Association nationale des Auditeurs jeunes de l'Institut des Hautes Etudes de Défense nationale

Première association française de jeunes sur les problématiques de défense et de sécurité

# LE RGPD, OU COMMENT RÉGULER LE MARCHÉ DES DONNÉES POUR DÉVELOPPER LA PUISSANCE NORMATIVE DE L'UNION EUROPÉENNE

COMITÉ : Comité Défense Économique & Comité Cyberdéfense – ANAJ-IHEDN



Le règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement Général sur la Protection des Données, RGPD), est entré en vigueur dans les vingt-sept États de l'Union européenne le 25 mai 2018. Il s'applique à tous les responsables de traitement de données personnelles de citoyens européens, que ceux-ci soient établis en Europe ou non.

Le RGPD a fait l'objet d'une grande médiatisation car il met à jour le rapport entre progrès technique et enjeux économiques et sociaux. Le règlement induit pour les institutions privées et publiques de nombreuses obligations, révisées ou nouvelles, qui visent la protection des données à caractère personnel des citoyens de l'Union européenne.

Les conséquences de l'entrée en vigueur du RGPD ne seront perceptibles qu'à moyen ou long terme. Il s'agit de mettre en place un arsenal technique et juridique qui prenne en compte les évolutions passées et anticipe l'avenir dans le domaine de l'économie numérique.

Dans une approche de défense économique et de cybersécurité, cette série de trois publications a pour objectif de comprendre la nouvelle réglementation à la lumière des grands enjeux de ce qui pourrait être une guerre économique 2.0. Le RGPD résulte d'un constat unanime : l'importance de la donnée dans le monde économique contemporain. Il donne des droits aux citoyens et responsabilise les acteurs du traitement de données (i). Cette réglementation est un outil de développement de la puissance normative de l'Union européenne (ii) et marque une nouvelle forme de guerre économique (iii).

Le RGPD s'inscrit dans une dynamique de globalisation du droit et des pratiques des organisations. Il s'agit de sensibiliser mondialement à la protection des données. Le RGPD oblige les organisations étrangères et notamment les entreprises, à se conformer à la loi européenne à partir du moment où elles utilisent des données de ressortissants européens. A cet égard, maîtres Emmanuel Daoudet et Hugo Partouche soutiennent que « le développement d'une responsabilité internationale de l'entreprise est le principal point commun aux chantiers de *compliance* » dans lesquels le RGPD s'inscrit[1]. La responsabilité juridique des entreprises (en ce qu'elles ont une personnalité juridique, et sont à ce titre justiciables) est en effet au cœur de la prise en

[1] « Loi Sapin II, RGPD et loi Vigilance : enjeux internationaux de la compliance », Emmanuel Daoud et Hugo Partouche, Revue Lamy droit des affaires, N° 136, 1er avril 2018 [en ligne], URL : https://lamyline-lamy-fr.bibliopum.u-paris2.fr/Content/DocumentNew.aspx?params=H4sIAAAAAAAAAEAE3PwWqEMBAG4KdpjiWutu4eclhXKIWlLNb2PppBw6ZJm4xZffuOK4UePhiSn8yfnwnD0uJMqnm51CIuzrvlS7VhQkHQRZVJ-VD2q4ztWM4K9sSeWcn27LA6COhpAlv7Xu3X2SRsoVOZ8EFjqBYlBXkC22BUOyni6G9vkMwAZLyrIGyrjdaqbqWUuczLvChEwhA5oD7NgI5QjGYYz4y2fEQL_XiBAVWDacL4CPF7FtZducj7_XILJoM3ZZzG-QRBH51e_y5M_HBcNIL9n90erSYiXtyR2-6O1ore8lgD4QksOv3XGpI3-uxBv3I23vuu579GMGSZZAEAAA==WKE

compte du comportement de celles-ci par les États. La personnalité juridique des entreprises permet aux gouvernements de sortir de leurs frontières pour appliquer leur loi à ces personnes morales, et pour les sanctionner pénalement le cas échéant.

Le retrait récent des États-Unis de l'accord iranien sur le nucléaire a permis à son gouvernement de faire peser la menace de sanctions économiques sur les entreprises européennes présentes en Iran grâce à une législation extraterritoriale. Ces entreprises risquent en effet d'être sanctionnées à cause des relations commerciales qu'elles entretiennent avec un État jugé dangereux par les États-Unis.

