, les syndicats mixtes, les établissements publics locaux qui leur sont rattachés ainsi que les groupements d'intérêt public et les sociétés publiques locales dont ils sont membres de traitements automatisés de données à caractère personnel ayant pour objet la mise à disposition des usagers d'un ou de plusieurs téléservices de l'administration électronique https ://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027697207.

263. A noter qu'à ce jour aucune acquisition en Europe n'a été remise en cause spécifiquement sur ce point, seul le risque a été relevé par les autorités qui ont privilégié les effets positifs sur le marché de l'acquisition.

En dépit du fait que les utilisateurs et l'efficacité économique bénéficient des gains de productivité associés au développement de la collecte des données et des usages possibles, l'accroissement des barrières à l'entrée du marché pour les nouveaux entrants et la réduction de concurrence qui en résulte, s'avèrent préjudiciables pour l'économie et le principe de libre concurrence, faisant converger les marchés liés aux données personnelles vers une situation de monopole.

B. Pouvoir de marché et problématiques spécifiques dans le secteur des services numériques

Ces problématiques se rencontrent en particulier sur le marché des prestations de service en ligne (publicité ciblée, moteur de recherche, plateforme, réseau social) dont le business model repose sur le traitement de données personnelles en permettant à la fois de proposer des services gratuits[264]adaptés aux besoins des utilisateurs et en utilisant des données personnelles dans le cadre de publicités ciblées permettant aux annonceurs de financer le service en ligne concerné[265].

Dans le secteur du numérique, les effets de réseau (réseaux de télécommunication ou réseaux sociaux) amplifient la problématique. Ceux-ci se manifestent par le fait que l'utilisation d'un service par un utilisateur impacte la valeur de ce service pour les autres utilisateurs. Autrement dit, plus il y a d'utilisateurs, plus le service est pertinent, ce qui a pour effet de restreindre la concurrence.

La détention des données personnelles participe au poids économique de l'entreprise qui n'est plus seulement définie en termes de chiffre d'affaires, mais également au regard de son accès aux données. La détention de données personnelles peut permettre à une entreprise d'acquérir un pouvoir de marché, qui n'est pas illicite en tant que tel, tout comme ne l'est pas le traitement de grandes quantités de données personnelles, toutefois à la condition qu'il soit opéré en conformité avec la réglementation applicable. Il devient illicite lorsqu'il est couplé à un comportement impliquant les données personnelles qui fait franchir la ligne de la légalité, l' « abus » et qui convertit le pouvoir de marché en abus de position dominante.

264. On peut se demander si les services sont véritablement gratuits et si l'utilisateur ne revient pas en fait à payer les services avec ses données Personnelles.

265. Décision n° 16-SOA-02 du 23 mai 2016 relative à une saisine d'office pour avis portant sur l'exploitation des données dans le secteur de la publicité en ligne. http ://www.autoritedelaconcurrence.fr/user/avisdec.php?numero=16SOA02.

II. LE TRAITEMENT DES DONNÉES PERSONNELLES, INFRACTION AU DROIT DE LA CONCURRENCE

Le traitement de données personnelles peut également potentiellement passer sous les fourches caudines du régulateur de la concurrence à partir du moment où les données sont utilisées en infraction avec le droit de la concurrence (A) voire même en infraction avec la réglementation sur les données personnelles (B).

A. L'utilisation des données en infraction avec le droit de la concurrence – l'utilisation déloyale des données vis-à-vis des concurrents

Au titre de l'article L. 420-2 du Code de commerce, l'entreprise ayant un pouvoir de marché s'interdit tout comportement déloyal vis-à-vis de ses concurrents, y compris dans le cadre de l'utilisation des données personnelles (et ce même si cette utilisation est réalisée en stricte conformité avec la réglementation sur la protection des données personnelles).

Cette situation est susceptible de viser en particulier l'entreprise publique ou anciennement publique. Celle-ci dispose d'un monopole sur une infrastructure quelconque et en même temps exploite un service à partir de cette infrastructure, comme en matière des télécommunications (France Telecom), des transports (SNCF), de l'énergie (GDF Suez)... L'abus peut alors être constitué soit par un refus injustifié de l'accès à l'installation à ses concurrents, soit par une pratique de prix non proportionnée, non orientée vers les coûts, ou non transparente ou discriminatoire.

Afin de prévenir ce type de pratique, et d'abus, le droit de la concurrence oblige la société concernée par la pratique déloyale à limiter l'utilisation des données personnelles[266], ou à donner accès à son fichier clients à ses concurrents[267]. Dans ce dernier cas, le respect de la réglementation sur la protection des données personnelles doit passer par la possibilité pour les personnes concernées, de s'opposer à la communication de leurs données personnelles aux concurrents[268].

Dans cette course à la détention de données, les axes d'évolution des entreprises passent par la fusion ou l'acquisition d'autres acteurs détenant de grands volumes de données, lesquelles

266. Décision de l'Autorité de la Concurrence n°09-D-06 du 5 février 2009 « SNCF – Expedia » : sanction de 5 millions d'euros d'amende pour la SNCF et 500 000 euros d'amende pour Expedia pour des pratiques mises en œuvre par la SNCF et Expedia Inc. dans le secteur de la vente de voyages en ligne : engagement de la SNCF de n'utiliser les données qu'aux fins d'exécution de la commande sans les exploiter commercialement.

267. Décision de l'Autorité de la Concurrence n° 14-MC-02 du 9 septembre 2014 « GDF Suez » : l'Autorité impose, en urgence et à titre conservatoire1, à GDF Suez de rendre accessible à ses concurrents une partie des données de son fichier clients aux tarifs réglementés du gaz (TRV).

268. Décision de l'Autorité de la Concurrence n° 14-MC-02 du 9 septembre 2014 « GDF Suez » : l'Autorité renvoie à l'avis de la CNIL du 13 juin 2014 qui précise que la communication des données personnelles des clients ne peut se faire que dans le respect des dispositions relatives à la protection de la vie privée et demande à GDF Suez de mettre en place un système permettant d'informer ses clients et de recueillir leurs éventuelles oppositions à cette communication.-

doivent être traitées conformément à la réglementation qui leur est « naturellement » applicable. La réglementation relative à la protection des données personnelles pourrait ainsi servir de point d'ancrage au régulateur de l'économie pour qualifier un abus de position dominante résidant dans l'application de conditions d'utilisation de données personnelles potentiellement non conformes au droit de la protection des données personnelles.

B. L'utilisation des données en infraction avec le droit des données personnelles – l'utilisation déloyale des données vis-à-vis des individus

Cette situation apparaît à première vue étonnante du fait de l'empiétement du régulateur économique dans un domaine où il revient normalement aux autorités de protection des données personnelles de qualifier les infractions à la réglementation sur la protection des données personnelles. Telle est néanmoins la situation actuelle en Allemagne où le *Bundeskartellamt* a lancé une enquête à l'encontre du réseau social Facebook afin d'analyser si la société aurait potentiellement abusé d'une éventuelle position dominante sur le marché des réseaux sociaux par le biais de conditions d'utilisation concernant les données personnelles des utilisateurs du réseau social qui seraient en contradiction, non pas avec le droit de la concurrence, mais avec le droit de la protection des données personnelles

Le régulateur économique pourrait également considérer que les politiques et procédures concernant le traitement des données personnelles ainsi que les pratiques contractuelles de l'entreprise doivent être prises en compte dans le cadre de l'analyse au regard du droit de la concurrence si elles sont le fait d'une entreprise en situation de position dominante.

De même, des conditions excessives en termes de protection des données personnelles - dans un contexte où les utilisateurs ne prennent pas systématiquement le temps de les lire - pourraient être considérées comme une exploitation abusive d'une position dominante (permettant l'application de ces conditions abusives).

La protection des données personnelles peut également être utilisée comme argument pour se démarquer de ses concurrents. A contrario, lorsque les concurrents sont peu nombreux et la concurrence faible, les notions de pouvoir de marché et d'abus pourraient même engendrer une dégradation de la protection des données personnelles (« privacy degradation »).

Si les problématiques liées à la confidentialité ne relèvent pas naturellement du champ d'intervention des autorités de concurrence, tout élément en lien avec la protection des données personnelles doit néanmoins être examiné. La Commission européenne s'est inscrite dans cette approche à l'occasion de l'examen de l'opération « Facebook/WhatsApp »[269]. Le 18 mai 2017, la Commission européenne a prononcé une sanction de 110 millions d'euros à

269. Décision de la Commission européenne, relative à l'opération d'acquisition de WhatsApp par la société Facebook, « Facebook/Whatsapp », COMP/M.7217, en date du 3 octobre 2014, http ://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf § 164. La Commission n'a analysé la concentration potentielle des données que dans la mesure où elle est susceptible de renforcer la position de Facebook sur le marché publicitaire en ligne ou ses sous-segments.

l'encontre de Facebook pour avoir fourni de fausses informations concernant son acquisition de WhatsApp en 2014[270]. L'entreprise américaine avait annoncé en 2014 qu'elle était dans l'incapacité d'établir une correspondance entre un compte utilisateur Facebook et un compte utilisateur WhatsApp, mais les résultats des enquêtes de la Commission européenne, déclenchées suite à la mise à jour des conditions d'utilisation de WhatsApp, ont prouvé le contraire. La sanction survient après l'amende infligée par la Commission de la concurrence italienne le 16 mai 2017 (sanction de 3 millions d'euros) pour des faits similaires[271].

Si plusieurs affaires ont fait ou pourraient faire l'objet de condamnations au travers du prisme du droit de la concurrence en France et à l'étranger, en impliquant des pratiques relatives au traitement de données personnelles, l'arrivée du RGPD et l'augmentation significative du montant des sanctions administratives définies en pourcentage du chiffre d'affaires de la société contrevenante à l'instar du droit de la concurrence, devra assurer une cohérence entre les interventions des différentes autorités de régulation. Cela pourrait passer par des actions d'interrégulation afin d'éviter par exemple la double sanction pour des faits identiques.

C'est sans compter sur les nouvelles problématiques liées à l'open data dont l'objectif est de favoriser l'accessibilité, l'exploitation et la réutilisation des informations et qui ne manqueront pas de générer également des questions touchant à la fois le droit de la concurrence et la protection des données personnelles.

270. Décision de la Commission Européenne à l'encontre de Facebook : http ://europa.eu/rapid/press-release_IP-17-1369_fr.htm L'amende annoncée par la commission européenne représente 1 % du bénéfice mondial réalisé par Facebook en 2016, ou 6 % du bénéfice européen.

271. Voir par exemple « WhatsApp condamnée en Italie pour son partage de données avec Facebook » (16 mai 2017) accessible à : http ://www.lemonde.fr/pixels/article/2017/05/16/whatsapp-condamne-en-italie-pour-son-partage-de-donnees-avec facebook_5128277_4408996.html.

LA *BLOCKCHAIN* À L'HEURE DE L'ENTRÉE EN APPLICATION DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Florence CHAFIOL,
Avocate associée August Debouzy
-
Alice BARBET-MASSIN,
Doctorante

Le développement des *blockchains,* qui se caractérisent notamment par la transparence de leurs modes de fonctionnement, est-il compatible avec la réglementation applicable en matière de données personnelles, renforcée depuis mai 2018 par l'entrée en application du Règlement Général sur la Protection des Données (« RGPD »)[272] ?

La *blockchain* est une technologie de stockage et de transmission distribuée de transactions, qui fonctionne de pair-à-pair, sans tiers de confiance et sans administrateur central de contrôle[273]. Cette dernière se matérialise par une chaîne de blocs, regroupés en transactions, qui sont vérifiés (techniques de cryptographie asymétrique et fonction de hachage) puis validés (algorithme de consensus distribué) par les nœuds du réseau c'est-à-dire par les participants. Ces transactions sont ensuite accessibles sur un livre virtuel, ouvert et infalsifiable. En fonction des blockchains concernées, celles-ci peuvent faire l'objet de collectes et de stockages de données et d'informations de toutes sortes, même si leur rôle est avant tout (I) de permettre la réalisation de transactions sécurisées entre individus en l'absence de tout intermédiaire et (II) de conserver les preuves infalsifiables de l'existence de ces transactions.

Dans le contexte actuel de protection renforcée des libertés individuelles et de la vie privée des personnes, il est pertinent de s'interroger sur la compatibilité de la blockchain avec la réglementation applicable en matière de données à caractère personnel et plus précisément avec le RGPD qui est entré en application le 25 mai 2018. Dans l'affirmative, les modalités pratiques d'une telle applicabilité et application seront étudiées.

272. Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016.

273. Voir la définition récemment dégagée dans le Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés), JORF n°0121 du 23 mai 2017 texte n°20 : « *Mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification* ». Pour des éléments de définition voir : Eric Caprioli, « La blockchain ou la confiance dans une technologie », La semaine juridique Edition Générale n°23, 672, Lexis Nexis, 6 juin 2016 et Eric Caprioli, « Les enjeux juridiques et sécurité des blockchains », Cahiers de droit de l'entreprise n°3, dossier 29, Lexis Nexis, mai 2017.

I. LA VARIABILITÉ DE LA NATURE DES DONNÉES TRAITÉES PAR LES *BLOCKCHAINS* EN FONCTION DU PROTOCOLE UTILISÉ

En fonction du protocole utilisé par les *blockchains,* qui peuvent être publiques (A) ou privées (B), la nature des données collectées et traitées variera, ces blockchains étant susceptibles de contenir ou non des données à caractère personnel.

La *blockchain* privée est un réseau privé par lequel un gérant choisit ses participants, contrôle et modifie le processus d'approbation. Dans un consortium ou « blockchain hybride », les droits d'écriture et de modification appartiennent à certains participants identifiés et limités en nombre. Au contraire, dans la blockchain publique, l'accès est possible par tous les participants, sans faculté de les restreindre et la vérification et la validation des transactions est possible par tous. Dans cette blockchain, tous les acteurs sont en situation égalitaire dans leur participation au réseau et les décisions sont celles validées par la majorité des participants.

La question de savoir si les données traitées sur une blockchain sont personnelles, pseudonymes ou inversement complètement anonymes est un prérequis indispensable puisqu'il détermine l'application ou non du RGPD[274].

A. L'existence possible mais non certaine de données à caractère personnel dans les blockchains publiques

L'anonymat initial qui caractérisait la blockchain publique à son origine n'impliquait pas, en principe, l'application de la réglementation en matière de données personnelles et du RGPD (1) ; compte tenu néanmoins de l'évolution des blockchains publiques, des données personnelles peuvent désormais être traitées par de nouveaux tiers (2).

1. L'absence de données personnelles, du fait de l'anonymat des participants, dans les premiers modèles de blockchains publiques

La blockchain publique utilise l'anonymat *via* la technique de la cryptographie asymétrique. Selon cette méthode, deux clés fonctionnant en couple sont détenues par chacun des participants à la transaction : une clé publique qui correspond à une adresse publique aléatoire composée de chiffres et de lettres (information publique) et une clé privée qui correspond à un mot de passe (information privée). À titre d'illustration, A, l'émetteur de la transaction a besoin de la clé publique de B, destinataire de la transaction pour lui envoyer des fonds à cette adresse. Une fois qu'il la possède, A signe la transaction à envoyer à B avec sa clé privée, puis envoie les fonds à B. Ce dernier, grâce à sa clé privée pourra utiliser les fonds désormais placés sur son adresse publique (voir ci-dessous).

