Internet rattrapé par le droit

Maryline Grange

Dans Politique étrangère 2019/4 Hiver , pages 61 à 72
Éditions Institut français des relations internationales

ISSN 0032-342X
ISBN 9791037300065
DOI 10.3917/pe.194.0061
Date de mise en ligne : 09/12/2019

Article disponible en ligne à l'adresse
https://shs.cairn.info/revue-politique-etrangere-2019-4-page-61?lang=fr

CAIRN.INFO

Découvrir le sommaire de ce numéro, suivre la revue par email, s'abonner...
Scannez ce QR Code pour accéder à la page de ce numéro sur Cairn.info.

Distribution électronique Cairn.info pour Institut français des relations internationales.
Vous avez l'autorisation de reproduire cet article dans les limites des conditions d'utilisation de Cairn.info ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Détails et conditions sur cairn.info/copyright.
Sauf dispositions légales contraires, les usages numériques à des fins pédagogiques des présentes ressources sont soumises à l'autorisation de l'Éditeur ou, le cas échéant, de l'organisme de gestion collective habilité à cet effet. Il en est ainsi notamment en France avec le CFC qui est l'organisme agréé en la matière.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

Internet rattrapé par le droit

Par **Maryline Grange**

Maryline Grange est maître de conférences en droit public à l'université de Lyon, UJM-Saint-Étienne. Elle a récemment co-dirigé l'ouvrage *Cyberattaques et droit international,* Paris, Pédone, 2019.

À l'origine, Internet apparaissait comme un nouvel espace de liberté. Dépourvu de frontières, il semblait pouvoir s'affranchir du contrôle des autorités étatiques. Toutefois, des dérives et des atteintes à la sécurité ont poussé les États à affirmer leur souveraineté sur le cyberespace. Ce dernier a progressivement été rattrapé par le droit. Toutefois, cette évolution ne se fait pas sans résistance et révèle de fortes tensions entre les États eux-mêmes et entre les secteurs public et privé.

politique étrangère

« Nous devons reconnaître que le temps est venu pour nous, en tant qu'industrie du monde entier, de nous unir pour nous adresser aux gouvernements de ce monde. » (*We need to recognize that the time has come for us to come together as an industry around the world to call on the world's governments*[1].) Cet appel, lancé en 2017 par le président de Microsoft, à une intervention des États en vue d'adopter une convention internationale protégeant les utilisateurs du cyberespace a de quoi surprendre. Elle contraste avec une autre déclaration, émise par John Perry Barlow près de vingt ans plus tôt, par laquelle il déclarait l'indépendance d'Internet. Chantre d'un Internet libre et dérégulé, il s'adressait frontalement aux États en leur demandant de ne pas interférer dans le cyberespace[2]. Si les relations entre opérateurs privés du numérique et États ont toujours été ambivalentes, il est néanmoins surprenant de constater que les géants de l'Internet réclament aujourd'hui une présence forte des États dans cet espace plébiscité précisément pour sa liberté. La question de la régulation de cette liberté est source de tensions

1. B. Smith, « The Need for a Digital Geneva Convention », Blogs Microsoft, février 2017, disponible sur : <https://blogs.microsoft.com>.
2. J. P. Barlow, « A Declaration of the Independence of Cyberspace », Electronic Frontier Foundation, février 1996, disponible sur : <www.eff.org>.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

entre États eux-mêmes. Depuis ses origines, Internet est ainsi un nouvel espace de confrontations diverses.

Internet est né pendant la guerre froide, alors qu'Américains et Soviétiques se livraient à une course technologique. Afin de se prémunir d'une attaque sur leur système de communications, les autorités américaines ont constitué au sein du département de la Défense un groupe de chercheurs pour développer un réseau fiable et décentralisé de communications, le réseau ARPANET[3]. Dépourvu de centre névralgique de contrôle, et donc de vulnérabilité physique, ce réseau naît officiellement en 1969 et relie les machines telles des points de convergence d'une toile d'araignée en fractionnant les informations transmises en paquets de données. Il assure une continuité dans les communications, initialement entre autorités et centres universitaires américains. C'est donc par une collaboration entre le Pentagone et des sociétés privées qu'Internet prend forme. Peu à peu, la toile s'émancipe de ce créateur gouvernemental et s'étend à travers le développement exponentiel des acteurs privés et des utilisateurs civils. Il en résulte un espace virtuel planétaire au sein duquel des échanges instantanés d'informations se développent sans frontières.

