INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

ISSN 2553-6893

IMODEV
LES ÉDITIONS

Vol. 8 - 2022

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons_CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

LES ENJEUX POUR LA SOUVERAINETÉ DES ÉTATS DE L'EXTRATERRITORIALITÉ DU DROIT DES DONNÉES PERSONNELLES

par **Adam COGAN**, Doctorant à l'Université Paris 1 Panthéon-Sorbonne.

Le développement des activités numériques, et l'émergence du *world wide web* en particulier, se sont accompagnés d'enjeux croissants liés à la portée extraterritoriale des règles s'appliquant aux données personnelles générées par ces activités.

À la suite du professeur Jean Salmon, l'extraterritorialité d'une norme peut être caractérisée dès lors qu'un « État prétend appréhender, à travers son ordre juridique, des éléments situés en dehors de son territoire »[2]. Il s'agit d'étendre la portée d'une norme hors de son champ territorial d'application.

Il importe de relever, en première analyse, que l'extraterritorialité n'est pas nouvelle et n'est pas davantage le seul fait des activités numériques. La justice américaine peut par exemple condamner, éventuellement à l'initiative d'étrangers, des étrangers pour des actes commis à l'étranger, dès lors que leur activité peut être rattachée au territoire américain, même de manière distante. Ainsi de la loi dite Helms-Burton de 1996[1], qui défend à tout particulier ou entreprise, sous peine de sanctions, d'acquérir ou d'user des biens américains qui ont été nationalisés par le gouvernement cubain, ou de la loi dite d'Amato-Kennedy[2], de la même année, qui vise à lutter contre le terrorisme international, notamment au moyen de sanctions économiques et commerciales à l'égard d'Etat étrangers. C'est en vertu de ces textes aux portées extraterritoriales qu'en juin 2014 la banque BNP-Paribas a accepté, en plaidant coupable, de payer une amende de 8,9 milliards de dollars, pour avoir violé l'embargo américain sur l'Iran et Cuba notamment.

Dans cette dynamique d'ensemble, contemporaine de la globalisation des personnes, des services, des biens, de l'information et des capitaux, les activités numériques forment un terrain particulièrement propice aux normes de portées extraterritoriales. L'intensification rapide des échanges et le caractère essentiellement immatériel et transfrontalier des réseaux numériques donnent à ce secteur une dimension qui par nature ne s'arrête pas aux frontières nationales. Ainsi que le relève le

---

[1] Cuban Liberty and Democratic Solidarity (Libertad) Act, 12 mars 1996.
[2] Iran and Libya Sanctions Act, 8 août 1996.

professeur Jean-Jacques Lavenue, « *le cyberespace est un territoire virtuel qui dépasse le champ des États* »[3].
Les enjeux de souveraineté qui dérivent de ce phénomène d'extraterritorialité sont dès lors significatifs et tendent à gagner en acuité dans la période récente, à la faveur de différentes législations extraterritoriales s'appliquant à l'accès et au traitement des données personnelles. C'est ainsi le schéma de l'ordre issu du traité de Westphalie[4] qui se trouve en son cœur bousculé par la logique que poursuit l'extraterritorialité des normes. En effet le droit international repose sur l'idée que la norme qui procède d'un l'Etat s'applique sur un territoire limité et aux populations qui y résident, suivant le principe d'égalité et de souveraineté des Etats, rappelé dans le préambule de la Charte des Nations Unies[5]. Il semble dès lors que seule une convergence internationale autour de standards exigeants de protection des données des personnes physiques puisse dépasser les tensions qui dérivent de l'extraterritorialité du droit des données.

§ 1 – LA PORTÉE EXTRATÉRITORALE DES LÉGISLATIONS SUR LA PROTECTION DES DONNÉES FACE À L'ENJEU DE SOUVERAINETÉ DES ÉTATS

Plusieurs législations donnent au droit des données un caractère fortement extraterritorial, portant ainsi une dynamique d'ensemble qui questionne la souveraineté des États.

A) Une dimension extraterritoriale constitutive du Règlement général sur la protection des données[6]

Le Règlement général sur la protection des données (RGPD) consacre les raisonnements de la Cour de justice de l'Union européenne, laquelle a entendu, de manière prétorienne, doter progressivement les législations relatives au droit des données d'une portée extraterritoriale, ce qui constitue de fait une dérogation à la règle de rattachement du droit au territoire de l'Union.

La jurisprudence européenne a joué un rôle de précurseur dans l'extraterritorialité du droit des données européen

Avant même le RGPD, l'approche extraterritoriale était perceptible dans les raisonnements de la Cour de justice de l'Union européenne (CJUE).