274. Article 4 et Considérant 26, RGPD.

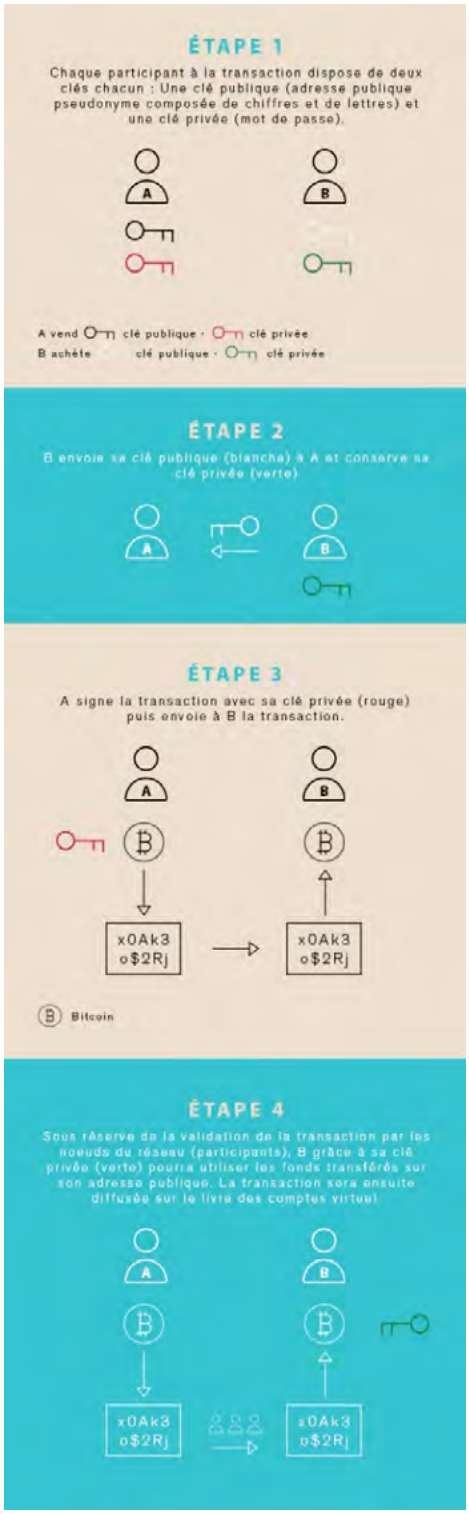


SCHÉMA N°1 :
CRYPTOGRAPHIE ASYMÉTRIQUE

Pour le protocole Bitcoin, l'adresse publique est générée par le portefeuille de l'utilisateur (le « wallet ») sans que ce dernier n'ait besoin de révéler son identité. L'identité de l'utilisateur et sa signature à la transaction n'étant pas révélée, il n'est pas possible de faire directement le lien entre les deux. Une fois validée par le réseau, la transaction visible par tous sur le registre fera uniquement apparaître les données transactionnelles (les adresses publiques, l'actif numérique, et l'identifiant de transaction). A l'origine, les premières adresses publiques accessibles sur le registre ne pouvaient pas être qualifiées de données personnelles car elles n'étaient pas identifiantes, entrainant de fait la non applicabilité du RGPD pour ces modèles de blockchains.

Cependant, comme l'a soulevé un rapport du gouvernement anglais sur la technologie des registres distribués, le lien d'anonymat utilisateurs/portefeuilles n'est pas parfait dans la mesure où les transactions qui sont visibles par tous, peuvent être tracées et suivies[275]. Il serait possible de reconstruire les actions d'une personne en suivant l'historique des transactions, notamment lors de plusieurs usages de la même adresse publique pour réaliser différentes transactions. Dans ce cas, l'identité d'une personne serait dévoilée. La plupart des portefeuilles modernes comme le «Ledger Wallet» délivrent, pour le reste, une nouvelle adresse publique à chaque transaction à des fins de garantie de protection de la vie privée. Aussi, l'utilisation d'internet relié à des adresses IP traçables permettrait, lors de la réalisation d'enquêtes par exemple, de définir une identité (sous réserve de non-dissimulation des traces).

2. Les données personnelles désormais requises par les plateformes d'échange de monnaies virtuelles

Initialement, les participants à la blockchain recevaient directement des monnaies virtuelles en récompense du minage qu'ils effectuaient afin de valider les

275. UK Government Office for Science, Distributed Ledger Technology : beyond Blockchain, 2016, pp.50, 51.

transactions[276]. Dorénavant, les participants achètent directement ces monnaies virtuelles sur des plateformes et le minage est effectué par des serveurs - pour la plupart situés à l'étranger - disposant de capacités de calculs très importantes. A cet égard, des données personnelles peuvent être détenues par certaines plateformes d'échange de monnaies virtuelles, c'est-à-dire des bureaux de change « électroniques » qui échangent des monnaies virtuelles contre des monnaies à cours légal (la maison du bitcoin, Paymium ou Kraken).

Les « bonnes pratiques » mises en œuvre par la plupart de ces plateformes consistent à garantir l'identité réelle de leurs clients en exigeant de leur part la communication de données à caractère personnel telles que : nom, prénom, données de vérification du mot de passe, date de naissance, adresse électronique, numéro de téléphone, emploi, carte de crédit, carte d'identité.

Le droit positif évolue nettement en ce sens. En effet, une communication de la Commission européenne prévoit d'étendre le champ d'application de la quatrième directive sur la lutte contre le blanchiment de capitaux afin d'y inclure les plateformes d'échange de monnaies virtuelles, voire les fournisseurs de portefeuilles de monnaies virtuelles, ce qui induirait la collecte obligatoire et le traitement de données personnelles à caractère financier[277]. La Commission a également annoncé le lancement du projet « **Titanium** », un consortium d'organismes publics et d'agences nationales qui travailleront de concert avec **Interpol** à l'élaboration d'outils d'exploration de la blockchain afin de réduire les usages illégaux[278]. L'Autorité de contrôle prudentiel et de résolution a rendu, pour sa part, une décision le 30 mars 2017 qui sanctionnait la société « Lemon Way » d'un blâme et d'une amende de 80 000 euros pour, notamment, ne pas avoir identifié des clients qui effectuaient des opérations d'achat et de vente de bitcoin[279].

Aux États-Unis, la levée de l'anonymat est déjà effective dans certains cas. L'« Internal Revenue Service » a déposé une assignation à l'encontre de la plateforme « Coinbase » exigeant l'identité de tous les utilisateurs sur le sol américain et leurs historiques de transactions de 2013 à 2015[280]. L'« Anti-money laundering regulations » identifie, de plus, la liste des adresses bitcoins qui sont liées à des activités criminelles[281].

En outre, les autorités de protection des données personnelles pourraient parfaitement considérer l'adresse publique comme une donnée personnelle. La Cour de justice de l'Union européenne a en effet déjà déclaré dans un arrêt du 19 octobre 2016 « B. contre Bundesrepublik Deutschland », que sous réserve de l'existence de moyens légaux permettant de faire identifier une personne grâce aux informations détenues par un tiers (le fournisseur d'accès à internet), l'adresse IP constitue une donnée à carac-

276. Le minage consiste en l'exécution de calculs coûteux en temps et en énergie afin de confirmer et chiffrer l'ensemble des transactions d'un bloc. Les mineurs sont récompensés pour la mise à disposition de leur puissance de calcul informatique. Pour chaque transaction, des milliers de mineurs lancent des calculs mais seul un mineur trouve la solution qui le valide. Chaque bloc supplémentaire fait donc l'objet de ce consensus distribué « proof of work (PoW) » pour être ajouté à la chaîne de blocs. La difficulté augmente à chaque 2016 bloc (à mesure de la puissance du réseau).

277. Communication de la Commission au Parlement européen et au Conseil, Communication sur d'autres mesures visant à renforcer la transparence et la lutte contre la fraude et l'évasion fiscales, le 05/07/2016, p.5 et voir l'annexe 1 de Communication de la Commission au Parlement européen et au Conseil relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme qui projette cette modification pour le 2e trimestre 2016.

278. Voir : http ://cordis.europa.eu/news/rcn/141335_fr.html (consulté le 15/07/2017).

279. Décision de l'ACPR rendue le 30 mars 2017, LEMON WAY, Procédure n°2016-05.

280. Tribunal de district du nord de la Californie, cas n° 3 :16-cv-06658-JSC, Etats Unis c. John Doe, 17/11/16 et la doctrine de l'IRS : https ://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance (consulté le 01/06/2017).

281. Voir : https ://www.finra.org/industry/aml (consulté le 7/06/2017).

tère personnel[282]. En se fondant sur l'article 2 de la loi du 6 janvier 1978 dite « informatique et libertés », la Cour de cassation reprend cette solution et précise que « les adresses IP, qui permettent d'identifier indirectement une personne physique sont des données à caractère personnel »[283]. Le G29 a par ailleurs considéré à deux reprises qu'il convenait de qualifier les adresses IP de données à caractère personnel[284]. La CNIL a, quant à elle, estimé dans une délibération que l'adresse IP des internautes « constitue une donnée à caractère personnel puisqu'elle permet d'identifier indirectement la personne physique titulaire d'un abonnement à internet »[285]. Le RGPD vise précisément, les adresses IP qui « lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes »[286]. Dans ce contexte, par analogie à l'adresse IP, l'adresse publique pourrait être une donnée permettant indirectement d'identifier une personne, et donc une donnée à caractère personnel.

B. Le stockage de données personnelles dans les *blockchains* privées spécifiques

Pour ce qui est de l'utilisation de la blockchain en tant que base de données (même si d'intérêt réduit pour ce seul usage), des blockchains privées collectent parfois des données à caractère personnel (données bancaires, de santé, en matière d'assurance, ou encore d'immobilier). Certains secteurs d'activité régulés nécessitent aussi de connaître l'identité du participant et se voient obligés de lever l'anonymat pour leur cas d'usage. Par exemple, le consortium R3 qui réunit des banques. En définitive, la pratique nous prouve que l'anonymat comporte ses limites. Pour permettre d'encadrer les *blockchains* traitant de données à caractère personnel, il importe de savoir qui pourrait être le responsable de traitement afin d'analyser quelles données seront sur la blockchain et d'en assurer un niveau de sécurité adéquat.

II. L'IDENTIFICATION D'UN RESPONSABLE DE TRAITEMENT / SOUS-TRAITANT

A l'aune du règlement européen, à chaque traitement de données personnelles correspond un responsable de traitement, en charge de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément audit règlement[287]. Encore faut-il savoir, appliqué à la blockchain, qui est le responsable de traitement. De nouveau, cette réponse est inconstante eu égard aux différents protocoles blockchains sous-jacents.

282. CJUE, 2e ch., 19-10-2016, aff. 582/14, Breyer c/ Bundesrepublik Deutschland.

283. Cass., 1e civ., 3-11-2016, n° 15-22.595 FS-PBI, Sté Cabinet Peterson c/ Sté Groupe logisneuf.

284. WO 37 : Le respect de la vie privée sur internet – Une approche européenne intégrée sur la protection des données en ligne, adopté le 21 11-2000 ; WP 136 : Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20-6-2007.

285. Délibération 2006-294 du 21-12-2006.

286. Considérant 30, RGPD.

287. Article 24 (1), RGPD.

Lorsqu'il s'agit de plateformes d'échanges qui collectent et traitent des données personnelles, ce sont elles et non les mineurs (qui eux mettent simplement à disposition du réseau leur capacité de calcul), qui seront désignées comme responsables de traitement. La question peut se poser de savoir si l'on pourrait imaginer, dans le cadre d'une blockchain publique, une coresponsabilité du traitement entre l'ensemble des membres du « réseau » ; la multiplicité des participants fait néanmoins douter qu'une telle coresponsabilité ait un quelconque sens en pratique, une éventuelle sanction pécuniaire ne pouvant, par exemple, pas être infligée dans ce type de circonstances.

Pour une *blockchain* privée, le responsable de traitement est plus facile à déterminer puisque cette qualité pourrait être attribuée au concepteur du protocole ou au gérant de la blockchain privée. Dans le consortium, le réseau « restreint » identifié pourrait ici supporter la responsabilité conjointe du traitement (article 26). Cela pourrait être le cas, par exemple, pour Foxconn, Gemalto, Cisco et Bosch, qui réfléchissent aux usages de la blockchain dans le cadre de l'Internet des objets, si ces derniers déterminaient au préalable les finalités et les moyens du traitement conjointement.

III. LE PRINCIPE D'*ACCOUNTABILITY* AISÉMENT HONORÉ

Dans l'objectif de responsabiliser les entreprises, le responsable de traitement devra se conformer au respect du principe de protection des données dès leur conception et de protection des données par défaut[288]. Il lui appartiendra de déterminer la probabilité de gravité du risque (évaluation objective) pour les droits et libertés de la personne[289] et d'en analyser l'impact. Le responsable de traitement aura également une obligation de sécurité des données[290] et de notification à leurs clients en cas de violation des données[291]. Les techniques de cryptographie utilisées par la blockchain depuis la conception du protocole sécurisent naturellement cette technologie, et ce, conformément aux nombreuses recommandations délivrées par les autorités de protection des données personnelles et l'ANSSI[292]. Le responsable de traitement aura pour obligation de vérifier, en pratique, que l'adresse publique ne permet aucun croisement de données et triangulation qui aurait pour effet de permettre une ré-identification du participant.

Le règlement européen prévoit aussi qu'un registre des activités de traitement détaillé avec un certain nombre de mentions doit être obligatoirement conservé, non seulement par le responsable du traitement, mais également par ses éventuels sous-traitants, pour les entreprises de plus de 250 salariés. Ce registre doit pouvoir être mis à tout moment à disposition des autorités de contrôle[293]. La blockchain peut, à ce titre, constituer une preuve puisque la gestion des registres distribués assure la traçabilité des opérations effectuées avec un historique de toutes les transactions

288. Article 25 (b) et Considérant 78.

289. Considérant 76, RGPD.

290. Article 32, RGPD.

291. Articles 33 et 34, RGPD.

292. La technique de cryptographie asymétrique est citée par le G29 dans son rapport sur les techniques d'anonymisation (Groupe de travail « article 29 » sur la protection des données, Avis 05/2014 sur les Techniques d'anonymisation, Adopté le 10 avril 2014, pp.22-24).

293. Article 30 et Considérant 82, RGPD.

passées. La fonctionnalité principale de la blockchain - tenue d'un registre assurant la traçabilité - peut donc constituer une bonne première base pour démarrer ce registre des activités de traitement et pour justifier des informations qu'il contient.