Le président de la Commission des affaires européennes, Jean Bizet, déclarait à ce sujet que « la mise en cause systématique, croissante et généralisée du multilatéralisme par l'administration américaine doit désormais conduire l'Union européenne à défendre, de façon unie et ferme, sa souveraineté diplomatique et économique ainsi que les organisations multilatérales qui régissent les relations entre États ».[2]

C'est dans ce contexte de tensions que l'extraterritorialité du RGPD est à considérer comme un outil économique et diplomatique au service de l'Union européenne.

**Extraterritorial** : [Droit constitutionnel / Droit international public] Se dit des lois et actes nationaux susceptibles d'être appliqués à des comportements ou des situations sis hors du territoire de l'État dans lesquels ils sont adoptés.

## L'EXTRATERRITORIALITÉ DU RGPD : VERS UNE GOUVERNANCE MONDIALE DES DONNÉES ?

Le RGPD est d'application extraterritoriale : il permet aux autorités publiques européennes de contrôler et sanctionner des entreprises ou autorités étrangères. Plus encore, il impose aux entreprises européennes ou responsables du traitement de données européennes des outils spécifiques, notamment pour pouvoir transférer des données en dehors du territoire de l'UE.

« En matière de transferts hors de l'Union, le responsable de traitement peut être tenu de déployer des outils spécifiques tels que les règles internes d'entreprise ou les clauses types adoptées par la Commission. Ces outils ne sont pas nouveaux mais ils ont été renforcés par l'adoption du RGPD qui inclut également un mécanisme de certification ou la possibilité de se doter d'un code de conduite »[3].

Les Règles Contraignantes d'Entreprise (BCR pour *Binding Corporate Rules*) constituent un « code de conduite, définissant la politique d'une entreprise en matière de transferts de données personnelles. Les BCR permettent d'offrir une protection adéquate aux données transférées depuis l'Union européenne vers des pays tiers à l'Union européenne au sein d'une même entreprise ou d'un même groupe.[4] »

Grâce à la mise en place de différents mécanismes, tels que les codes de conduite ou les règles internes d'entreprises, le RGPD a donc un champ d'application très large qui s'étend bien au-delà des frontières de l'UE. Pour asseoir le caractère extraterritorial de ce règlement, l'article 3 du RGPD identifie la *data* européenne comme lien de rattachement principal entre le responsable de traitement et la législation européenne. Les débats juridiques concernant l'extraterritorialité du RGPD se sont notamment cristallisés dans le contentieux *Google Spain*.

L'affaire *Google Spain* (affaire C-131/12)[5] a suscité plusieurs controverses, parmi lesquelles celle de l'extraterritorialité du droit de l'UE. La Cour de Justice de l'Union Européenne (CJUE) devait, pour pouvoir faire valoir le droit à l'oubli d'un citoyen européen face à *Google*, appliquer une norme européenne à un

---

[2] « Face à l'extraterritorialité des lois américaines, l'Union européenne doit sécuriser ses entreprises et ses marchés internationaux », communiqué de presse du Sénat, Lundi 14 mai 2018 [ en ligne ], URL : **http://www.senat.fr/presse/cp20180514.html**

[3] « Loi Sapin II, RGPD et loi Vigilance : enjeux internationaux de la compliance », Emmanuel Daoud et Hugo Partouche, Revue Lamy droit des affaires, N° 136, 1er avril 2018 [en ligne], URL : https://lamyline-lamy-fr.bibliopum.u-paris2.fr/Content/DocumentNew.aspx?params=H4sIAAAAAAAAAEAE3PwWqEMBAG4KdpjiWutu4eclhXKIWlLNb2PppBw6ZJm4xZffuOK4UePhiSn8yfnwnD0uJMqnm51CIuzrvlS7VhQkHQRZVJ-VD2q4ztWM4K9sSeWcn27LA6COhpAlv7Xu3X2SRsoVQZ8EFjqBYlBXkC22BUOyni6G9vkMwAZLyrIGyrjdaqbqWUuczLvChEwhA5oD7NgI5QjGYYz4y2fEQL_XiBAVWDacL4CPF7FtZducj7_XILJoM3ZZzG-QRBH51e_y5M_HBcNIL9n90erSYiXtyR2-6O1ore8lgD4QksOv3XGpI3-uxBv3I23yuu579GMGSZZAEAAA==WKE

[4] « Les BCR (règles internes d'entreprises) » in CNIL [en ligne], URL : https://www.cnil.fr/fr/les-bcr-regles-internes-dentreprise