---

[3] J-J. LAVENUE, « Internationalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyber espace confronté à la notion d'ordre public », *Lex Electronica*, vol. 11 n° 2, 2006.
[4] J.S. SALMON (dir.), *Dictionnaire de droit international public*, Bruxelles, Bruylant, 2001, p. 211.
[5] Charte des Nations-Unis, Préambule, 26 juin 1945.
[6] Règlement UE 2016/679 du 27 avril 2016, entrée en vigueur le 25 mai 2018.

L'arrêt *Google Spain*[7] de 2013 y a joué un rôle majeur. Dans cette décision, les juges ont étendu le domaine d'applicabilité de la directive 95/46/CE du 24 octobre 1995[8] pour admettre que si l'établissement principal de l'entreprise attaquée se situe aux Etats-Unis (en l'espèce Google), le droit espagnol transposant la directive 95/46/CE s'applique à ses activités dès lors qu'une de ses filiales exerce ses activités en Espagne. Elle a pour ce faire réalisé, d'abord, un effort d'interprétation de la nature juridique de l'exploitant et de son activité de moteur de recherche, avant de rattacher ses activités au territoire de l'Union. L'article 4 de la directive directive 95/46 disposait que « chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque : a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre ». Pour interpréter extensivement cette disposition et responsabiliser la filiale, les juges opèrent en premier lieu une lecture téléologique de la directive 95/46 qui visent à « éviter qu'une personne soit exclue de la protection qui lui est garantie en vertu de la [directive de 1995] »[9]. Ainsi, guidés par cette volonté d'assurer une protection effective des personnes, les juges avancent que par la promotion et la vente d'espace publicitaire, en ce que cette opération est liée à l'affichage de données personnelles sur des pages web, la filiale espagnole opère un traitement de données à caractère personnel et est responsable de ce traitement, « dans le cadre des activités » de son établissement principal.

C'est cette même logique qu'a poursuivi le Juge européen dans l'arrêt *Weltimmo*[10]. Il y retient ainsi une définition extensive de la notion d'établissement, lequel est caractérisé par la seule présence d'un représentant d'un compte bancaire et d'une boîte aux lettres sur une juridiction.

Ainsi, par ces arrêts, la Cour permet de donner toute sa portée et toute son effectivité aux règles européennes de protection de données à caractère personnel, et pose les grandes orientations de la législation à venir.

Le RGPD, par une approche centrée sur les personnes et non sur le lieu de traitement, donne au droit des données une forte dimension extraterritoriale

Le RGPD, venant largement consacrer les raisonnements de la CJUE, présente ainsi un fort volet extraterritorial, justifié par la

[7] CJUE, 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, aff. C-131/12.

[8] 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.

[9] Considérants considérant 18 et 20 de l'arrêt.

[10] CJUE, 1er octobre 2015, Weltimmo s.r.o. c./ Nemzeti Adatvédelmi és Információszabadság Hatóság, aff. C-230/14.

même exigence de protection effective des droits et libertés des personnes physiques. L'article 3, intitulé « champ d'application territorial », comporte des ajouts en ce sens par rapport à l'article 4 (précité) de la directive de 1995. Il dispose en effet que « 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 ». La mention « que le traitement ait lieu ou non dans l'Union » laisse entendre que le législateur passe d'une application territoriale essentiellement fondée sur le territoire, soit le lieu de traitement, à une protection territoriale qui repose davantage sur la personne concernée, sans considération du lieu du traitement ni du lieu de résidence de l'entreprise réalisant ce traitement.
De la même manière, les dispositions du RGPD s'appliquent également de façon explicite aux « sous-traitants », en sus des responsables de traitement. De cet ajout découle l'obligation pour toute entreprise traitant des données personnelles d'Européens de vérifier la conformité de ses sous-traitants aux standards de protection en vigueur, ce qui constitue une obligation au cœur du rayonnement des standards européens dans le monde en matière de protection des données.
Ainsi, le législateur européen a entendu donner corps, dans le texte, à la jurisprudence extensive de la CJUE, qui a conçu l'extraterritorialité du droit des données comme une condition de son effectivité.

B) Une concurrence du RGPD par l'existence d'autres grandes législations extraterritoriales en matière de droit des données

Dans le monde, en parallèle de la législation européenne, d'autres grandes législations extraterritoriales viennent concurrencer le RGPD et interroger la souveraineté des États. La législation fédérale américaine dite du *Cloud act*[11] joue un rôle majeur dans cette dynamique d'extraterritorialisation du droit des données, tendance aussi portée par la volonté chinoise d'assurer un réel contrôle sur les flux qui transitent sur ces réseaux globalisés.