IV. LA COMPATIBILITÉ POSSIBLE MAIS DÉLICATE DU DROIT À L'EFFACEMENT / CONSERVATION DES DONNÉES LIMITÉES / DROIT D'ACCÈS ET DE RECTIFICATION

Le droit à l'effacement prévu dans le RGPD[294]sous-tend une suppression pure et simple des données. Les données personnelles contenues dans certaines blockchains se heurtent à son caractère inaltérable, par définition, qui vient obérer ce droit à effacement. L'effacement est cependant possible par un mécanisme de déconstruction et de reconstruction des nœuds mais il semble en pratique très difficilement réalisable. Pour supprimer une donnée, il faudrait en effet que plus de la moitié des nœuds du réseau travaillent ensemble pour reconstruire la chaîne de blocs depuis le moment où la donnée a été ajoutée (majorité requise pour la blockchain publique). Outre cette alternative de consensus difficile à mettre en œuvre, une minorité peut toujours invoquer un « fork », ce qui suppose la division de la chaine de blocs en deux, si elle estime pouvoir apporter des améliorations au protocole[295].

L'Open Data Institute a considéré que l'effacement d'une donnée ou un arrêt total du fonctionnement des nœuds exigé par un tribunal pourrait causer des dommages collatéraux et altérer l'ensemble de la chaîne de blocs car certaines données « légales » effacées dans un bloc pourraient être vitales. Le risque étant que de fausses données ou incomplètes restent sur la blockchain pour éviter que ces données vitales ne soient endommagées[296]. Cependant, les données personnelles des blockchains publiques traitées par les plateformes d'échange seront plus facilement effaçables puisque non liées au protocole. Pour les blockchains privées, il sera aussi plus simple d'effacer une donnée personnelle par décision du gérant ou, pour le consortium, avec l'accord des participants désignés.

L'article 5 (e) et le Considérant 39 du RGPD visent « une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées » et exigent qu'une « durée de conservation des données soit limitée au strict minimum ». Les informations placées dans une blockchain sont conservées sans limitation de durée et l'accès au registre est spatio-temporellement illimité, ce qui peut aller à l'encontre de ces dispositions.

Enfin, les articles 15 et 16 visent le droit d'accès et de rectification. Les utilisateurs de la blockchain peuvent tous accéder au registre public à tout moment. C'est le droit à la rectification qui s'avérera problématique car les données inscrites sont par définition non modifiables.

294. Article 17 et Considérants 65 et 66, RGPD.

295. Le protocole de blockchain Bitcoin prévoit, lorsque les utilisateurs estiment pouvoir apporter des améliorations au protocole, la possibilité de déclencher un « *hard fork* », soit une nouvelle version du protocole divisant la chaine en deux et la rendant incompatible avec l'ancienne version. Les transactions postérieures ne pourront de ce fait s'inscrire dans la continuation de la chaîne.

296. Open Data Institute, Applying blockchain technology in global data infrastructures, ODI-TR-2016-001, 2016, p.17.

V. LE TRANSFERT DES DONNÉES SANS FRONTIÈRES

En vertu des articles 44 et suivants du RGPD, les données personnelles ne peuvent être transférées vers des pays tiers que s'ils garantissent un niveau adéquat de protection. La blockchain - registre mondial partagé - suppose une duplication de toutes les données dans le monde. Ce transfert mondial de données nous conduit à nous interroger sur sa licéité dès lors que de nombreux états n'assurent pas un niveau de protection suffisant[297]. Nous pourrions néanmoins considérer que le transfert de données se fait avec le consentement de la personne physique dès lors que les données sont gérées par le couple mot de passe/clé publique pour réaliser une transaction (une des exceptions de l'article 49). Cependant, les autorités de contrôle ne privilégient pas les transferts hors de l'Union européenne basés sur le consentement des personnes dès lors que ces transferts sont massifs et répétés, ce qui pourrait être le cas en l'espèce.

Associer les techniques de cryptage et d'échanges de pair-à-pair distribuées pour aider à l'application du RGPD ?

En définitive, sous réserve de davantage de maturité, la technologie blockchain elle-même, grâce à ses techniques de cryptage et son système distribué, pourrait être utilisée par les entreprises pour les aider à atteindre au mieux les objectifs de conformité visés par le RGPD[298]. Une blockchain permettant, par exemple, aux usagers de mieux contrôler leurs données pourrait d'ailleurs être envisagée, à l'instar du projet Enigma initié par le MIT media Lab[299].

Conseils pratiques

Notre analyse fait apparaitre certains points de friction entre le RGPD et la blockchain. Il conviendra donc d'être attentif aux positions adoptées par les autorités de protection des données personnelles sur les sujets liés à la blockchain car celles-ci vont très vraisemblablement devoir se positionner rapidement ; une certaine souplesse dans leur appréciation serait souhaitable car une application trop stricte du RGPD aux blockchains ne sera pas sans poser d'évidentes difficultés.

297. Thibault Verbiest, *Technologie de registre distribué (blockchain) : premières pistes de régulation* , Lamy, RLDI n°129, août-septembre 2016.

298. Lire dans ce sens : Primavera De Phillipi, *The interplay between decentralization and privacy : the case of blockchain technologies, Journal of Peer Production*, Alternative Internets n°7, 15 octobre 2016.

299. Voir à ce sujet : Guy Zysking, Oz Nathan, Alex Pentland, *Decentralizing Privacy : Using Blockchain to Protect Personnel Data*, MIT media lab, 21 mai 2015 et le projet Enigma (https ://www.media.mit.edu/projects/enigma/overview/ (consulté le 01/08/2017).

LA GESTION DES DONNÉES À CARACTÈRE PERSONNEL AU SEIN DES VÉHICULES CONNECTÉS EN 10 QUESTIONS

Denise Lebeau-Marianna,
-
Carole Chartier,
Etudiante,
Promotion DU *Data Protection Officer* Paris II – 2017

I. QU'EST-CE QUE LE VÉHICULE CONNECTÉ ?

A. Définition du véhicule connecté

Le véhicule connecté appartient à la sphère de l'Internet des objets -en anglais « Internet of Things » (IoT)- et des objets connectés ou intelligents. Il n'existe pas de définition officielle du véhicule connecté ; parfois également appelé véhicule communicant, il s'agit d'un véhicule (voiture, deux-roues, camion…) doté de technologies lui permettant d'échanger en continu des données avec son environnement.

Les technologies de communication présentes dans les voitures connectées empruntent les réseaux de téléphonie mobile pour établir une connexion à Internet. Dans certains cas c'est la connexion du smartphone du conducteur ou d'un passager qui est utilisée (connectivité intégrée) ; les applications mobiles sont incorporées au véhicule grâce à un écran tactile ou à des commandes vocales. Dans d'autres cas le véhicule peut être équipé d'un boîtier télématique et d'une carte SIM (connectivité embarquée) qui remontent des données d'usage vers le serveur Cloud.

Ces systèmes de connectivité permettent ainsi au véhicule de collecter des informations qu'il pourra ensuite exploiter et distribuer vers l'extérieur, notamment vers d'autres véhicules (V2V) ou vers des infrastructures (V2I).

Cette connectivité permet d'offrir au conducteur et aux passagers toute une gamme de services connectés : navigation en temps réel, alertes trafic, alertes de sécurité, services de conciergerie, envoi de messages, partage de musique, réservation de places de parking, services d'éco-conduite, alertes liées à la maintenance du véhicule, *pay-as-you-drive, pay-how-you-drive…*

Mais les services connectés ne sont pas uniquement destinés aux clients particuliers : ces dernières années se sont développés des services en B2B, destinés aux entreprises, tels que les services de gestion de flotte de véhicules qui permettent aux sociétés gérant des flottes de véhicules de disposer de services et d'informations leur permettant une gestion optimisée de leur flotte.

Par ailleurs, les véhicules connectés peuvent également servir l'intérêt général puisque les informations qu'ils remontent peuvent être utilisées par les pouvoirs publics pour répondre à des problèmes généraux liés aux transports ou aux infrastructures (amélioration de la qualité des routes et de la signalisation routière…) ou aux autorités judiciaires dans le cadre de réquisitions (mise à disposition d'informations dans le cadre d'enquêtes pour vol ou autres infractions).

Le véhicule connecté est parfois confondu avec le véhicule autonome mais il s'agit en réalité de concepts assez différents puisque ce dernier désigne un véhicule capable de rouler sur route ouverte sans intervention du conducteur.

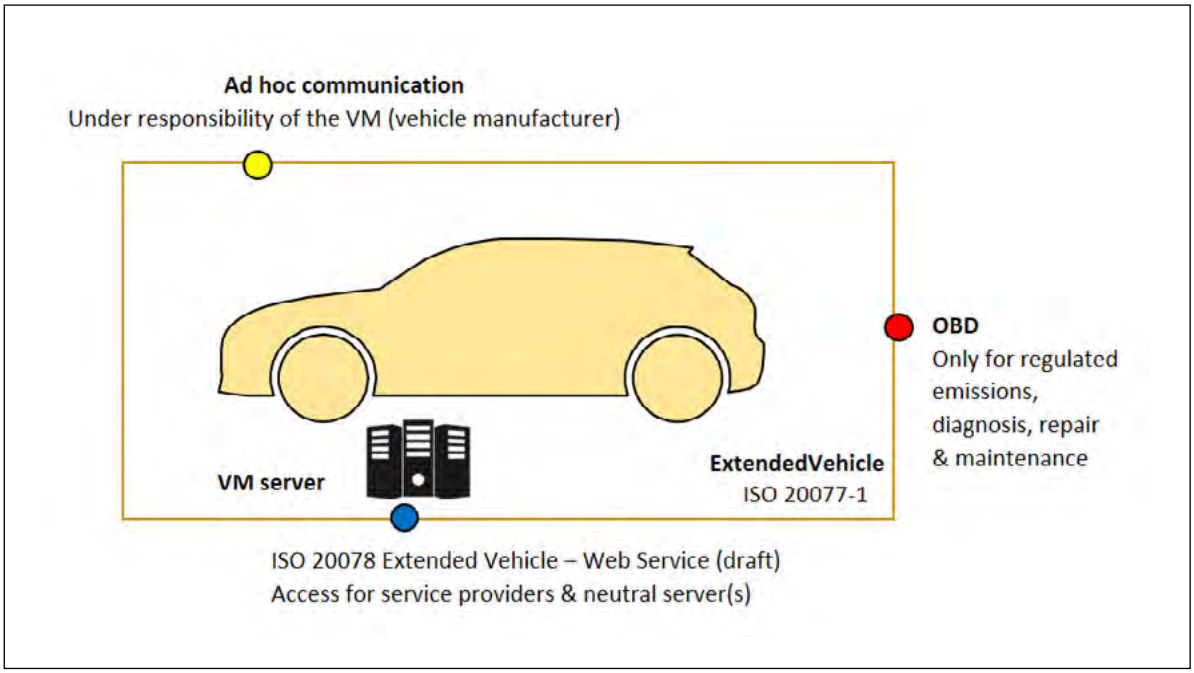
Dans un rapport de 2015, le cabinet d'études IDATE estimait que le marché du véhicule connecté devrait atteindre 9 milliards d'euros et concerner 420 millions de véhicules d'ici 2020. Le véhicule connecté constitue donc un enjeu majeur.

B. Le véhicule connecté et la norme véhicule étendu (ExVe)

Afin d'assurer le traitement sécurisé des données issues du véhicule dans le cadre de services connectés, les constructeurs européens ont travaillé à l'élaboration de normes sur la méthodologie du véhicule étendu[300].

La méthodologie décrit les conditions dans lesquelles les fournisseurs de services peuvent accéder aux données du véhicule, via trois interfaces :

- une interface OBD permettant aux réparateurs de récupérer les données relatives au diagnostic embarqué à bord du véhicule ;
- une interface pour les services web à travers un serveur faisant partie intégrante du véhicule étendu ;
- et une interface pour les communications sans fil en temps réel.



Source : ACEA position paper

300. *Norme Iso 20077-1* Véhicules routiers – méthodologie du véhicule étendu – information générale, décrivant le véhicule étendu, ses différentes interfaces et les différents usages possibles.

Le véhicule étendu est donc constitué du véhicule connecté en lui-même et du serveur associé et en faisant partie intégrante, permettant de traiter les données en débarqué, sans avoir à accéder directement au véhicule.

La norme établit des règles dont le but est de garantir la sécurité et la confidentialité des données, permettre à des tiers d'accéder aux données du véhicule sans créer de failles de sécurité, favoriser la concurrence entre tous les acteurs des services connectés et définir la responsabilité de chacun de ces acteurs.

II. QUELS SONT LES ACTEURS DU VÉHICULE CONNECTÉ ?

A. Les utilisateurs

Nombreux sont les acteurs qui peuvent prendre place à bord du véhicule et être en relation avec le ou les fournisseurs de services connectés. Alors que par le passé le constructeur automobile s'adressait quasi-exclusivement au propriétaire du véhicule, le fournisseur de services connectés se trouve face à différents « clients » potentiels, puisque les services connectés s'adressent non seulement au conducteur (qui aujourd'hui est de moins en moins souvent le propriétaire du véhicule) mais également aux passagers. Avec le développement croissant de services B2B, le fournisseur de services connectés ne s'adressent plus seulement à des clients particuliers mais de plus en plus à des clients professionnels.

L'avènement du véhicule connecté a permis la création de nouveaux modèles économiques autour du véhicule et de la mobilité (services d'autopartage, services de gestion de flottes de véhicules…) qui impliquent de raisonner en termes d'« utilisateur des services » et non plus en termes de « propriétaire du véhicule ».

La principale difficulté réside dans la capacité du fournisseur de services à identifier cet utilisateur, afin d'être en mesure (notamment) de l'informer de la collecte et des modalités du traitement de ses données et de recueillir son consentement le cas échéant, ainsi que l'informer de ses droits (droit d'accès, d'opposition…). Or dans un contexte où l'utilisateur peut faire usage du véhicule ou du service connecté de façon ponctuelle et où il s'attend souvent à ce que les formalités de mise en service soient allégées et à pouvoir facilement mettre fin au service, si possible à distance, cette tâche peut s'avérer compliquée. Cela implique de mettre en place des systèmes d'authentification de l'utilisateur, par exemple via un compte client sur internet, au travers duquel le fournisseur de services pourra porter à sa connaissance toutes les informations requises et recueillir son consentement.

B. L'écosystème technique et commercial

En plus des opérateurs classiques du secteur automobile tels que les constructeurs, les équipementiers, les réparateurs, les loueurs, les crédit-bailleurs ou les assureurs, l'écosystème du véhicule connecté comprend de nouveaux acteurs tels que les développeurs d'applications, les prestataires de services cloud ou les organismes publics.

La multiplicité des acteurs implique de définir des règles, comme par exemple les règles d'accès aux données via la norme véhicule étendu mentionnée au point 1-B ci-dessus.