[5] Affaire C-131/12, dans Recueil de la jurisprudence, arrêt de la Cour de Justice de l'Union européenne, Grande Chambre, le 13 mai 2014, [en ligne], URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62012CJ0131&from=FR

groupe dont la société mère est établie aux États-Unis. Tandis que la directive alors en vigueur (directive 95/46)[6] prévoit trois liens de rattachement pour l'application du droit de l'UE à des entreprises étrangères, la CJUE fait une interprétation extensive pour condamner la société américaine : « dont l'activité vise les habitants de cet État membre »[7]. Cette interprétation extensive est justifiée par une approche téléologique[8] qui permet à la CJUE d'imposer le droit européen à une entreprise américaine, au nom du respect des droits fondamentaux des Européens : « l'objectif de la directive 95/46 [est] d'assurer une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée, à l'égard du traitement des données à caractère personnel, cette dernière expression ne saurait recevoir une interprétation restrictive » *(*cons. 53 aff C-131/12*)*[9].

Le RGPD vise à protéger les données des citoyens européens et à cet égard le lieu d'établissement du responsable de traitement et le lieu du traitement sont indifférents. Cette interprétation de la CJUE fait de la mise en cause d'un droit fondamental le lien de rattachement principal du RGPD.

L'article 3 du règlement codifie cette jurisprudence et confère à la législation européenne un champ territorial des plus étendus.

**Article 3 RGPD Champ d'application territorial** :

**« 1**. **Le présent règlement s'applique** au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, **que le traitement ait lieu ou non dans l'Union**.

**2**. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un **responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union**, lorsque les activités de traitement sont liées :

**a)** à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou

**b)** au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

**3**. **Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public**. »

Le RGPD est un outil de développement de la puissance normative de l'UE. Par la mise en conformité des entreprises multinationales, et par l'extension de la compétence territoriale des autorités européennes, le règlement promeut une culture européenne de protection des droits fondamentaux.

Cette influence normative croissante de l'UE s'est fait sentir lors de la récente audition de Mark Zukerberg devant le Congrès américain concernant l'affaire *Cambridge Analytica*. Le PDG de Facebook a convenu à cette occasion que « Tout le monde sur la planète à le droit au respect de sa vie privé […] J'imagine que les choses seraient un peu différentes aux États-Unis, où nous avons une sensibilité qui n'est pas la même, mais nous voulons mettre en place partout dans le monde le "consentement éclairé" et d'autres choses qui sont contenus dans le RGPD. »[10]. Plus encore, la rencontre entre le PDG de *Facebook* (370

---

[6] 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 [en ligne], URL : http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[7] Affaire C-131/12, dans Recueil de la jurisprudence, arrêt de la Cour de Justice de l'Union européenne, Grande Chambre, le 13 mai 2014, [en ligne], URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62012CJ0131&from=FR

[8] Une approche téléologique renvoie à l'interprétation, par le juge, d'une norme en fonction de son but et de la finalité qu'elle poursuit.

[9] Affaire C-131/12, dans Recueil de la jurisprudence, arrêt de la Cour de Justice de l'Union européenne, Grande Chambre, le 13 mai 2014, [en ligne], URL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62012CJ0131&from=FR

[10] « Audition du PDG de Facebook, Mark Zuckerberg : une discrète revanche pour l'Europe », Alexandre Picquard in Le Monde, 11/04/2018 [en ligne], URL : http://www.lemonde.fr/pixels/article/2018/04/11/audition-de-mark-zuckerberg-une-discrete-revanche-de-l-europe_5283962_4408996.html#JH4MSxD8t8ySYFVq.99

millions d'inscrits en Europe) et le Parlement européen le 22 mai 2018 autour de ce scandale témoigne de l'urgence de la mise en conformité des multinationales avec la réglementation européenne.[11]

Au jour de l'entrée en vigueur du règlement, la vision européenne de la vie privée et la politique de régulation ambitieuse de l'Union européenne sur le marché de la *data* sont confortées par une opinion publique sensibilisée à ces questions et soucieuse de l'utilisation faite des données personnelles. Le RGPD est un tour de force qui a des chances d'aboutir à un renforcement de la puissance normative de l'Union européenne.

## ENTRE PROCÉDURES D'ADÉQUATION ET NÉGOCIATIONS INTERNATIONALES : LE RGPD COMME OUTIL DIPLOMATIQUE

La nouvelle législation européenne sur la protection des données renforce la protection des données européennes en encadrant encore davantage leur transfert en dehors de l'UE. Cette forme de « protectionnisme digital » a suscité des critiques, étant entendu que d'un point de vue concurrentiel, l'UE manque de géants du numériques pour rivaliser avec les GAFAM (*Google, Apple, Facebook, Amazon, Microsoft*) américains ou les BATX (*Baidu, Alibaba, Tencent* et *Xiaomi*) chinois. Ainsi, le Chapitre V du RGPD concerne les « transfert de données vers des pays tiers ou organisations internationales ».