Et c'est précisément le fait que ce réseau ne connaisse pas de frontières, ces séparations juridiques entre États, qui incite à s'interroger sur la place du droit dans le cyberespace. Ce dernier ne semble en effet lié à aucun État, à aucune autorité susceptible de régir ses activités. Pour autant, cela ne signifie pas que le droit est absent du cyberespace : l'espace de liberté sans frontières que constituait à l'origine Internet a été rattrapé par le droit, et Internet est devenu un nouvel espace d'expression de confrontations au sein de la société internationale.

Aux origines d'Internet : un espace de liberté négligé par le droit

Dès sa création, Internet est un espace de diffusion d'informations largement ignoré par le droit, même si certains aspects, tel le nommage, font l'objet d'une normalisation progressive. Des revendications sont alors clairement exprimées pour refuser la présence des États dans le cyberespace.

Un espace de diffusion d'informations ignoré par le droit

Après la naissance officielle d'Internet, l'effervescence scientifique est encouragée et ne subit pas de contrainte juridique particulière. Vont ainsi apparaître le courrier électronique, le protocole TCP/IP (identifiant les appareils connectés), le *World Wide Web* permettant l'utilisation d'Internet

3. Réseau créé sur demande de l'ARPA (Advanced Research Projects Agency).

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

par le grand public ainsi que le développement de navigateurs. Depuis, les innovations se multiplient et facilitent l'échange d'informations entre utilisateurs géographiquement éloignés.

En parallèle de ces développements scientifiques, aucun cadre juridique dédié ne se dessine et ce, en raison de plusieurs facteurs. Ces avancées interviennent dans un contexte libéral où prime la volonté de ne pas entraver un développement technologique et économique précieux. De plus, on ne peut exclure un désintérêt pour la réglementation d'activités dont la technicité ne facilite pas la compréhension. Et l'enthousiasme pour un partage aisé de connaissances avec toute personne où qu'elle se trouve ne paraissait pas devoir être encadré dans un monde en voie de globalisation. Enfin, l'absence de frontières dans cet espace virtuel paraissait peu propice à un encadrement normatif, habituellement segmenté en fonction des territoires des États. L'information circulant sur Internet sans tenir compte des frontières étatiques, son appréhension par le droit n'est guère évidente.

L'encadrement relatif de l'activité de nommage

Pour des raisons pratiques, il est néanmoins apparu nécessaire d'encadrer l'activité de nommage, autrement dit l'attribution des noms de domaine. Ces noms se multipliant il fallait veiller à ce que chaque identification soit unique et que le système soit centralisé. À cet effet, le gouvernement des États-Unis a décidé, en 1998, de confier la gestion du système des noms de domaines (DNS) à l'ICANN (Internet Corporation for Assigned Names and Numbers), société privée californienne[4]. Les craintes suscitées par les relations qu'elle entretient avec le gouvernement américain faiblissent désormais, une plus grande transparence étant mise en œuvre. Le rôle de cette société est considérable dans la gouvernance d'Internet même si elle prétend ne s'occuper que de la « tuyauterie », et non du contenu. Elle décide la création des noms de domaine de haut niveau (.org ou .com, par exemple) et confie leur gestion à des opérateurs régionaux (les registres), lesquels supervisent la commercialisation des noms de second niveau par des bureaux d'enregistrement[5]. L'enjeu économique est considérable alors même que cette société se veut à but non lucratif[6]. Les États ne sont pas totalement exclus puisqu'ils fournissent des avis relatifs aux intérêts publics dans l'activité de nommage, à travers le GAC (Governmental

4. Voir sur : <www.icann.org>.
5. Voir P. Jacob, « Le programme des nouveaux noms de domaine génériques de haut niveau de l'ICANN : témoin de l'affirmation d'un droit administratif global ? », *Annuaire français des relations internationales*, Paris, CNRS éditions, 2014, pp. 755-784.
6. Les candidats à l'obtention d'un nom de domaine de haut niveau doivent verser 185 000 dollars puis des frais annuels associés à chaque registre (25 000 dollars).