Du point de vue de la responsabilité des données, il faudra déterminer, pour chaque cas de figure, qui est responsable de traitement et

qui est sous-traitant, ou voir s'il s'agit d'un cas de responsabilité conjointe. Cet exercice peut s'avérer périlleux, d'autant que le juge n'est pas tenu par la répartition décidée par les parties, et que les sanctions peuvent être considérablement lourdes.

Au vu des enjeux importants et des nombreux acteurs concernés, la CNIL a souhaité la mise en place d'un Pack de conformité sur le véhicule connecté[301]. Ce Pack définit des lignes directrices de conformité spécifiques au véhicule connecté, tout en délimitant la sphère de responsabilité des différents acteurs. Il s'agit également d'un gage de confiance pour les usagers du véhicule connecté.

III. QUELLES SONT LES LOIS APPLICABLES AU VÉHICULE CONNECTÉ ?

Du point de vue de la réglementation sur la protection des données à caractère personnel, les services connectés doivent se conformer aux législations de l'ensemble des pays dans lesquels ils ont vocation à être commercialisés, voire dans certains cas, le pays de circulation. Il peut s'agir d'un défi pour les développeurs qui conçoivent généralement ces services à l'échelle mondiale.

Le nouveau Règlement européen sur la protection des données (« RGPD »)[302] vise certes à harmoniser les règles de protection des données à caractère personnel dans toute l'Union Européenne. Toutefois, plus de la moitié des articles du RGPD renvoient aux législations nationales. Les lois nationales des pays européens sont revues afin de prendre en compte les dispositions du RGPD, mais des spécificités locales persistent, ce qui introduit une certaine complexité pour les entreprises.

Par exemple, en France, l'article 9 de la loi informatique et libertés du 6 janvier 1978 tel que modifié par la loi du 20 juin 2018 dispose que les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre, entre autres cas cités, que par les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales,les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ou bien encore les personnes physiques ou morales aux fins de leur permettre de préparer, d'exercer ou de suivre une action en justice. La collecte de la vitesse instantanée est nécessaire dans le cadre de certains services comme le *pay-how-you-drive.* Les concepteurs des services doivent donc jongler, pour un même service, avec des règles qui peuvent différer d'un pays à l'autre.

301. Pack de conformité « Véhicule connecté et données personnelles » du 17 octobre 2017 : https ://www.cnil.fr/sites/default/files/atoms/files/pack_vehicules_connectes_web.pdf.

302. 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 (règlement général sur la protection des données) dit « RGPD ».

Au-delà de l'Union Européenne, les projets transversaux doivent intégrer les règles applicables dans les autres pays du monde, dont l'esprit et la philosophie sont parfois assez différents des règles européennes. Ainsi, en Russie, les données des citoyens russes doivent être stockées uniquement sur des serveurs présents du le sol russe. Il en va de même en Chine où l'envoi des données hors du territoire est très encadré et où la loi impose même à certains services en ligne de stocker les données de leurs utilisateurs sur le territoire chinois, citant notamment les « infrastructures critiques d'information » (Critical Information Infrastructure), une notion assez floue susceptible de concerner toutes les entreprises, selon les intérêts des autorités chinoises.

En plus de la législation applicable, il existe également de la « soft law », comme par exemple le Pack de conformité « véhicule connecté » (cf. : supra II-B), qui propose des lignes directrices, pour une utilisation responsable des données dans les prochaines générations de voitures.

IV. *PRIVACY BY DESIGN, PRIVACY BY DEFAULT, PRIVACY IMPACT ASSESSMENT,* QUELS ENJEUX ET QUELLES CONTRAINTES ?

A. Les principes de « privacy by design » et « privacy by default »

L'article 25 du RGPD introduit deux nouveaux principes impactant le véhicule connecté : le « privacy by design » et le « privacy by default ».

Le « privacy by design » signifie que la protection des données à caractère personnel doit être prise en compte dès la conception des traitements, ce qui oblige le responsable du traitement à prendre des mesures et procédures techniques et organisationnelles appropriées - tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même - afin de le rendre conforme au RGPD, compte tenu des risques du traitement.

Tout le cycle de conception, production et de vie du véhicule connecté doit intégrer les règles de protection des données, dans tous les process internes et externes, dès le début de la phase de conception.

Le « privacy by default » ou « data protection by default » oblige le responsable à adopter des mesures consistant à limiter par défaut le traitement de données à caractère personnel à ce qui est strictement nécessaire, en ce qui concerne la quantité de données traitées, leur accessibilité et à leur période de conservation.

Ainsi, tel qu'exprimé dans le Pack de conformité « véhicule connecté et données personnelles » (cf. : supra II-B), un service ne pourra être mis en œuvre tant que la personne concernée n'aura pas fait un acte positif pour accepter la mise en place du service.

Cela représente un challenge pour les acteurs du véhicule connecté en raison des contraintes liées aux phases de conception longues et à la durée de vie des véhicules.

B. L'étude d'impacts (PIA)

Comme le stipule l'article 35 du RGPD, l'entreprise doit procéder à une analyse d'impact relative à la protection des données préalablement à tout traitement de données susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes, afin de s'assurer que l'ensemble des risques spécifiques à la vie privée ont été maîtrisés.

A cet égard il faudra systématiquement procéder à une classification des données pour voir s'il existe des données présentant des risques et déterminer s'il y a lieu ou non de réaliser une étude d'impacts.

V. QUELLES SONT LES FINALITÉS ENVISAGÉES ?

La mise en place de capteurs, applications et autres technologies embarquées dans les véhicules permettent de collecter et traiter différentes catégories de données pour des finalités qui se doivent, conformément à la loi du 6 janvier 1978 telle que modifiée par la loi du 20 juin 2018[303] et au RGPD, d'être déterminées, explicites et légitimes, et de ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités[304].

A cet égard, on peut distinguer sans prétendre à l'exhaustivité, les catégories de finalité suivantes : les finalités ayant vocation à avoir une meilleure appréhension technique du véhicule et de son environnement de circulation (A), les finalités ayant vocation à faciliter la conduite (B), les finalités ayant pour objet de permettre la fourniture de services en partenariat avec des prestataires tiers (C), et les finalités ayant vocation à assurer une meilleure sécurité (D).

A. Les finalités ayant vocation à avoir une meilleure appréhension technique du véhicule et de son environnement de circulation

Les finalités essentiellement techniques permettent aux fabricants de véhicules d'accéder à des informations agrégées sur l'état de la circulation, l'activation de feux de détresse, les conditions des routes, les véhicules en état d'urgence, les barrages routiers etc. mais également d'accéder à des informations plus spécifiques aux véhicules de leur marque (exemple : perception du marquage des voies, capteurs de données propriétaire, cartographie du fonctionnement du moteur, cartographie du fonctionnement de la boîte de vitesse etc.).

Ces données essentiellement techniques étant agrégées ne devraient à priori pas être appréhendées par la règlementation des don-

303. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2018-493 du 20 juin 2018.

304. Article 5 (1) (b), RGPD.

nées personnelles mais peuvent comporter des aspects « propriété intellectuelle » et « secret des affaires », dont il faut tenir compte.

Leur finalité peut consister notamment à alimenter des développeurs d'application sur l'état de la circulation, les zones de parking les plus proches, etc. En revanche, les données techniques propres aux véhicules d'une certaine marque sont principalement destinées à la marque et ses partenaires avec pour finalité de permettre aux fabricants d'analyser le fonctionnement des différentes composantes du véhicule pour en améliorer les performances.

Dès lors que ces données techniques ne peuvent être liées au conducteur, au détenteur de la carte d'immatriculation du véhicule ou au passager ou encore au VIN (Numéro d'Identification ou de série du véhicule), elles n'ont pas lieu d'être considérées comme des données à caractère personnel.

B. Finalités ayant vocation à faciliter la conduite

Un certain nombre de données peuvent être collectées afin d'offrir aux personnes concernées des fonctionnalités fournissant plus de confort. Tel est le cas des fonctionnalités suivantes :

• ***Infotainment*** : fonctionnalités visant à améliorer l'expérience de conduite (par exemple : réglage automatique des sièges en fonction de la taille du conducteur, bénéficier en temps réel d'informations sur le kilométrage, l'utilisation du moteur, la consommation du carburant, les limitations de vitesse, les points d'intérêt à proximité, les parkings, stations-service, boutiques, annuaire téléphonique, etc.).

• **Fonctions automatisées d'assistance à la conduite** : par exemple, à travers un régulateur de vitesse, une fonction de stationnement automatique, des capteurs assurant un freinage d'urgence automatique.

• **Authentification** des différentes personnes concernées avec des possibilités d'autorisation spécifiques quant aux différentes actions qu'ils vont pouvoir réaliser, en ayant notamment recours à des données biométriques exemple : dévérouillage du véhicule.

C. Finalités ayant pour objet de permettre la fourniture de services en partenariat avec des prestataires tiers

1. Optimisation et amélioration des produits et services

Le fabricant de véhicule confie à un fournisseur de services des données liées à un VIN aux fins d'établir des statistiques sur les paramètres de fonctionnement du véhicule ou l'état d'usure des pièces sur la base des usages de la personne concernée

2. Etudes

Etudes comportementales à des fins marketing, ou visant à mieux comprendre les causes des accidents de la route, études sur les facteurs d'amélioration de la sécurité au volant, etc.

3. Exploitation commerciale des données du véhicule

Offre de services à valeur ajoutée relatifs au véhicule (par exemple, contrat avec les assureurs « Pay-as-you-drive » ou assistance dépannage ou maintenance à distance (exemple : messages ou alertes liés au fonctionnement du véhicule, alerte sur l'état d'usage des freins ou rappel de la date de contrôle technique ou mises à jour techniques à distance des fonctions du véhicule), collecte de la géolocalisation afin d'identifier les points de charge, les zones de parking à proximité etc., collecte des centres d'intérêts pour offrir des services personnalisés.

D. Finalités ayant vocation à assurer une meilleure sécurité

D'une part, les fonctions basées sur le comportement de la personne et visant à améliorer la sécurité routière et à fournir une maintenance préventive : guide afin d'améliorer la conduite (par exemple, signal sonore ou vibration du volant en cas de dépassement sans clignotant, de franchissement du marquage au sol ou d'excès de vitesse, conduite prolongée sans suffisamment de pause, etc. ou pour l'alerter sur l'état du véhicule (par exemple, alerte sur l'état d'usage des pièces).

D'autre part, le « e-Call » : numéro d'appel d'urgence européen obligatoire à partir d'avril 2018, basé sur un service public et instaurée par la Commission Européenne

Enfin, la géolocalisation notamment aux fins de retrouver le véhicule en cas de vol

Si ces finalités peuvent paraître toutes légitimes, il convient néanmoins de veiller à ce qu'elles ne soient pas détournées. En effet, il peut être tentant pour un employeur d'obtenir des informations sur la conduite de son employé au volant notamment à travers des informations collectées sur l'usage des véhicules par le gestionnaire d'une flotte (société de leasing) mettant des véhicules à disposition de l'entreprise.

Afin d'éviter de telles dérives, il importe donc d'être vigilant quant aux conditions de traitement des données, aux personnes pouvant y accéder, à leur durée de conservation et à la proportionnalité des données collectées qui milite donc en faveur de l'anonymisation autant que possible et de restriction d'accès à un nombre limité de personnes ayant besoin d'en avoir connaissance.

VI. QUELLES SONT LES CONDITIONS SPÉCIFIQUES AU PROFILAGE ET LES RISQUES (DONNÉES SENSIBLES, DONNÉES D'INFRACTION ETC.) ?

Les données collectées dans le cadre d'un véhicule connecté peuvent être extrêmement riches. Ainsi les habitudes et préférences du conducteur, des passagers ou autres personnes concernées ayant un lien avec le véhicule peuvent être tracées grâce aux technologies embarquées. La « publicité contextualisée » devrait permettre à la voiture connectée d'être un nouveau point de contact entre le consommateur et ses marques préférées.

Conformément à l'article 22 du RGPD, les personnes concernées devront être informées de l'existence d'un tel profilage, des conditions de sa mise en œuvre et de la finalité recherchée et être à même de pouvoir s'opposer à ce qu'une action puisse résulter exclusivement d'un traitement automatisé, résultant d'un tel profilage.

Le profilage peut être justifié si la personne concernée y a consenti ou si ce profilage

est nécessaire à l'exécution d'un contrat en vue de lui fournir un service (notamment fourniture d'études sur les accidents, géolocalisation, fourniture de services d'assurance).

Dans ce cas, il conviendra de veiller à ce que le profilage ne puisse donner lieu à un traitement discriminatoire de la personne concernée (notamment exclure la personne du bénéfice d'un contrat de leasing ou d'assurance parce que sa conduite est jugée à risque) en accordant à la personne concernée notamment la possibilité de demander une intervention humaine.

VII. QUELLES SONT LES CONDITIONS DE COLLECTE ET TRAITEMENT : IN-IN, IN-OUT, IN-OUT-IN?

La CNIL propose dans le cadre du Pack de conformité « Véhicule connecté et données personnelles » (cf. : supra II-B) d'adapter le régime de protection des données personnelles selon les risques soulevés par le traitement conformément au RGDP.

Elle opère ainsi une distinction entre :

- les données collectées dans le véhicule qui restent dans le véhicule (IN-IN) : les données restent sous le contrôle des personnes concernées et ne sont fournies à aucun tiers. Elles devraient dans ce cas bénéficier de l'exception domestique et ne pas se voir appliquer les contraintes de la règlementation des données personnelles. Les données sensibles susceptibles de révéler des infractions, tels que les excès de vitesse peuvent être traitées pour guider le conducteur et le sensibiliser aux risques d'infraction.
- les données collectées dans le véhicule et transmises à un prestataire tiers (par exemple des prestataires de services d'assurance) pour fournir un service sur mesure selon le mode de conduite de la personne (conduite à risque, conduite fréquente etc.) (IN-OUT) : exemple : Pay-As-You-Drive.
- Les données collectées dans le véhicule et transmises à l'extérieur mais pour déclencher une action automatique sur les fonctions du véhicule (IN-OUT-IN) : par exemple, information sur l'état de la circulation pour permettre de prendre un itinéraire moins encombré.

VIII. QUELS SONT LES PRINCIPAUX FONDEMENTS LÉGAUX DES TRAITEMENTS ENVISAGÉS : CONTRAT, INTÉRÊT LÉGITIME, CONSENTEMENT, OBLIGATION RÈGLEMENTAIRE ?

A. Le consentement

Les études (par exemple sur les causes d'accident), sont soumises au consentement de la personne concernée. Ce sera également le cas des traitements ayant recours à la géolocalisation pour fournir des services de proximité (restaurants, parking etc.) sur la base de la géolocalisation. Ce consentement sera également nécessaire si le fabricant de véhicules souhaite partager les données collectées sur les personnes concernées par l'usage du véhicule connecté avec un partenaire

(exemple : assureur, partenariat avec les marques et enseignes préférées du consommateur utilisant le véhicule en tant que conducteur ou passager par exemple).