L'un des moyens classiques pour transférer des données de l'UE vers des pays tiers est la décision d'adéquation, dont l'article 45-1 du RGPD précise la teneur.

> Article 45-1 du RGPD : « Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat ».

Le renforcement du contrôle de la Commission européenne du niveau de protection des données à l'extérieur de l'UE intervient dans un contexte où l'obtention de données de citoyens est un moyen de pouvoir économique et politique. Peu à peu, les contours d'une forme de conflit numérique se dessinent.

L'affaire Schrems est à cet égard particulièrement intéressante. Après les révélations de M. Edward Snowden sur les activités de la *National Security Agency* (NSA) et les pratiques des États-Unis en matière de surveillance, un Autrichien, M. Schrems, a souhaité interdire à *Facebook Ireland* de transférer ses données à caractère personnel vers les États-Unis, siège social de *Facebook*. La Commission européenne avait pourtant reconnu les États-Unis comme étant une "zone de sécurité" pour les données personnelles des Européens par sa décision 2000/520. Le *Safe Harbor* est un « ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux États-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne. Ces principes, négociés entre les autorités américaines et la Commission européenne en 2001, sont essentiellement basés sur ceux de la directive 95/46 du 24 octobre 1995 »[12]. On comprend à travers cette définition que l'adhésion volontaire à ces principes ne présente pas ou peu de caractère contraignant pour les entreprises qui ne sont par ailleurs pas soumises à contrôle.

L'affaire Schrems a été l'occasion pour la CJUE d'examiner la décision d'adéquation passée entre la Commission et les États-Unis lors de la signature du *Safe Harbor*. L'avocat Général Yves Bot, dont la CJUE suivra l'avis, estime que la législation américaine ne garantit pas suffisamment la protection des droits fondamentaux protégés par la Charte des Droits Fondamentaux de l'Union Européenne (CDFUE) : « Une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée »[13].

---

[11] « Zuckerberg sera auditionné par le Parlement européen », in Sciences et Avenir avec Reuters, **17.05.2018** [ en ligne], URL : **https://www.sciencesetavenir.fr/high-tech/web/mark-zuckerberg-sera-auditionne-par-le-parlement-europeen_123989**

[12] « Le Safe Harbor », CNIL [en ligne], URL : https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf

[13] Conclusions de l'Avocat Général Mr Yves Bot, présentées le 23 septembre 2015 Affaire C362/14 Maximillian Schrems contre Data Protection Commissioner dans demande de décision préjudicielle formée par la Haute Cour de justice irlandaise. [en ligne], URL : http://curia.europa.eu/juris/document/document.jsf?docid=168421&doclang=FR

Dans cette affaire, la Commission, dans ses observations avait constaté que « [l]les révélations en question font apparaître un degré de surveillance indifférenciée à grande échelle qui n'est pas compatible avec le critère de nécessité prévu dans cette exemption ni, de manière plus générale, avec le droit à la protection des données à caractère personnel consacré à l'article 8 de la Charte ».

La CJUE a finalement invalidé la décision d'adéquation de la Commission européenne et a donc permis à Mr Schrems de voir sa demande visant à interdire le transfert de ses données aux États-Unis examinée par l'autorité nationale de protection irlandaise.

L'impact de cette affaire est considérable puisque les États-Unis se sont vus contraints de négocier un nouvel accord d'adéquation avec les exigences européennes en matière de protection des données. Ces négociations ont conduit à l'adoption d'un « Bouclier de protection des données UE – États-Unis » en 2016 dit « *Privacy Shield* ». Ce mécanisme d'auto-certification considéré comme suffisamment protecteur pour les données personnelles en provenance de l'UE, a été créé pour les entreprises établies aux États-Unis[14]. Malgré ce nouvel accord d'adéquation, des nouvelles voix s'élèvent pour dénoncer l'insuffisance de la protection des données européennes lorsque celles-ci sont transférées aux États-Unis.