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

Advisory Committee). Il n'en demeure pas moins que la gestion et l'attribution des noms résulte seulement de procédures internes décidées et mises en œuvre par une société privée, soumise aux seules normes américaines comme toute société californienne. La présence du droit n'est donc ici que peu significative et assurée par un acteur privé.

Le refus de la présence des États dans le cyberespace

C'est en 1996 que John Perry Barlow prononce sa « Déclaration d'indépendance du cyberespace ». La veille, le président des États-Unis avait signé le *Telecom Reform Act* qui allait bouleverser le marché des télécommunications et sanctionner la tenue de propos « obscènes » sur ce média[7]. Le refus de la présence des États et de toute tentative de réglementation dans cet espace de liberté est sans ambiguïté : « Les gouvernements tirent leur pouvoir du consentement des gouvernés. Vous n'avez ni sollicité, ni reçu le nôtre […]. Le cyberspace ne se situe pas dans vos frontières. […] Nous construisons notre propre contrat social. » Barlow revendique ainsi une complète indépendance du cyberespace, comme s'il s'agissait d'un nouvel espace – immatériel – affranchi de tout contrôle extérieur et au sein duquel les seules règles applicables seraient celles des utilisateurs guidés par une quête de liberté suprême.

La revendication d'une complète indépendance du cyberespace

Tant que les activités sur Internet semblaient seulement permettre un partage de connaissances, et que la croissance économique des opérateurs était modeste, les États ne se sentaient pas directement concernés par le cyberespace civil. C'est avec le développement de dérives – selon certains, inhérentes à toute société, virtuelle ou non – que le retour de l'État va s'opérer, et ce à travers le droit.

La captation d'Internet par le droit

Alors qu'à l'origine, le cyberespace était considéré sans frontière, les États vont le re-territorialiser en lui appliquant des règles pour régir le comportement des utilisateurs et opérateurs situés sur leurs territoires. La mise en cause des fonctions régaliennes des États par certaines activités sur Internet les pousse à agir en utilisant le droit comme outil. Il en va ainsi en raison des atteintes à la sécurité et des dérives dans l'exercice des libertés fondamentales constatées sur Internet. Par ailleurs, l'activité des géants du numérique étant devenue lucrative, certains États veulent les soumettre à l'imposition.

7. Voir sur : <www.fcc.gov>.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

Empêcher les atteintes à la sécurité

Lorsqu'il s'est avéré que les activités sur Internet pouvaient porter atteinte à la sécurité des personnes ou de l'État lui-même, le droit a alors été utilisé pour les endiguer.

Sécurité des personnes

Les malfaiteurs ont su saisir l'évolution des technologies pour diversifier leurs activités. Ces opérations criminelles sans frontières s'avèrent prospères. Pour 2018, le coût de la cybercriminalité est estimé à 600 milliards de dollars par an, soit 0,8 % du PIB mondial[8], alors que Symantec affirme avoir bloqué 142 millions de cybermenaces par jour dans 157 États[9]. Les principales attaques sont les *formjacking*, *cryptojacking* et *ransomware*[10]. Les actes malveillants visant des *clouds* et des objets connectés devraient augmenter au cours des prochaines années. Les cybercriminels dérobent des informations personnelles et les revendent, souvent *via* le *darknet*.