B. L'intérêt légitime

L'intérêt légitime du responsable de traitement permet de justifier un traitement à condition que cet intérêt légitime soit contrebalancé par des mesures permettant de préserver les droits et libertés de la personne concernée. Tel sera le cas par exemple du recours à la géolocalisation par un employeur pour une meilleure allocation des déplacements et en cas de vol du véhicule à condition toutefois que cette fonction puisse ne pas donner lieu à un contrôle des déplacements du salarié utilisateur du véhicule ou de tracer ses trajets en dehors de ses horaires de travail. L'intérêt légitime peut également être invoqué pour justifier les traitements basés sur une analyse comportementale du conducteur ou passager par exemple pour avoir une meilleure connaissance de leurs habitudes et leur adresser des publicités ciblées.

C. L'exécution du contrat

L'exécution du contrat permet de justifier le traitement des données visant à permettre la fourniture d'un service (service de maintenance à distance, assurance « pay-as-you-drive » etc.).

D. Le respect d'une obligation règlementaire

Tel est le cas du service e-call embarqué fondé sur le service 112 système embarqué dans un véhicule permettant de générer un appel de détresse, soit de manière automatique grâce aux capteurs du véhicule, soit de manière manuelle par les occupants. Grâce à ce dispositif, une notification à un centre de secours et une géolocalisation de l'incident sont possibles. Il devra être mis en œuvre à partir d'avril 2018 en vertu du règlement UE 2015/758 du 29 avril 2015.

Si les données sur lesquelles repose le traitement sont anonymisées, celles-ci ne sont plus des données à caractère personnel et peuvent donc être librement utilisées. L'anonymisation suppose notamment la suppression irréversible du lien entre les données d'usage et le numéro de série du véhicule rendant impossible la ré-identification des personnes concernées.

IX. QUELLES SONT LES CONDITIONS DE SÉCURITÉ DES DONNÉES TRAITÉES ?

La richesse des informations collectées par les véhicules connectés soulèvent des risques indéniables en terme de sécurité : (I) intégrité : sécurité physique des conducteurs en cas de compromission des fonctions critiques (désactivation ou activation intempestive des freins, blocage de la direction, etc.) ou intégrité du véhicule (II) confidentialité et vie privée : vol de données à caractère personnel, comme la liste des contacts, captation des conversations par exemple, (III) risque d'apparition de ransomwares avec prise de contrôle du véhicule par des tiers etc.

Les différentes composantes des systèmes mis en œuvre au sein du véhicule devront donc intégrer selon la finalité des mesures de sécurité afin de veiller à ce :

• que les données restant sous le contrôle des personnes concernées ne puissent être accédées par des tiers ou être piratées ;

• qu'un accès restreint soit prévu pour ne donner accès aux données du véhicule connecté devant être partagés avec des tiers (fabricant automobiles, assureurs, prestataires de services etc.) qu'aux personnes ayant besoin d'y accéder pour les finalités légitimes prévues ;

• Ces mesures de sécurité pourront notamment consister à mettre en place des mesures de chiffrement, des mesures d'habilitation d'accès, des mesures d'authentification ou de sécurité contre les intrusions.

X. QUELLES SONT LES OBLIGATIONS DE CONSERVATION ?

Les données collectées à partir des véhicules connectés doivent être traitées pour une durée limitée à celle nécessaire pour répondre à la finalité recherchée, à l'exception des données anonymisées qui peuvent être conservées de manière indéfinie.

Le processus d'anonymisation devra être examiné attentivement afin de vérifier qu'il est irréversible et conforme aux exigences règlementaires.

Concernant les autres catégories de données à caractère personnel, il convient de bien identifier les différentes catégories de données traitées selon les finalités afin de déterminer la durée de conservation applicable.

Ainsi, à titre d'exemple, les données collectées à des fins de fourniture de service qui demeurent sous le contrôle des personnes concernées doivent être conservées le temps nécessaire à la durée des services demandées. Ces données doivent pouvoir être conservées tant que la personne concernée le souhaite et être supprimées avant que le véhicule ne soit cédé à un tiers.

Les données qui seront traitées sur les systèmes du véhicule connecté et ensuite partagées avec le fabricant automobile notamment aux fins d'amélioration du véhicule devront être soumises à la durée nécessaire à l'étude des composants techniques pertinents pour la finalité recherchée. La CNIL a, dans le cadre de la formalisation du Pack de conformité « Véhicules

connectés et données personnelles », déterminé cette durée qui peut varier de 3 à 5 ans.[305]

Pour les données collectées dans le cadre de situations sensibles telles que situations d'urgence ou vol, elles ne devraient pas être conservées au-delà de la durée nécessaire à la résolution ou au traitement de ces situations[306].

Le paramétrage des systèmes embarqués devra permettre de limiter la durée de conservation conformément à ces différentes finalités.

Conformément aux directives de la CNIL, les conditions de paramétrage devront permettre d'intégrer les durées de conservation selon l'utilisation des données en base active (archivage courant), à des fins de contentieux (archivage intermédiaire permettant une conservation avec un accès), ou à des fins scientifiques, statistiques ou historiques (archivage définitif).

305. CNIL, Pack de conformité – Véhicules connectés et données personnelles, octobre 2017 : « Pour la finalité 1 (optimisation de modèles, amélioration du produit) : en cas de pseudonymisation, une durée de conservation de 3 ans semble proportionnée par rapport à la finalité poursuivie.Une fois anonymisées, les données d'usage peuvent être conservées pour une durée illimitée. Pour la finalité 2 (études d'accidentologie) : il convient de distinguer deux types de données : Les données relatives aux participants et aux véhicules : ces données peuvent être conservées pendant la durée de l'étude. Les données techniques issues des véhicules : la CNIL recommande que la conservation de ces données n'excède pas 5 ans à compter de la date de fin de l'étude. À l'issue de cette durée, les données doivent être supprimées ou anonymisées. Pour la finalité 3 (exploitation commerciale des données du véhicule), nécessitant la conclusion d'un contrat de prestation de service, il convient de distinguer deux types de données : Les données commerciales (identité de la personne, données relatives aux transactions, aux moyens de paiement, etc.) : ces données peuvent être conservées en base active pendant toute la durée du contrat. A l'issue du contrat, elles peuvent faire l'objet d'un archivage physique (sur support distinct : cédérom, etc.) ou logique (par gestion des habilitations) pour prévenir d'éventuels contentieux. Puis, à l'issue des durées de prescription légale, les données doivent être supprimées ou anonymisées. Les données d'usage : ces données doivent être conservées pendant une durée limitée sous forme détaillée, puis doivent être agrégées pour le reste de la durée du contrat. Pour la finalité 4 (« eCall ») : Ces données doivent être totalement effacées lorsqu'elles ne sont pas nécessaires à cette fin. En outre, dans la mémoire interne du système « eCall », les données doivent être automatiquement effacées. Seules les trois dernières positions du véhicule peuvent être conservées, dans la mesure où cela est strictement nécessaire pour préciser la position actuelle du véhicule et la direction suivie au moment de l'événement [...] ».

306. « *Pour la finalité 5 (lutte contre le vol) : les données de localisation ne peuvent être conservées que le temps de l'instruction du dossier par les autorités judiciaires compétentes ou jusqu'à l'issue d'une procédure de levée de doute n'aboutissant pas à la confirmation du vol du véhicule.* ».

SMART CITIES ET NOUVEAUX ENJEUX DE PROTECTION DES DONNÉES : COMMENT TIRER PROFIT DU NOUVEAU RÈGLEMENT EUROPÉEN ?

Juliette SCHWEIGER,

La mise en application du règlement (UE) 2016/679 (« RGPD ») en mai 2018 renforce les enjeux de protection des données personnelles qui font partie intégrante des politiques territoriales. Le potentiel de développement des smart cities pourrait ne pas s'avérer durable si les collectivités et les opérateurs privés ne se soucient pas davantage de la protection et de la sécurité des données des citoyens. La prévention du risque de sanctions introduites par le RGPD pesant sur les acteurs publics comme les acteurs privés milite également en faveur d'une évolution de l'approche smart city. L'équation entre protection des données personnelles et démarche d'innovation est souvent complexe. L'arrivée d'un nouvel acteur, le Délégué à la Protection des Données personnelles (ou Data Protection Officer « DPO »), qui devra être capable de s'appuyer sur les leviers offerts par le règlement pour contourner ces difficultés constitue une nouvelle opportunité.

La smart city évolue de plus en plus vers une réalité de territoire intelligent. Elle s'inscrit au cœur des stratégies urbaines et se caractérise par un ensemble d'innovations, en particulier l'utilisation de systèmes de gestion intelligents. Leur but est de tendre à une personnalisation optimale des services aux usagers via notamment la fourniture de nouveaux services par les grands opérateurs privés. Cela nécessite d'équiper la ville et les personnes de capteurs afin de les mettre en réseau.

En France, des dizaines de villes, de grands groupes et de start-up déploient des capteurs et applications à visée prédictive, dans des domaines comme l'environnement, l'énergie, (tels les compteurs d'électricité connectés Linky), la mobilité, la sécurité, la propreté. Le véritable défi pour les villes consiste à innover en capitalisant sur le Big Data[307]. Ces technologies visent à capter massivement les données incluant les données personnelles[308]des citoyens. La donnée devient par conséquent un élément essentiel de la politique territoriale. Ces innovations passent par la prise en compte de critères, tels que la protection de la ressource, la mobilité, la gouvernance.

Il est surprenant, qu'avec l'entrée en application du RGPD, la prise en compte d'autres critères liés au respect de la vie privée et de la protection des données personnelles ne soit pas davantage au cœur des préoccupations des acteurs de la *smart city.* En effet, la protection

307. La CNIL rappelle que ce terme caractérise « des données massives ». Les ensembles de données traités correspondant à la définition du *Big Data* répondent à trois caractéristiques principales : volume, vélocité et variété.

308. Une donnée personnelle est définie, conformément à l'article 6 du Règlement comme « toute information relative à une personne physique identifiée ou 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, etc. ». Cela couvre évidemment les informations à caractère personnel considérées comme « données sensibles qualifiées de « catégories particulières de données personnelles » par l'Art. 9 du RGPD.

de la vie privée constitue un enjeu majeur car le droit à la vie privée est un droit fondamental reconnu par les textes nationaux et internationaux. La Charte des droits fondamentaux de l'Union européenne dans son article 8 et l'article 16 § 1 du traité sur le fonctionnement de l'UE consacre la protection des données à caractère personnel comme un droit autonome, séparé et différent du respect de la vie privée visé à l'article 7 de ladite Charte.

Le RGPD va au-delà en soulignant la nécessité de « susciter la confiance afin de permettre à l'économie numérique de se développer ». Pour ce faire, « Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant. La sécurité tant juridique que pratique devrait être renforcée pour les personnes physiques, les opérateurs économiques et les autorités publiques »[309].

Dans ce contexte, il est essentiel de dépasser la logique centrée sur l'usager pour évoluer vers une logique centrée sur le citoyen en position d'empowerment sur ses données. En introduisant une responsabilité conjointe entre les responsables de traitement et leurs sous-traitants dans l'écosystème très transversal de la smart city, le RGPD accroît les enjeux juridiques et de sécurité liés à la protection des données personnelles (I), favorisant la recherche de solutions au travers des nouvelles mesures organisationnelles et techniques offertes par le RGPD (II).

I. PRINCIPAUX ENJEUX JURIDIQUES ASSOCIÉS À LA COLLECTE, À LA RÉUTILISATION ET À LA SÉCURITÉ DES DONNÉES

En vertu du principe d'*accountability*[310], les responsables du traitement, qu'il s'agisse de personnes publiques ou d'organismes privés, devront être en mesure de démontrer qu'ils ont satisfait aux exigences du RGPD en adoptant les mesures techniques et organisationnelles appropriées. « Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne le traitement, à permettre à la personne concernée de contrôler le traitement, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité (incluant la protection de l'intégrité et de confidentialité des données) ou de les améliorer »[311].

Le RGPD incite les acteurs à prendre en compte ces principes de protection, y compris dans le contexte des marchés publics[312]. L'analyse d'appels à projets et des marchés de partenariat lancés depuis l'entrée en vigueur du règlement montre que les principaux enjeux juridiques spécifiques aux *smart cities* sous l'angle de la protection des données personnelles ne sont pas toujours suffisamment anticipés par les maîtres d'ouvrages et par les entreprises privées à l'appui de leurs offres. Ces enjeux ont principalement trait aux IoT[313] (A) et au *Big Data* (B).

309. Considérant 7, RGPD
310. Article 24 (1), RGPD
311. Considérant 78et Article 5 (1) (f), RGPD
312. Considérant 78 in fine, RGPD
313. Groupe Article 29, *Internet of Things ou Internet des Objets -Avis /2014 sur les dernières évolutions relatives à l'internet des objets* (WP 223 du 16 09 2014)

A. Principaux enjeux liés aux IoT dans les *smart cities*

1. Enjeux associés à la licéité de la collecte automatisée

Dans la *smart city,* la collecte et l'exploitation de données sont réalisées par deux typologies d'acteurs : es collectivités locales et l'administration publique via les régies de transports, la voirie, la collecte des déchets, les services d'urgence, les hôpitaux. La création des plateformes centrales de gestion de « données territoriales », comprenant un volet en *open data* (en accès libre) est encouragée par la loi pour une République numérique[314]. Elles deviennent dépositaires d'un grand nombre de données personnelles, en collectant des données auprès de citoyens, eux-mêmes producteurs de données, pour développer des services. Les acteurs privés comme les opérateurs télécoms, les distributeurs d'énergie sont également collecteurs de données personnelles.

Le grand nombre de systèmes, de dispositifs et d'acteurs opérant dans la ville, ainsi que les multiples transferts qui circulent d'une plateforme à l'autre rendent le consentement, le contrôle et la sécurité des données très complexes, la collecte des données personnelles étant le plus souvent automatisée et potentiellement continue.

CARTOGRAPHIE DES CAPTEURS DE LA *SMART CITY* ILLUSTRANT LES SECTEURS CONCERNÉS PAR LES « SMART TECHNOLOGIES », LES TECHNOLOGIES UTILISÉES AINSI QUE LES PARTIES PRENANTES (INDIVIDUS, ACTEUR PUBLIC, ENTREPRISES, PARTENARIATS PUBLIC-PRIVÉ)[315].

314. Loi Lemaire du 07 10 2016 dont l'un des 3 principaux objectifs vise à créer un cadre de confiance clair, garant de droits des utilisateurs et protecteur des données personnelles.

315. Régis Chatellier, Laboratoire d'Innovation Numérique de la CNIL, *Cartographie des capteurs de la smart city,* 04 mai 2017

2) Enjeux associés à l'obtention du consentement

Le respect du droit à l'information des personnes concernées et l'obtention de leur consentement, gage de la licéité du traitement, sont les pierres angulaires de la protection des données personnelles. Or elles sont particulièrement affaiblies dans les technologies de la *smart city.*

L'utilisation des capteurs de données illustre cette problématique. Pour exercer leurs droits, les citoyens doivent être informés, selon l'article 13 du RGPD, de l'identité du responsable de traitement. Il s'agit là d'une condition essentielle à l'exercice du droit d'accès, que les informations soient ou non collectées auprès de la personne concernée. Or dans une smart city, la mutualisation des systèmes de collecte et de traitement ainsi que la multiplicité des acteurs rendent difficile cette identification.