Le Cloud act est conçu comme une réponse à l'aspect extraterritorial du RGPD, dont il méconnaît certaines dispositions

Adopté par le Congrès américain, le *Cloud act* donne compétence aux autorités compétentes pour exiger des fournisseurs de services de communications créés aux Etats-Unis la transmission

[11] *Clarifying Lawful Overseas of Data Act*, 23 mars 2018.

des données situées sur leurs serveurs, que ces derniers se situent ou non à l'étranger, et qu'ils traitent ou non des données de personnes ne résidant pas aux Etats-Unis.
Ce texte a été élaboré dans le contexte de l'affaire Microsoft c/ United States[12], en cours depuis 2013, et alors pendante devant la Cour suprême. Un mandat des autorités américaines demandait alors à Microsoft de communiquer toutes les informations stockées sur un serveur situé à Dublin, en Irlande, sur le fondement du *Stored communication act*[13] alors en vigueur. Suite au refus de Microsoft, qui opposait le droit irlandais de protection des données personnelles, dérivé de la directive européenne, l'affaire a été portée devant une Cour d'appel puis la Cour Suprême des Etats-Unis. Face à ces difficultés juridiques, le législateur fédéral a entrepris une réforme du *Stored Communication Act,* afin d'assurer une réelle portée extraterritoriale au droit des données personnelles américains dans ce type de circonstances.
Aussi la portée du Cloud Act est-elle renforcée, comme cela a été le cas dans la jurisprudence européenne, par une définition extensive de la notion de société américaine, laquelle comprend toute société contrôlée par une société créée aux États-Unis.

L'approche chinoise participe également de cette extraterritorialisation du droit des données

De la même manière, Loi dite « Cyber sécurité pour la République Populaire de Chine », adoptée en novembre 2016, comporte une forte dimension extraterritoriale, en particulier au regard de son article 5 qui prévoit que « L'État prend des mesures pour surveiller, prévenir et traiter les risques et les menaces en matière de cybersécurité, tant à l'intérieur qu'à l'extérieur du territoire continental de la République populaire de Chine ». Au-delà de cet article, de nombreuses dispositions tendent à faire prévaloir les intérêts souverains de l'Etat chinois sur les considérations de confidentialité et de respect des droits fondamentaux des personnes physiques ou des intérêts des entreprises, étrangères ou chinoises. L'article 9 du texte énumère ainsi les obligations des opérateurs de communications, lesquelles doivent notamment accepter la coopération avec le gouvernement dans des objectifs de sécurité publique et de maintien de l'ordre public. L'article 28 ajoute que lorsque les intérêts fondamentaux de la Nation sont en jeu, tout opérateur de réseaux est appelé à fournir une assistance aux autorités publiques. À titre de comparaison, en France, ce sont les services spécialisés tels l'Agence nationale des systèmes de sécurité et

[12] The US department of Justice, « US v Microsoft: Court findings of facts », 2018 : https://www.justice.gov/atr/us-v-microsoft-courts-findings-fact.
[13] Stored communication act, 21 octobre 1986.

d'information (ANSSI) qui sont compétents dans de telles champs d'intervention.
Par ailleurs, l'article 37 de la loi chinoise de 2016 instaure une obligation générale de stockage des données personnelles et des systèmes d'information critiques sur le territoire chinois à des fins de sécurité et de souveraineté. Les possibilités de stocker des données sur un territoire étranger s'en trouvent réduitent à la portion congrue et fortement conditionnées et encadrées.
Plus largement, le mode de gouvernance du régime chinois, notamment sur les acteurs économiques, est très éloigné des standards libéraux des démocraties occidentales, et constitue ainsi un fort potentiel d'extraterritorialisation des règles attachées aux données.

§ 2 – LA NÉCESSAIRE COOPÉRATION INTERNATIONALE FACE AUX ENJEUX DE SOUVERAINETÉ RÉSULTANT DE LA PORTÉE EXTRATERRITORIALE DU DROIT DES DONNÉES

Plusieurs enjeux de souveraineté se dégagent de ces textes et de leur portée extraterritoriale, lesquels appellent une réponse coopérative au niveau international.
Les textes européens, américains et chinois soulèvent un potentiel de conflictualité entre législations extraterritoriales et menacent en leur cœur la souveraineté des Etats et la confidentialité des données à caractère personnel. La voie coopérative à travers la Convention 108, seul instrument universel en la matière et récemment modernisée, apparaît à privilégier.