Afin de protéger les victimes, il a fallu créer des normes pour juger les auteurs de ces attaques. Dans la mesure où cette cybercriminalité ne connaît pas de frontières, la réponse devait être internationale. Ainsi le Conseil de l'Europe a-t-il élaboré une Convention sur la cybercriminalité en 2001[11]. Ce seul instrument international contraignant exige des États l'insertion d'infractions pénales dans leurs droits internes pour sanctionner certains actes visant les systèmes informatiques (interceptions ou atteintes à l'intégrité du dispositif), ou des actes criminels réalisés par le biais d'un système informatique (pornographie enfantine ou atteintes à la propriété intellectuelle). Les États ont alors développé leurs législations internes pour réprimer ces comportements[12]. La lutte contre la cybercriminalité exige une coopération internationale entre autorités compétentes pour identifier et appréhender les criminels. La nécessité de déployer des moyens opérationnels efficaces a conduit certains États à créer des agences et autorités judiciaires ou policières dédiées à la lutte

8. Rapport 2018 de McAfee et Center for Strategic and International Studies, disponible sur : <www.businesswire.com>.
9. Rapport Symantec sur les cyber-menaces : <www.symantec.com>.
10. Le *formjacking* introduit un code malveillant sur un site de commerce en ligne pour recueillir les données saisies dans le formulaire de paiement ; le *cryptojacking* introduit un script sur le processeur d'ordinateur pour utiliser ses capacités afin de générer de la *cryptomonnaie* ; le *ransomware* est un logiciel infectant les ordinateurs pour crypter des données et exiger une rançon pour les déchiffrer.
11. Cette Convention est en vigueur depuis 2004 et lie 64 États parties.
12. En France, sont réprimées les atteintes aux systèmes de traitement automatisé de données (art. L.323-1 et suivants du Code pénal), aux droits de la personne liés aux fichiers ou traitements informatiques (art. 226-16 à 226-24 du Code pénal), aux mineurs (art. 227-23 du Code pénal), aux personnes (menaces, usurpation d'identité), les infractions à la loi sur la presse (loi de 1881), les escroqueries (fausse loterie, utilisation frauduleuse de moyens de paiement), etc. Voir sur : <www.ssi.gouv.fr>.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

contre la cybercriminalité[13], qui coopèrent entre elles et avec des organisations internationales, tels INTERPOL ou ENISA au niveau de l'Union européenne[14].

Sécurité des États

Les personnes et entreprises ne sont pas les seules cibles des cyberattaques. La cyberattaque subie par l'Estonie en 2007, le virus Stuxnet en Iran en 2010, l'attaque d'une centrale électrique en Ukraine en 2015 ou les activités de l'Armée électronique syrienne contre les médias et personnalités d'États hostiles au régime, en sont des illustrations.

À l'instar de la sécurité des personnes privées, les États recourent au droit pour tenter d'empêcher ces cyberattaques d'États ou engager la responsabilité de leurs auteurs. Mais quel droit peut être appliqué ? Le droit existant suffit-il pour saisir ce phénomène nouveau ? Faut-il créer un droit dédié ? Autant de questions qui ont agité les enceintes diplomatiques. Finalement, l'Assemblée générale des Nations unies déclare en 2013 que le droit international existant s'applique au cyberespace[15]. Autrement dit, un État ne peut pas porter atteinte à la souveraineté d'un autre par une cyberattaque, ni utiliser la force armée contre un autre État en réaction à une cyberattaque sauf s'il est en état de légitime défense, sous peine d'engager sa responsabilité internationale. Une fois cette étape franchie, s'ouvre celle, toujours actuelle, visant à décliner les règles internationales pour s'adapter aux spécificités techniques des cyberattaques : à partir de quel seuil de gravité une cyberattaque constitue-t-elle une agression armée justifiant le recours à la légitime défense ? Une cyberattaque peut-elle déclencher un conflit armé, régi par un droit spécial ? Un État peut-il adopter des contre-mesures face à une cyberattaque ? etc. Les réponses ne sont pas aisées[16]. Il n'en demeure pas moins que le droit a investi la sphère des cyberattaques. La détermination des modalités de la réponse est liée aux avancées technologiques car à ce jour l'identification des auteurs de telles attaques n'est pas toujours permise. L'ampleur du phénomène a conduit un certain nombre d'États ou d'organisations à développer des entités militaires dédiées à la cyberdéfense[17].