De plus, le consentement éclairé de la personne dont les données sont collectées et traitées doit être recueilli, conformément à l'article 12 du RGPD « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ». La CNIL a d'ailleurs condamné Google à payer une amende de 100.000 euros pour avoir collecté des données personnelles lors de la mise en place de Google Street View en 2011 sans le consentement des personnes concernées. Le problème pourrait également se poser avec d'autres objets connectés omniprésents dans les smart cities.

Aussi, puisque la personne concernée peut retirer son consentement à tout moment, et afin de surmonter cette difficulté, les entreprises concernées pourront exploiter l'exception prévue à l'Art 6 (e) du RGPD concernant « l'exécution d'une mission de service public », exception étant potentiellement soumise à un principe d'interprétation stricte.

B. Enjeux liés au *Big Data* : risque de réutilisation indue et de compromission des données

Le *Big Data* soulève quatre difficultés principales :

- risque de ré-indentification de la personne pouvant déboucher sur de nouveaux types de « class actions »[316] ;

- difficulté de réconciliation avec le principe de minimisation énoncé à l'article 5.1 (c) du RGPD ;

- risque détournement de finalité ("repurposing") car la finalité ultime est souvent imprévisible et différente de la finalité initiale ;

- manque de transparence des algorithmes[317], l'exploitation des résultats (justice prédictive en matière de criminalité urbaine) allant jusqu'à un risque de « redlining », de « data underclass », source de risques de discrimination pour les citoyens concernés.

316. Voir en ce sens Loi N° 2016-1547 du 18 11 2016 de modernisation de la justice du xxi[e] siècle permettant aux personnes physiques « placées dans une situation similaire » ayant subi un dommage consécutif à une atteinte aux données personnelles d'initier une action de Groupe.

317. CNIL, Algorithmes utilisés par l'administration : vers plus transparence, 05 09 2017.

1. Risque de réutilisation pour des usages et finalités non souhaités, comme le profilage

De nombreuses technologies de la *smart city* (dont la géolocalisation) captent des données personnelles de citoyens. Leur croisement rend possible la création de profils de ses habitants en fonction des habitudes, des lieux fréquentés, voire même la prise de décisions les concernant.

Les compteurs dits intelligents permettent de collecter de très nombreuses informations dont celles concernant la courbe de charge. La courbe de charge est constituée de relevés à intervalles réguliers, elle permet d'avoir une connaissance précise de la consommation des ménages très rapidement. La connaissance et le traitement de ces informations peuvent permettre d'obtenir de nombreuses informations sur les habitudes de vie des abonnés. C'est pourquoi, dès 2012, la CNIL a considéré que ces données ne pouvaient pas être collectées de façon systématique mais uniquement dans certains cas[318]. La courbe de charge peut faciliter le recours au profilage au sens de l'article 4. 4) du RGPD, défini comme l'utilisation de données à caractère personnel pour évaluer, analyser ou prédire certains aspects personnels ou comportements. Si le profilage n'est pas prohibé par le RGPD, il requiert la mise en place de mesures appropriées dès lors que la décision n'est pas fondée sur le consentement explicite de la personne concernée[319]. Parmi ces mesures figure l'analyse d'impact[320] obligatoire en cas de profilage et qui a donné lieu à des recommandations par le G29.

Les données personnelles peuvent être également être agrégées, pseudonymisées[321], puis revendues pour des usages tiers. Le principal enjeu les concernant tient à la ré-identification : les données pseudonymisées permettent encore l'identification des personnes et ne doivent pas être confondues pas l'anonymisation qui rend toute identification de la personne impossible. Rob Kitchin note que les données pseudonymisées peuvent avoir un impact direct ou indirect sur la vie des personnes, notamment dans le cas des données vendues à des data brokers à des fins de marketing, ou dans leur usage par des algorithmes (i.e : prédiction du crime), menant à une forme de « data déterminisme »[322]. Ces inférences peuvent se révéler fausses et avoir des conséquences pour les individus. Même si l'anonymisation[323] est une garantie du droit au respect de la vie privée, elle n'est pas, selon les experts, une technique très fiable car l'on peut facilement retrouver l'identité d'une personne par des recoupements de données.

318. Délibération CNIL N°2012-404 du 15 11 2012 visant à encadrer les conditions de collecte et d'utilisation de la courbe de charge et formulant des recommandations sur les finalités des traitements, la durée de conservation des données, les destinataires des données et l'information des personnes concernées.

319. Article 22 (3), RGPD.

320. Article 35 (3) (a), RGPD.

321. Définition pseudonymisation (Art 4 5) du RGPD : « traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires ».

322. Kitchin, R. (2016) *Getting smarter about smart cities : Improving data privacy and data security*. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

323. L'avis du G29 du 16 04 2014 rappelle qu'un processus d'anonymisation est un traitement du fait, notamment, que des données personnelles ont été initialement collectées. Il rappelle qu'une donnée anonyme n'est pas une DCP mais que les données pseudonymisées ne sont pas des données anonymes. Le G29 propose trois critères pour évaluer l'anonymisation : l'individualisation : est-il toujours possible d'isoler un individu. La corrélation : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu. L'inférence : peut-on déduire de l'information sur un individu ? D'après Arvind Narayanan - Princeton, « l'anonymat est devenu est devenu algorithmiquement impossible ».

2. Enjeux associés à la sécurité et au risque Cyber

Le risque cyber « se définit par la rencontre entre les vulnérabilités d'un système d'information, les menaces générées par un ou des agents malveillants et les impacts potentiels ». Il fait potentiellement peser un risque sur la sécurité qui régit l'accès à la donnée et menace son intégrité.

Dans une smart city, le risque cyber est accru par la présence d'objets connectés et par l'interconnexion des services. Il concerne tout particulièrement les opérateurs d'importance vitale[324], acteurs clefs de la smart city, ainsi que les futurs opérateurs d'importance essentielle définis par la Directive UE 2016/1148[325].

Dans ce contexte, le défaut d'harmonisation des référentiels de sécurité dans les smart cities constitue un enjeu important. C'est pourquoi il est recommandé d'inclure systématiquement la cyber-sécurité dans les marchés liés à la digitalisation des collectivités. Des clauses sur la sécurité avec des critères d'exigence minimale définis au niveau national, en concertation avec les associations de collectivités et l'ANSSI, voire le recours à un cloud homologué par l'ANSSI sont préconisés. La création d'un service public local de la donnée incluant un stockage des données en Europe est également recommandée[326].

Sans attendre que les données soient collectées, il faut donc s'assurer de leur sécurisation. C'est pourquoi l'article 32 du RGPD fait peser sur le responsable de traitement et ses sous-traitants une obligation de sécurité renforcée qui se décline sous la forme de « mesures techniques et organisationnelles » adaptées au risque.

Parmi ces mesures, figurent « les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ». Les mécanismes de sauvegarde de la vie privée (confidentialité/sécurité) sont encore plus impérieux dans le contexte de la smart city, en raison de l'obligation de notification à l'autorité de contrôle d'une violation de donnée à caractère personnel dans les conditions définies par les articles 33 et 34 du RGPD.

En cas de défaillance, l'article 226-17 du Code pénal prévoit des sanctions pouvant aller jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende.

Partant de ces différents enjeux, comment utiliser les leviers du RGPD afin que la protection des données personnelles ne soient plus perçue comme une contrainte mais devienne un axe de politique stratégique des villes et un avantage compétitif pour des acteurs privés de la smart city qui cherchent à se démarquer des acteurs traditionnels ?

324. Opérateurs d'importance vitale dans 12 secteurs définis par l'Art R1332-2 du Code de la Défense dont la gestion de l'eau et l'énergie.

325. Directive UE 2016/1148 du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

326. Voir en ce sens l'expérience menée au Forum international de la cyber sécurité en janvier 2016 où une faille au niveau de la passerelle utilisée pour connecter un compteur électrique a été volontairement mise en lumière pour démontrer les risques de vulnérabilité.

II. LE DPO, UN NOUVEL ATOUT AU SERVICE DE LA STRATÉGIE DATA ET DU « PRIVACY MANAGEMENT »

Dans le contexte particulier des smart cities, le principal défi des DPOs consistera à accompagner les projets innovants souvent difficilement conciliables avec la prise en compte des nouvelles exigences du RGPD, dont le non-respect peut exposer les responsables de traitement et leurs sous-traitants au montant maximal des sanctions prévues par le règlement, soit 4 % du CA annuel mondial ou jusqu'à 20 millions d'euros, pour les opérateurs privés, le montant le plus élevé étant retenu.

A. Comment satisfaire aux exigences d'accountability dans le contexte des *smart cities* ?

1. Le DPO, nouvel acteur d'une « smart gouvernance »

Le DPO apparaît comme un rempart essentiel contre une possible intrusion des pouvoirs publics dans la sphère privée risquant de miner la confiance des usagers. Le DPO, au titre de ses missions de conseils prévues par l'article 39 du RGPD, devient l'interlocuteur privilégié pour répondre aux besoins d'accompagnement à tous les stades des processus de numérisation des services urbains. Le DPO étant bien souvent, de par sa culture, issu d'un mélange de professions, il doit se positionner comme un seul acteur essentiel dont l'objectif est d'entraîner les autres acteurs de façon transversale car le RGPD impose de modifier la gouvernance des données personnelles.

Le DPO, régulateur interne de la conformité encré dans la transformation digitale, se doit d'être proactif et instigateur de valeur ajoutée en amont des projets et ceci au niveau de chacun des intervenants. La complexité de ces enjeux de protection dans la *smart city* milite en faveur d'une collaboration renforcée entre les DPO de la sphère publique et de la sphère privée.

Le G29 dans les lignes directrices « WP 243 rev. 1 » recommande, en tant que bonne pratique, que les organismes privés exerçant des missions publiques (dont les délégataires de services publics) désignent un DPO. Par ailleurs, l'article 37(1)(b) du RGPD requiert désignation obligatoire d'un DPO en cas de traitements impliquant le « suivi régulier et systématique » des personnes concernées. Le G29, au travers de l'avis précité, interprète « régulier » comme en cours ou se produisant à des intervalles particuliers, récurrent ou constant, et précise que le terme « systématique » vise le suivi dans le cadre d'un plan général de collecte de données. Parmi ces activités figurent les « compteurs intelligents ».

Les organismes publics, dont les collectivités devront obligatoirement désigner un DPO. Les DPO désignés dans ce contexte auront un important travail de sensibilisation et de formation des services achats afin que ceux-ci utilisent plus efficacement les leviers de la commande publique en matière d'achats innovants, par exemple par l'introduction de nouveaux critères de performance des mesures de protection de type « smartness perception index ».

En phase d'exécution, la remise de rapports d'activités réguliers par les entreprises, destinés à garantir l'effectivité des mesures de protection mises en place dans une logique de mesure opérationnelle de « l'accountability » serait opportune. Le DPO pourra également utiliser les leviers du *contract management* pour sécuriser les opérations en cours et les

nouveaux contrats par la rédaction de chartes définissant les chaînes de responsabilités dans le traitement des données, la répartition des coûts liés aux mesures de sécurité. Des audits des marchés en cours seront également nécessaires afin d'identifier les marchés dont les prix devront être ajustés pour prendre en compte les surcoûts induits par les mesures exigées par le RGDP.

2. Exemple des *Privacy Committees*

La multiplicité des acteurs et la nécessité d'emporter l'adhésion des citoyens dont le consentement ne peut pas être recueilli individuellement milite en faveur d'une gouvernance collaborative et coordonnée entre les acteurs publics et privés. Ceci répondrait aux exigences du RGPD quant à l'adoption de mesures organisationnelles appropriées. Au titre de ses missions de conseils, le DPO pourrait encourager la mise en place de Comités consultatifs ou Comités d'experts chargés de fournir des avis ou d'assister les acteurs de la *smart cities* dans leurs choix de protection. Comme le recommande le député Belot dans son rapport sur l'avenir de la « ville intelligente »[327], il est nécessaire que soient élaborées des chartes d'utilisation avec les citoyens pour définir les modalités d'utilisation de leurs données, incluant l'open data élargi à des données de plus en plus sensibles. Le nouveau cadre juridique relatif à l'open data permet une meilleure prise en compte de la protection de la vie privée concernant la mise à disposition des données personnelles nominatives ou indirectement identifiantes et leur réutilisation. Pour accompagner cette démarche d'*open data*, la CNIL souhaite élaborer un pack de conformité spécifique[328].

Le DPO a vocation à jouer un rôle d'accompagnement au sein des comités de pilotage de l'open data pour s'assurer que la collectivité collecte, stocke, sécurise traite, exploite ces données en principe anonymisées et les met à la disposition des opérateurs privés dans le respect des droits des personnes. En termes de responsabilité, les enjeux sont réels pour les opérateurs privés : ceux-ci peuvent se voit confier en tant qu'opérateurs uniques, en charge de la conception et/ou de la mise en place du système intelligent, une masse de données de type « data lake » qui jusqu'à lors étaient externalisées au travers d'une multiplicité de contrats. Ceci va obliger les contrats publics à évoluer vers de nouveaux modes de contractualisation prenant de « contrats d'ensembliers » car en dépit de la dernière réforme du droit de la commande publique, la pratique montre que le droit des marchés publics et l'innovation ne fonctionnent pas forcément bien ensemble.

Il est intéressant d'observer certaines pratiques déjà adoptées à l'étranger. La ville de Seattle a mis en place un *Privacy Advisory Committee,* correspondant à un comité de gouvernance, d'éthique et de sécurité à vocation opérationnelle, chargé de suivre chacun des projets, de s'assurer de leur respect de la vie privée. Une équipe travaillant en complémentarité est spécifiquement chargée de

327. Rapport remis au premier Ministre le 18 avril 2017 - (Voir en ce sens rapport Belot, Proposition N°9) Chaque collectivité jouerait un rôle de tiers de confiance en adoptant une charte de protection des données.

328. Voir en ce sens, CNIL, bilan d'activité 2016, page 30.

la sécurité afin de parer les potentielles vulnérabilités ou cyberattaques. Il serait dès lors opportun d'expérimenter de nouveaux modes de régulation de la protection des données au travers d'organes de gouvernance dédiés ou existants à vocation plus large et les tester auprès des citoyens.