A) Les enjeux de souveraineté et l'extraterritorialité du droit des données

Des enjeux de souveraineté existent tant en situation d'extraterritorialité forte et offensive que de manque d'extraterritorialité du droit des données.
Les enjeux de souveraineté se posent tant en situation de forte extraterritorialité, pour les Etats étrangers, que pour les Etats aux législations faiblement extraterritoriales, dont les données sont dès lors peu protégées.

Les enjeux tirés de l'extraterritorialité croissante des données sont nombreux pour les Etats tiers, et intéressent en son cœur la souveraineté, malgré les quelques mécanismes de coordination mis en oeuvre

Le premier enjeu d'une telle situation d'extraterritorialité est celui de la confidentialité et de la protection des données. En effet, dans la logique de ces textes, la localisation géographique de données sur un territoire ne constitue plus une garantie assurée de confidentialité. Celles-ci sont en effet désormais

accessibles, dans certaines conditions, depuis l'étranger sur le fondement d'un texte étranger. Il en dérive un enjeu, plus large, de souveraineté, c'est-à-dire de capacité pour un État de régir et de protéger de manière effective les activités et personnes présentes sur son territoire.

Moins mis en avant par la doctrine, l'enjeu de sécurité juridique et de lisibilité du droit se pose également de manière croissante dans ce contexte d'extraterritorialité. Les personnes morales et physiques connaissent en effet à la fois une superposition de normes juridiques aux sources différentes s'appliquant à leurs activités, et, dans le même temps, des régimes qui peuvent rapidement évoluer, tant les dispositifs de coordonnations apparaissent précaires. L'arrêt « Schrem II » rendu par la CJUE à l'été 2020[14], venant invalider le *privacy shield* autorisant le transfert de d'acteurs européens vers des entreprises américaines, lequel procédait lui même de l'arrêt « Shrem I » d'octobre 2015[15] , a ainsi jeté les entreprises, une fois encore, dans une insécurité juridique qui pèse de fait sur leurs activités.

Différents mécanismes de coordination ont certes vu le jour. Ainsi par exemple, au-delà des clauses contractuelles de la Commission et des standards de protection comme le *privacy shield,* des guichets uniques[16] des autorités de contrôle en Europe permettent de coordonner les litiges relatifs au droit des données comportant une dimension extraterritoriale.

Dans les faits, loin de réduire la portée extraterritoriale du droit des données, ces outils renforcent cet aspect, mais dans une logique coopérative et non plus offensive. Ainsi, dans les faits de l'arrêt Kadi[17], l'autorité de contrôle autrichienne a en partie eu à connaître d'un litige attaquant une entreprise Suisse, constituant ainsi la première procédure d'une autorité de contrôle étrangère qui a un impact sur une entreprise suisse sur le fondement du RGPD.

Toutefois, en l'absence d'extraterritorialité, d'autres difficultés s'élèvent, telles que les interrogations sur la réelle l'effectivité d'un droit des données territorialement limité

La dynamique d'extraterritorialité du droit des données ne va pas sans limites. Dans la décision *Google Spain* par exemple, la Cour, en application du principe de proportionnalité, ne reconnaît pas une application mondiale au droit au déréférencement, à rebours de la position retenue par la Commission nationale informatique et liberté (CNIL). Elle s'attache ainsi à mettre en balance le principe de compétence territoriale exclusive des États tiers à celui de protection effective des personnes physiques, au profit du premier.

[14] CJUE, 16 juillet 2020, Affaire C-311/18.
[15] CJUE, 6 octobre 2015, affaire C-326/14.
[16] Considérants 126 et 127 du RGPD.
[17] CJUE, 3 septembre 2008, Kadi, aff. C-402/05 P et C-415/05 P

Si cette limitation de l'extraterritorialité préserve une certaine compétence territoriale des Etats, elle pose un enjeu d'effectivité du droit. L'arrêt Telekabel[18] de la CJUE fournit à cet égard une illustration. Dans cette affaire, les mesures d'exécution prises en application des injonctions de la Cour de ne plus rendre accessible certaines données personnelles sur internet doivent, non pas mettre un terme aux violations constatées à la vie privée, mais « être suffisamment efficaces pour assurer une protection effective du droit fondamental en cause » afin de « décourager sérieusement » les utilisateurs ayant recours aux services du destinataire de cette injonction de consulter les objets mis à leur disposition en violation dudit droit fondamental. Si ces conclusions tenaient en partie à des considérations techniques, la portée territoriale limitée des décision des juges de la Cour de justice participe de cette réserve dans l'appréciation de l'exécution de la décision.