Ces questions sont d'autant plus sensibles qu'au-delà des intérêts commerciaux, les flux de données sont un élément essentiel dans les opérations de sécurité et de maintien de la paix. Tandis que l'affaire Schrems soulève essentiellement des questions juridiques, « l'affaire *Microsoft* » soulève quant à elle des questions relatives à la lutte contre le terrorisme :

*Microsoft*, entreprise de nationalité américaine, possède les données de citoyens européens domiciliés en Europe. En 2013, la justice américaine réclame à l'entreprise les e-mails d'un Irlandais soupçonné de trafic de drogue. *Microsoft* refuse puisque ces e-mails sont hébergés sur des serveurs situés en Irlande, et que le gouvernement américain n'est pas passé par une procédure classique de coopération judiciaire internationale. Le gouvernement américain peut-il réclamer des données à une entreprise américaine sans recourir à la coopération judiciaire avec les autorités européennes lorsque ces données concernent des Européens et sont hébergées en Europe ? L'affaire est pendante devant la Cour Suprême des États-Unis.

Les données personnelles sont un objet de crispation entre les États-Unis et l'UE, notamment compte tenu de la nationalité américaine des GAFAMs, et du marché européen des données, attractif pour ces entreprises. Dans une résolution du 6 avril 2017[15] sur l'adéquation de la protection offerte par le bouclier de protection des données UE – États-Unis, le Parlement européen exprime encore beaucoup de réserves sur la suffisance de la protection des données outre-Atlantique. Les récentes affaires qui traversent le continent Nord-Américain confortent la position européenne en faveur d'une protection plus forte.

Entre mécanisme juridique et négociations internationales, les décisions d'adéquations sont hybrides. Elles témoignent de la complexification des rapports entre États, entreprises et citoyens.

En renforçant le recours aux décisions d'adéquations, le RGPD enjoint les pays tiers à repenser leur propre système de protection des données personnelles. Ainsi, dans son avis du 10 octobre 2017 sur la protection des données personnelles, le Conseil Économique et Social Européen « se félicite du dialogue engagé par la Commission avec ses principaux partenaires commerciaux en Asie de l'Est et du Sud-Est, y compris le Japon et la Corée, et éventuellement l'Inde, ainsi qu'avec les pays d'Amérique latine et les pays couverts par la politique européenne de voisinage, qui ont exprimé un intérêt en faveur de l'obtention d'un "constat d'adéquation" »[16]. Le Proche Orient et l'Afrique du Nord sont aussi concernés puisque des négociations en vue d'accords internationaux ont aussi été entamées avec l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie. Selon le contrôleur européen de la protection des données, « Ces accords internationaux constitueraient le cadre juridique nécessaire à l'échange de données à caractère personnel entre Europol et les autorités de ces pays tiers compétentes pour lutter contre les formes

---

[14] « Le Privacy Shield », CNIL, le 24 mai 2017 [en ligne], URL : https://www.cnil.fr/fr/le-privacy-shield

[15] Résolution du Parlement européen du 6 avril 2017 sur l'adéquation de la protection offerte par le bouclier de protection des données UE-États-Unis (2016/3018(RSP)), [en ligne], URL : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0131+0+DOC+XML+V0//FR&language=FR

[16] « Échange et protection de données à caractère personnel à l'ère de la mondialisation », Avis du Comité économique et social européen [COM(2017) 7 final], 10 octobre 2017, [en ligne], URL : https://www.eesc.europa.eu/fr/our-work/opinions-information-reports/opinions/echange-et-protection-de-donnees-caractere-personnel

graves de criminalité et le terrorisme ».[17] Ces décisions sont ainsi l'occasion pour l'UE de négocier avec les pays tiers souhaitant accéder au marché européen de la donnée en imposant son modèle.

Il s'agit donc d'un instrument utile de développement de la puissance normative de l'UE, dans un contexte où les États-Unis sont en proie à la critique concernant le traitement des données personnelles.

**Aurore CLÉMENT-TROUSSEL**
Membre du Comité Défense Économique de l'ANAJ-IHEDN
103e séminaire jeunes, Pau 2017

**Mathilde DELFOSSE-LEGAT**
Membre du Comité Cyberdéfense de l'ANAJ-IHEDN
104e séminaire jeunes, Dijon

**Antonin PEDOTTI**
Membre du Comité Défense Économique & du Comité Cyberdéfense de l'ANAJ-IHEDN
102e séminaire jeunes, Paris 2017

*Retrouvez toutes les publications de l'ANAJ-IHEDN sur :*
http://www.anaj-ihedn.org/category/actualites/publications-revues/

[17] Résumé de l'avis du contrôleur européen de la protection des données sur huit mandats de négociation en vue de la conclusion d'accords internationaux autorisant l'échange de données entre Europol et des pays tiers, 17 mai 2018, [en ligne], URL : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.C_.2018.170.01.0002.01.FRA&toc=OJ:C:2018:170:TOC