B. Les nouveaux défis du DPO dans le contexte des projets innovants tels que les *smart cities*

1. Devoir d'alerte en matière de prévention des risques liés aux risques d'atteinte à la vie privée

a. Nécessité d'anticiper le besoin de réalisation d'une analyse d'impact et les coûts associés

L'enjeu pour les porteurs de projet réside dans leur capacité à mettre en œuvre des services respectueux des droits des personnes, quelle que soit la complexité des systèmes. Bien que l'article 39 du RGPD prévoit qu'en matière d'analyse d'impact, le DPO « dispense des conseils, à la demande », il est impératif que les équipes projets associent le DPO dès la phase des POC (« Proof of concepts ») en amont des démarches d'innovation. Ceci ne va pas sans poser des difficultés car peu d'entreprises ont mis en place des procédures permettant de détecter la nécessité d'effectuer une analyse d'impact (« Privacy Impact Assessment » ou PIA) car il s'agit souvent de montants peu significatifs à ce stade[329]. Or dans le contexte de la smart city, la plupart des projets, même en phase embryonnaire, comportent un risque élevé pour les droits et les libertés des personnes.

Il est donc nécessaire, comme le recommande la CNIL, avant toute mise sur le marché de capteurs ou d'autres objets connectés, de réaliser une étude d'impact sur la vie privée afin de connaître les éventuels effets néfastes qu'ils pourraient provoquer sur celle-ci. Il serait opportun d'y associer des citoyens, de la même manière que ceux-ci sont associés aux débats sur les choix à opérer dans le cadre des études de diagnostic.

Les projets d'innovation urbaine doivent, comme tous projets d'innovation ou d'expérimentation, être suivis et évalués. L'étude d'impact apparaît comme doublement opportune car elle a vocation à être réitérée de manière à surveiller les risques dans la durée et à mesurer les impacts pour tenir compte des modifications du risque présenté par les opérations de traitement (article 35 *in fine*) liés aux développements des projets.

Un opérateur privé qui omettrait de prévoir la réalisation d'une étude d'impact rendue obligatoire par le RGPD s'exposerait à un manquement pour défaut d'identification du risque et de mise en œuvre des mesures destinées à atténuer ce risque. Un tel manquement serait doublé d'un manquement à l'obligation de consultation de l'autorité de contrôle prévue par l'article 36 préalablement aux traitements présentant un risque élevé[330]. L'autorité de contrôle serait dès lors privée (I) de la possibilité d'émettre un avis

329. Article 36, RGPD.

330. Article 32, RGPD.

écrit au responsable de traitement quant aux mesures et garanties envisagées et (II) de la possibilité d'adopter les éventuelles mesures correctrices destinées à mettre les traitements en conformité avec le règlement en vertu de l'article 58 du RGPD.

Le responsable de traitement s'exposerait alors à une amende administrative pouvant s'élever jusqu'à 10 M€ pour les personnes publiques ou jusqu'à 2 % du chiffre d'affaires mondial total de l'exercice précédent. Le fait d'avoir volontairement ou par négligence omis de réaliser une analyse d'impact pour obtenir des avantages financiers obtenus directement ou indirectement du fait de la violation pourrait constituer une circonstance aggravante en termes d'amendes administratives[331].

b. Nécessité de prise en compte du principe de « privacy by design »

Le développement de projets *smart city* implique de s'appuyer sur l'expérience et les attentes des citoyens dès la conception des services publics.

A ce titre, le DPO devra veiller à la prise en compte d'une autre avancée du règlement, la mise en pratique du *privacy by design*[332], visant à garantir que la protection de la vie privée soit intégrée dans les nouvelles applications technologiques et commerciales dès leur conception. Le DPO veillera à recommander la réalisation d'une analyse d'impact qui concourt à mieux appréhender cette exigence.

2. *Big Data* et protection des données : le DPO au cœur d'injonctions paradoxales

En apparence, il y a donc un conflit entre les principes informatique et libertés et ceux du Big Data qui se caractérise par la capacité à collecter un maximum de données, à les réutiliser et à les conserver aussi longtemps que possible, de manière parfois imperceptible pour l'individu. Cette logique basée sur des corrélations, des inférences et des prédictions contredit le principe de finalité repris par les articles 5(1)(b) et 6 du RGPD (les données personnelles doivent être collectées pour des finalités explicites, légitimes et spécifiques). Elles ne doivent pas faire l'objet d'un traitement ultérieur qui soit incompatible avec ces finalités. Par définition, ces finalités ne sont pas connues ou sont imprécises au moment où ces données sont collectées. D'où un risque de sanctions pénales et administratives en cas de violation de ce principe. De plus, le consentement éclairé ne peut être recueilli puisque d'une part, la finalité n'est pas définie et que d'autre part, la collecte souvent indirecte n'est pas connue des personnes concernées.

L'enjeu pour les responsables de traitement de la *smart city* est double : l'absence de transparence pour les citoyens qui peuvent être soumis à des décisions sur lesquelles ils n'ont aucun contrôle (d'où un risque de rejet des solutions mises en œuvre et de perte de confiance) et le risque associé à la privation d'exercice de leurs droits (il en résulterait alors un risque de collecte « déloyale » dénoncés régulièrement par la Cour de cassation et la CNIL).

Afin de concilier ces deux principes, le DPO encouragera les responsables de traitement à procéder à l'anonymisation préalable des données personnelles.

Par ailleurs, les responsables de traitement pourraient s'appuyer sur « l'intérêt légi-

331. Article 83 (2) (k), RGPD.

332. Considérant 78, RGPD.

time » pour démontrer que les traitements ne méconnaissent pas les libertés et droits fondamentaux de la personne concernée, sous réserve de conduire une évaluation des risques et de mettre en place des garanties appropriées telles que la pseudonymisation.

Une autre piste à explorer par le DPO consisterait à concevoir les projets de smart cities comportant un important volet Big Data comme poursuivant des finalités « statistiques ». « Les fins statistiques impliquent que le résultat du traitement à ces fins ne constitue pas des données à caractère personnel mais des données agrégées, et que ce résultat ou ces données à caractère personnel ne soient pas utilisés à l'appui de mesures ou de décisions concernant une personne physique en particulier »[333]. Les finalités statistiques ne s'adressent pas qu'aux entités publiques. Ces finalités sont expressément considérées comme compatibles avec la finalité initiale[334] et permettent de conserver les données plus longtemps[335]. En outre, la notion de finalité statistique n'est pas définie de façon restrictive et peut être interprétée largement, notamment par la loi nationale.

A delà des aspects juridiques liés à la protection des données, se pose des questions liées à l'éthique : le bénéfice des services attendus par les citoyens justifie-t-il que l'on rogne de plus en plus sur leur vie privée ?

La pérennité du business model des *smart cities* milite en faveur d'une politique d'innovation responsable et durable intégrant la protection des données. Il y a là de potentiels nouveaux gisements de valeur ajoutée pour les entreprises, à condition d'intégrer le coût de la conformité avec le RGPD en amont des projets.

A ce titre, les financeurs, publics ou privés, européens, nationaux ou locaux, conduits à soutenir ces démarches d'innovation urbaine devraient mieux prendre en considération cette nouvelle donne en mobilisant d'ores et déjà des capacités de financement supplémentaires.

En contrepartie, ils pourraient encourager la mise en place d'indicateurs permettant de mesurer le niveau de protection de la donnée tout au long de son cycle de vie des projets.

333. Considérant 162, RGPD.

334. Article 5, RGPD.

335. Considérants 50, 156, 162, RGPD : « *Le traitement ultérieur (...) à des fins statistiques devrait être considéré comme une opération de traitement licite compatible* ».

CLOUD ACT ET RGPD : QUELLE COMPATIBILITÉ ?

Julie MARTINEZ,
Enseignante, DU *Data Protection Officer* Paris II

« Une ingérence juridique jamais vue[336] » et même « un nouvel instrument de guerre économique renforçant l'ingérence des autorités américaines sur les prestataires de services de communications électroniques américains » : s'il a été possible de lire ces propos au sujet du *CLOUD Act,* c'est qu'il inquiète en France. Et pourtant, une étude plus approfondie de ses enjeux permet de nuancer les positions les plus radicales.

Le *Clarifying Lawful Overseas Use of Data Act*[337], également appelé *CLOUD Act,* est une loi américaine promulguée le 23 mars 2018 par le Président américain aux Etats-Unis permettant la simplification de l'accès par les autorités de poursuite américaines aux preuves électroniques détenues par des prestataires de services de cloud à l'étranger. Prenant de court l'entrée en vigueur du Règlement européen sur la protection des données[338] (« RGPD ») dans l'Union européenne – le 25 mai 2018 -, le *CLOUD Act* entend mettre un terme à une incertitude portée devant la Cour suprême des Etats-Unis dans le cadre de l'affaire Etats-Unis c. Microsoft[339].

Avant l'adoption surprise du *CLOUD Act,* une controverse avait émergé quant au fait de savoir si, en vertu du Stored Communications Act (« SCA »)[340], la communication de preuves électroniques lors du mandat d'autorités de poursuite américaines pouvait porter sur des données hébergées dans une autre juridiction que les Etats-Unis. Dans l'affaire Etats-Unis c. Microsoft[341], les autorités américaines avaient émis un mandat judiciaire au titre du SCA aux fins d'obtenir la communication de données liées à un compte de messageries électronique d'un client de Microsoft Corporation. Microsoft s'était exécuté concernant les informations relatives au client qui étaient hébergées sur le territoire américain. Cependant, et bien qu'étant en mesure technique de le faire, la société avait refusé de communiquer les contenus de la messagerie électronique qui étaient hébergés en Irlande puisque ces informations tombaient sous la protection des lois euro-

336. *Cloud Act, L'offensive américaine pour contrer le RGPD,* L. ACKERMAN : 22 juin 2018, www.portail-ie.fr dans R. BISMUTH, *Every Cloud has a Silver Lining - Une analyse contextualisée de l'extraterritorialité du Cloud Act,* La semaine juridique – Entreprises et Affaires - N° 40 - 4 octobre 2018, LEXISNEXIS, p.35.

337. *Clarifying Lawful Overseas Use of Data Act*, Consolidated Appropriations Act, 2018, §§2201-32.

338. 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 (règlement général sur la protection des données)

339. Pour l'opinion de la Cour suprême, *Etats-Unis c. Microsoft* (584 U. S), https ://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf, 2018.

340. Les *dispositions du Stored Communication Act* sont codifiées dans le Code pénal américain aux paragraphes 2701-2712 du Titre 18 de l'*U.S.C.* (le Code des Etats-Unis).

341. Sur cette affaire, V. R. J. Currie, Cross-Border Evidence Gathering in Trans- national Criminal Investigation : Is the Microsoft Ireland Case the "Next Frontier" ? : Canadian Yearbook of International Law, vol. 54, 2017, p. 63 et s. - T. Christakis, Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques : CEIS, The Chertoff Group, 2017, p. 18. - P. Jacob, Quand les nuages ne s'arrêtent pas aux frontières - Remarques sur l'application du droit dans l'espace nu- mérique à la lumière du Cloud Act : CDE 2018, dossier 28.

péennes et Irlandaises en matière de données personnelles. Microsoft avait aussi souligné qu'il ne pouvait être conféré une portée extraterritoriale au mandat. Le *CLOUD Act* est entré en vigueur avant que la Cour suprême n'ait pu statuer sur l'affaire au printemps, mettant ainsi fin à cette controverse : la localisation physique des données n'est pas un élément pertinent lorsqu'un juge américain émet un mandat de perquisition.

Contrairement à ce qui a pu être dit sur le sujet, l'administration de Donald Trump n'a pas modifié le SCA en vue de favoriser un espionnage massif des données de citoyens européens[342] – cette analyse serait bien trop alarmiste au regard du texte tel qu'il a été rédigé. Le *CLOUD Act* vise, dans le cadre d'une procédure judiciaire, à simplifier l'accès des autorités américaines aux preuves détenues dans d'autres juridictions. Pour ce faire, le CLOUD Act modifie le SCA afin d'exiger des prestataires de service de cloud la remise d'informations sur leurs clients qui sont « en leur possession, sous leur garde ou sous leur contrôle » et ce, quel que soit le lieu géographique où sont situées les preuves.

Entré en vigueur deux mois avant le RGPD, beaucoup de commentateurs y ont également vu une attaque directe à la souveraineté numérique européenne telle que récemment défendue par l'Europe sur la scène géopolitique internationale[343] et au respect du droit fondamental européen de la protection des données personnelles[344]. Le *CLOUD Act* ne peut être réduit à son seul dispositif extraterritorial. Loin des propos alarmistes à son sujet, il n'a pas été conçu dans l'optique d'offrir aux autorités américaines la possibilité illimitée d'obtenir les données personnelles européennes.

Il est vrai que le champ d'application du *CLOUD Act* interroge la compatibilité de celui-ci avec le RGPD (I). Le droit français et/ou européen offre cependant aux sociétés européennes des moyens juridiques efficaces pour s'opposer, si cela est opportun, à un mandat des autorités américaines fondé sur le CLOUD Act (II).

I. LE CHAMP D'APPLICATION DU *CLOUD ACT* SE HEURTE-IL AUX DISPOSITIONS DU RGPD ?

Tandis que le SCA était silencieux quant à la question de sa portée extraterritoriale, le *CLOUD Act* corrige cette ambiguïté (A) ce qui pose la question de sa compatibilité avec le RGPD européen puisque la divulgation d'informations personnelles aux autorités américaines portant sur des citoyens européens peut être un transfert de données à caractère personnel au sens du Règlement (B) et devrait être ainsi protégé comme tel.

342. *Le Cloud Act américain ne permet pas d'espionner les entre- prises européennes,* W. Maxwell : www.eurocloud.fr/le-cloud-act-americain-ne-permet- pas-despionner-les-entreprises-europeennes.

343. « *L'Europe : sujet ou objet de la géopolitique des données ?* », T. Gomart, J. Nocetti, C. Tonon, Études de l'Ifri, juillet 2018.

344. Article 8 « *Protection des données à caractère personnel* » de la Charte des Droits Fondamentaux de l'Union européenne, 2000/C 364/01, 2000.

A. L'extraterritorialité du *CLOUD Act*

Si le *CLOUD Act* interpelle autant les juristes, c'est parce qu'il dote la loi américaine d'une portée extraterritoriale.

Le paragraphe 2713 du Titre 18 du Code des Etats-Unis (U.S.C.) accorde une portée extraterritoriale aux mandats judiciaires fondés sur le *CLOUD Act,* en disposant qu'un « prestataire de service de communications électroniques ou de service informatique à distance se conformera aux obligations de préserver, sauvegarder ou divulguer les contenus d'une communication filaire ou électronique ainsi que tout enregistrement ou toute autre information portant sur un client ou abonné en possession, sous la garde ou sous le contrôle dudit prestataire, que ladite communication, ledit fichier ou toute autre information, soit situé/e aux Etats-Unis ou en dehors des Etats-Unis ». Tout manquement à cette disposition pourra être caractérisé d'outrage à la justice (contempt of court).