De la même manière, dans l'arrêt *Google Spain*, la limite de la portée du droit au déréférencement réduit de fait l'effectivité de ce nouveau droit. La CNIL, dans sa définition du droit au déréférencement, souligne ainsi le caractère limité de la portée de ce nouveau droit : « le contenu original reste inchangé et est toujours accessible via les moteurs de recherche en utilisant d'autres mots clés de recherche ou en allant directement sur le site à l'origine de la diffusion ». Elle y précise que « cette suppression ne signifie pas l'effacement de l'information sur le site internet source »[19].

B) La convergence des standards de protection au niveau international

Il est dès lors possible d'envisager une convergence des standards de protection au niveau international. La Convention 108+ constitue à ce titre le seul instrument international universel en la matière.

Face à cette tension entre l'effectivité de la protection des personnes d'une part, et le respect du principe de souveraineté d'autre part, une piste de réflexion résiderait dans l'approche retenue par la doctrine de droit mondial (*global law*). En effet, la numérisation des échanges et activités tend vers la création d'un espace propre de circulation des données au niveau mondial, régi par un droit qui dépasserait l'échelon national pour lier les Etats autour d'un corps de règles communes. Dans ce cadre d'analyse, le caractère extraterritorial d'une législation se justifie comme une réponse à une insécurité juridique faisant peser un risque systémique sur un ou plusieurs champs d'activités.

---

[18] CJUE, 27 mars 2014, Telekabel, aff. C-314/12.

[19] Site internet de la CNIL : https://www.cnil.fr/fr/droit-au-dereferencement#:~:text=Le%20droit%20au%20d%C3%A9r%C3%A9f%C3%A9rencement%20vous,la%20requ%C3%A8te%20%22nom%20pr%C3%A9nom%22.

C'est cette logique de stabilité juridique des échanges qui a présidé à la proposition d'une « convention de Genève du numérique »[20] face à l'attaque *Wanna Cry* en vue de former un espace digital *sui generis*. Le RGPD constitue d'ailleurs, à cet égard, à l'échelle européenne, une réponse supra-nationale s'imposant aux Etats membres de l'Union dans une logique de sécurisation et fluidification des échanges au sein du marché commun.

En suivant cette approche, l'extraterritorialité du droit des données constituerait moins une volonté unilatérale d'imposer sa norme qu'une réponse au constat d'interdépendance des Etats et activités et à l'importance de sécuriser leurs échanges en réduisant les risques nés de ces interdépendances.

La Convention 108[21] constitue dans ce cadre un instrument à privilégier. Adoptée par le Conseil de l'Europe, elle est ouverte à la signature en 1981, et a été modernisée en août 2018, après 7 années de négociations internationales. La Convention 108+ demeure aujourd'hui le seul instrument international juridiquement contraignant relative à la protection des données internationales. Selon le Conseil de l'Europe[22], cette modernisation répond à plusieurs objectifs. Elle réaffirme d'abord les dispositions conventionnelles appelées à être complétées par des textes sectoriels plus détaillés sous forme de recommandations ou de directives. Elle assure ensuite une cohérence accrue et la compatibilité entre différents cadres juridiques de protection des données, en particulier celui de l'UE depuis l'entrée en vigueur du RGPD. Enfin, la modernisation de la convention 108 réaffirme la vocation universelle de texte, visant à dépasser les différences de modèle de protection des données personnelles de part le monde.

Aujourd'hui, seule une quinzaine d'Etat ont ratifié la Convention 108+. Si cinq Etats ratifications étaient nécessaires à l'entrée en vigueur de la Convention réformée[23], il reste que, comme le souligne justement le texte, « un large champ d'application géographique [est] jugé essentiel pour l'efficacité de la Convention »[24].

D'autres ratifications sont donc encore à rechercher, afin que la convergence des standards nationaux dépassent en les atténuant les effets indésirables de l'extraterritorialité du droit des données personnelles.

---

[20] https://droitdu.net/2018/01/microsoft-propose-une-convention-de-geneve-digitale/.

[21] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite « Convention 108 »), STE n° 108, Strasbourg, 28 janvier 1981.

[22] https://www.coe.int/fr/web/portal/28-january-data-protection-day-factsheet

[23] Selon l'article 26 de la même Convention.

[24] *Ibid.*