Le paragraphe 2713 précise que le mandat ordonnant la divulgation de données de clients et d'abonnés peut concerner les sociétés affiliées de prestataires de services de cloud dont le siège se situerait à l'étranger dès lors que les informations en jeu sont « en possession, sous la garde ou sous le contrôle » de la société affiliée. S'il est simple de déterminer la possession physique en matière de données, il est plus compliqué de comprendre ce que le *CLOUD Act* entend par l'expression « sous la garde ou sous le contrôle ». Bien que les tribunaux américains n'aient pas statué sur cette question précise à la lumière du *CLOUD Act,* il est utile de considérer ici l'analyse du terme « contrôle » par un tribunal fédéral de l'état de New York dans la situation similaire d'une relation mère/filiale. Les juges ont en l'espèce tenu compte de quatre facteurs factuels différents : « le degré de possession et de contrôle que la société mère exerce sur la filiale », « une indication que les deux entités fonctionnent comme une entité unique », « un accès démontré aux documents dans le cadre habituel des activités », et « une relation de représentation »[345]. Ainsi, l'enjeu pour les autorités américaines sera de déterminer dans chaque situation si les données sont en possession ou sous le contrôle du prestataire pour donner pleinement effet à la portée extraterritoriale du *CLOUD Act*. Au niveau européen, en revanche, le débat se situe ailleurs.

B. La divulgation d'informations personnelles aux autorités américaines est un transfert de données vers des pays tiers au sens du RGPD

Les traitements de données personnelles mis en œuvre par les prestataires de service de cloud effectués dans le cadre d'activités exercées par des établissements implantés sur le territoire de l'Union européenne, ou qui portent sur des personnes se trouvant sur le territoire de l'Union européenne, sont soumis au respect des dispositions du RGPD, en vertu de son article 3. Dès lors que les autorités américaines ordonnent le transfert de données à caractère personnel en application du *CLOUD Act,* cette demande est en effet un « traitement » au sens du RGPD et peut ainsi entrer en conflit avec les dispositions du chapitre 5 du Règlement portant sur les transferts de données vers des pays tiers.

345. *Huang c. ITV Media, Inc. Et al*, n°2013 CV 03439, Tribunal fédéral de première instance du District Est de New York, 2017.

Plus particulièrement, l'article 48 du RGPD qui dispose que « toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre » peut soulever la question de la compatibilité du *CLOUD Act* avec une telle disposition.

L'article 48 du RGPD peut conduire à deux interprétations différentes quant à l'efficacité des mandats pris sur le fondement du *CLOUD Act* dans l'Union européenne.

La première interprétation consiste à affirmer que, même si les décisions de juridictions ou d'autorités administratives des Etats-Unis qui ne seraient pas fondées sur un accord international, tel qu'un traité d'entraide judiciaire, pourraient faire obstacle à la protection des personnes physiques garantie dans l'Union européenne par le RGPD, il semblerait pourtant possible d'outrepasser cet obstacle en vertu « d'autres motifs de transfert en vertu du présent chapitre » - de sorte que le *CLOUD Act* et le RGPD pourraient in fine être compatibles. C'est l'argumentation reprise par la Commission européenne dans son Amicus Curiae[346] porté devant la Cour suprême dans l'affaire Etats-Unis c. Microsoft. Elle souligne que le RGPD peut tolérer des transferts de données pris notamment sur le fondement de l'intérêt public ou de l'intérêt légitime de sorte que l'article 48 ne serait pas un obstacle infranchissable à l'applicabilité du *CLOUD Act.*

Cette compréhension de l'article 48 du RGPD s'oppose à celle selon laquelle, à défaut d'accord exécutif entre les Etats-Unis et l'Union européenne (ou ses membres), il est possible aux prestataires de services de cloud de s'opposer aux demandes des autorités américaines fondées sur le *CLOUD Act.* C'est en effet ce que soutient le Groupe de travail de l'Article 29, aujourd'hui remplacé par le Comité européen de la protection des données (« CEPD ») qui dans ses lignes directrices[347] favorise la voie des traités d'entraide judiciaire lorsqu'il s'agit de devoir communiquer des données personnelles dans le cadre de mandats judiciaires à l'initiative de pays tiers : « la législation de l'UE en matière de protection des données prévoit que les lois internationales existantes en la matière, tels que les traités d'entraide judiciaire, doivent – en règle générale – être respectés lorsque les autorités de pays tiers demandent au responsable du traitement des données de l'UE d'accéder aux données ou de les divulguer. Le contournement de ces traités existants ou d'autres bases juridiques applicables en vertu du droit de l'UE par le droit d'un pays tiers est donc une ingérence dans la souveraineté territoriale d'un membre de l'UE ».

Cette position permet d'affirmer que tout transfert de données réalisé en vertu d'un mandat judiciaire américain fondé sur le *CLOUD Act* ne peut être autorisé que sur le fondement d'un accord international. Le CEPD a très clairement précisé que s'il existe « un accord international, tel qu'un traité d'entraide juridique », ce qui est le cas, « les entreprises européennes doivent généralement refuser les demandes directes et référer l'autorité requérante du pays tiers vers les traités d'entraides judiciaire ou les accords existants ». Si le *CLOUD Act* prévoit par ailleurs un mécanisme juridique par lequel les Etats-Unis peuvent conclure des « accords exécutifs » avec d'autres Etats, il n'en existe cependant aucun à ce jour entre les Etats-Unis et l'Union européenne et/ou la France. Cette seconde interprétation permettrait ainsi aux entreprises européennes de s'opposer à une demande émanant des autorités américaines puisque la communication de ces données constituerait un transfert non autorisé vers un pays tiers susceptible d'exposer le prestataire de services de cloud aux sanctions du RGPD.

346. Commission européenne, Amicus Curiae, Etats-Unis c. Microsoft, n°17-2 (2nd cir 2017).

347. Lignes Directrices 2/2018 du CEPD concernant les dérogations de l'article 49 du RGPD, 25 mai 2018.

Au regard de ces deux interprétations, une position officielle des autorités concernées telles que la CNIL et le CEPD se fait attendre. Le Procureur Général du Ministère de la Justice américain a lui-même soulevé des interrogations concernant la compatibilité du *CLOUD Act* avec le RGPD dans un rapport récent en énonçant que « des questions et incertitudes significatives existent encore concernant le RGPD, ce qui pourrait négativement impacter le travail des autorités de poursuite, en ce compris en empêchant le partage des informations »[348].

II. QUELS MOYENS JURIDIQUES EFFICACES PEUVENT S'OPPOSER À UN MANDAT FONDÉ SUR LE *CLOUD ACT* ?

Puisqu'avec l'entrée en vigueur du RGPD, beaucoup d'entreprises internationales ont investi dans une gestion des données plus protectrice des individus, et que l'interprétation de l'article 48 n'est toujours pas tranchée, la question du transfert de données personnelles aux autorités américaines – et ce, en potentielle contradiction avec le Règlement - est une question délicate pour ces sociétés.

A. La demande en modification ou annulation du mandat exigeant des données relatives à un abonné ou un client

Le *CLOUD Act* prévoit qu'un prestataire de services de cloud peut agir en modification ou annulation du mandat « si les informations ou fichiers demandé(s) sont par nature inhabituellement volumineux, ou si la conformité à ladite ordonnance est susceptible d'imposer une charge injustifiée audit prestataire ».

Les conditions d'opposition aux mandats émis par les autorités américaines différeront selon que les Etats-Unis ont conclu un accord exécutif ou non avec la France. Le *CLOUD Act* crée en effet un mécanisme juridique permettant aux Etats-Unis de conclure des accords bilatéraux avec d'autres Etats, afin que les Etats parties à cet accord puissent obtenir plus rapidement la communication de données à caractère criminel et terroriste. Si un tel accord devait être conclu avec la France, (ce qui semble peu probable), les prestataires de services de cloud devront soulever une exception légale par le biais d'une requête en annulation ou modification dans un délai de 14 jours à partir de la date de réception de la demande de communication des données[349] si le respect des dispositions du *CLOUD Act* a pour effet (1) que le prestataire se mette en situation de violer le droit de l'État étranger ; ou si (2) l'intérêt de la justice (« the interests of justice ») exige justement d'annuler ou de modifier la demande des autorités ; et (3) si le prestataire concerné n'est pas une personne américaine et ne réside pas aux Etats-Unis[350]. Si aucun accord exécutif n'est pris, le prestataire de service pourra soulever le fondement de Common Law de « courtoisie internationale », uniquement en défense, afin d'inciter les juridictions américaines à prendre en compte les lois françaises et

348. *Report of the attorney general's cyber digital task force*, U.S., Department of Justice, 2 Juillet 2018, page 127 et suivantes.

349. CLOUD Act, 18 U.S.C. § 2703 (h)(2)(II).

350. CLOUD Act, 18 U.S.C. § 2703 (h)(2)(B).

les intérêts des citoyens français (tel qu'il est développé plus bas au point B).

Puisqu'il est possible qu'une entreprise n'ait pas connaissance d'une demande soumise par les autorités américaines aux prestataires de service de cloud, et puisque il revient à ces derniers de déposer la demande en annulation ou modification, il apparait important que chaque société choisisse ses prestataires en établissant contractuellement au préalable la position des prestataires de services à adopter eu égard aux demandes d'accès.

B. Les moyens juridiques opposables

S'il est possible d'agir en modification ou annulation d'un mandat fondé sur le *CLOUD Act,* il est utile d'analyser les fondements juridiques opposables au soutien d'une modification ou annulation de tels mandats.

L'extraterritorialité du CLOUD Act est susceptible d'avoir une incidence négative sur les lois d'autres pays (en l'occurrence, le RGPD tel qu'il a modifié par la loi Informatique et Liberté[351]). Ainsi, les tribunaux américains, en application de l'analyse de courtoisie internationale (dite comity analysis), devront tenir compte à la fois du devoir international et des convenances mais aussi des droits des citoyens ou des autres personnes qui sont protégées par les lois du pays dans lequel s'applique ladite législation américaine. En application de ce principe, les juridictions américaines devront prendre en considération le risque réel de poursuites à l'encontre des prestataires de services de cloud qui seront à l'origine de la communication des informations, dans leurs pays. Le quantum des peines est par exemple un élément important pris en compte par les juges. Le *CLOUD Act* mentionne lui-même les huit éléments clef devant être pris en considération par les juges : (1) les intérêts des Etats-Unis, y compris ceux de l'autorité américaine sollicitant l'information ; (2) les intérêts de l'État étranger au non-dévoilement de l'information ; (3) la probabilité, l'ampleur et la nature des sanctions auxquelles s'exposent les prestataires ou leurs employés ; (4) la localisation et la nationalité de la personne dont les données sont sollicitées ainsi que l'ampleur et la nature de ses liens avec les Etats-Unis et l'Etat étranger ; (5) l'ampleur et la nature des liens et de la présence du prestataire avec les Etats-Unis ; (6) l'importance de l'information sollicitée pour les investigations ; (7) la possibilité d'obtenir l'information par des moyens qui seraient moins dommageables ; (8) et, cas plus particulier, les intérêts de l'autorité d'un état tiers qui a sollicité les informations auprès des Etats-Unis dans le cadre de la coopération internationale en matière pénale[352].

A défaut d'accord exécutif, l'article 48 et le considérant 115 du RGPD pourraient être soulevés par des prestataires de services de cloud français pour s'opposer à une demande de communication de données personnelles vers les Etats-Unis. Le RGPD a considérablement augmenté le quantum des amendes susceptibles d'être prononcées, ces dernières pouvant être portées à 4 % du chiffre d'affaires mondial ou 20 millions d'euros[353], de sorte que les juridictions américaines pourraient en tenir compte dans le cadre de la comity analysis. Le quantum de la sanction concrétise en effet ces risques de conflits d'obligations entre le *Cloud Act* et le RGPD. Encore faut-il que les prestataires de services de cloud s'emploient à contester ces demandes si celles-ci s'avèrent contraires au droit de l'Union européenne. Puisqu'une incertitude pèse cependant toujours quant à l'interprétation de l'article 48, l'efficacité de ce moyen juridique dépendra bien évidemment de la position publique qu'adopteront les autorités pertinentes en la matière, telle que la CNIL et le CEPD.

351. Loi Informatique et Liberté, n° 2018-493 du 20 juin 2018.

352. CLOUD Act, 18 U.S.C. § 2703 (h)(3), tel qu'analysé par R. Bismuth, précité – note 362.

353. RGPD, article 83(5).

Il faut également souligner que d'autres lois françaises ou européennes existantes peuvent faire obstacle à un mandat des autorités américaines fondé sur le *CLOUD Act.*

La Loi dite de blocage[354] énonce par exemple la double interdiction de (I) communiquer des données de nature à porter atteinte à la souveraineté, sécurité ou intérêts économiques essentiels de la France ou à l'ordre public[355] ; et (II) de communiquer des données tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères[356] (sous réserve de traités ou accords internationaux, lois et règlements en vigueur). Cette double interdiction est pénalement sanctionnée d'un emprisonnement de six mois et d'une amende de 18.000 euros pour les personnes physiques et de 90.000 euros pour les personnes morales, de sorte que les juridictions américaines devraient en tenir compte[357]. En pratique, les juridictions américaines n'accordent que peu de crédit à la loi de blocage français, l'argument premier des juges américains étant que les juridictions françaises ne condamnent que rarement la violation des dispositions issues de la loi de blocage. Le gouvernement français envisage cependant de procéder à une modernisation de cette loi pour pallier aux arguments américains sur l'inapplicabilité du quantum de peines dans les juridictions françaises.

La loi relative à la protection du secret des affaires[358], transposant la directive sur la protection des savoir-faire et des informations commerciales non divulguées, serait également opposable lorsque des données couvertes par le secret d'affaire feraient l'objet d'une demande des autorités américaines fondée sur le *CLOUD Act.* En effet, le nouvel article L.152-1 sanctionne l'atteinte au secret d'affaire par l'engagement de la responsabilité civile de la personne qui est à l'initiative de la violation.

Pour finir, il est intéressant de noter le repositionnement de l'Union européenne sur la scène géopolitique internationale avec le projet législatif intitulé « E-evidence »[359] présenté le 7 avril 2018. Véritable pendant européen du *CLOUD Act,* ce projet de Règlement a également pour objectif de faciliter l'accès des autorités policières et judiciaires des Etats membres aux preuves électroniques et ce, quelque soit leur géolocalisation.

Conclusion

En tout état de cause, bien que le champ d'application du *CLOUD Act* interroge la compatibilité de celui-ci avec le RGPD, le droit français et/ou européen offre aux sociétés européennes des moyens juridiques efficaces pour s'opposer aux mandats des autorités américaines fondés sur le *CLOUD Act.* Le droit fondamental européen à la protection des données personnelles ne saurait ainsi souffrir d'une ingérence – prétendue ou non – américaine.

354. Loi n°68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

355. Loi n°68-678 précitée, Article 1.

356. Loi n°68-678 précitée, Article 3.

357. Cet argument est par exemple avancé dans l'affaire *Société Nationale Industrielle Aérospatiale v. U.S District Court for the Southern District of Iowa*, 482 U.S. 522 (1987).

358. Loi n°2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, publiée au journal officiel le 31 juillet 2018.

359. Proposition de Règlement du Parlement européen et du Conseil du 17 avril 2018, établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénales, COM (2018) 226 final.

UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

12 place du Panthéon 75005 Paris
www.u-paris2.fr

#UP2PA 2019 Service de la communication