13. Pour la France, mentionnons l'Agence nationale de la sécurité des systèmes d'information ou le Centre de lutte contre les criminalités numériques de la Gendarmerie nationale.
14. Respectivement l'Organisation internationale de police criminelle et l'European Union Agency for cybersecurity.
15. Résolutions 68/243 en 2013 et 70/237 en 2015 de l'Assemblée générale des Nations unies.
16. Voir spécialement M. Grange et A.-T. Norodom (dir.), *Cyberattaques et droit international. Problèmes choisis*, Paris, Pedone, 2019.
17. Par exemple, l'US Cyber Command, l'unité de cyberdéfense du Bundeswehr allemand, le COMCYBER pour les armées françaises, le CERT de l'Union européenne ou le Comité de cyberdéfense et les forces de réaction rapide de l'OTAN.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

Par ailleurs, la lutte contre le terrorisme conduit certains États à adopter des législations internes permettant aux autorités de saisir des informations et du matériel informatique afin d'empêcher des activités terroristes ou de punir leurs auteurs. La quête de sécurité justifie alors l'adoption de nouvelles règles de droit intrusives[18].

Encadrer les dérives dans l'exercice de libertés fondamentales

Internet est un espace d'expression libre : chacun peut y partager publiquement ses opinions, sans filtre conformiste ou étatique. Sauf que l'utilisation d'Internet peut conduire à certaines dérives dans l'exercice des libertés fondamentales face auxquelles les États ont dû recourir au droit. Trois domaines peuvent être évoqués.

Vie démocratique

Le processus démocratique est désormais perturbé par le biais d'Internet. C'est la campagne pour les élections présidentielles américaines en 2016 qui a mis ce phénomène au grand jour. Le piratage des messageries électroniques du camp démocrate a permis de rendre publics des documents de la candidate Hillary Clinton alors qu'en parallèle de fausses informations étaient diffusées au profit du candidat Donald Trump. L'impact sur le déroulement de la campagne a incité le président Obama à expulser du territoire américain 35 agents russes en poste à Washington soupçonnés d'avoir influencé le processus. Depuis, plusieurs campagnes ont été visées : élection présidentielle en France en 2017, référendum sur le Brexit, élections au Parlement européen en 2019, etc. Le processus démocratique peut être affecté par la manipulation du vote électronique ou par la divulgation d'informations susceptibles d'influencer le comportement des électeurs.

Le processus démocratique perturbé par le biais d'Internet

Face à ce phénomène inquiétant, certaines règles ont été adoptées. La France a adopté deux lois en 2018 pour lutter contre la manipulation de l'information (recours au juge pendant la période pré-électorale pour faire cesser la diffusion de fausses informations par les plates-formes numériques, suspension par le CSA de diffusion de services, et obligation de créer des dispositifs pour retirer les fausses informations[19]). La Commission européenne a fait le choix d'une régulation concertée, avec l'adoption

18. Voir la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme permettant aux autorités d'exploiter les données informatiques saisies ou intercepter les communications électroniques.
19. Voir la loi n° 2018-1202 et la loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

d'un Code de bonnes pratiques contre la désinformation en 2018, accepté notamment par Facebook, Google et Twitter, mais ne comportant pas d'obligations juridiquement contraignantes[20]. Il s'agit seulement d'adopter des pratiques vertueuses afin de supprimer les fausses informations. Le droit tente ici de rattraper les activités sur Internet, mais la rapidité de diffusion de fausses informations ne simplifie pas la tâche. Inciter aux comportements vertueux peut être efficace, mais le retard inéluctable paraît difficile à compenser.

Liberté d'expression

La liberté d'expression était une revendication des premiers explorateurs d'Internet, renouvelée avec la Déclaration d'indépendance du cyberespace et toujours d'actualité. Néanmoins, des dérives ont pu apparaître comme pour tout moyen d'expression. Garants de la protection des droits humains, les États se sont saisis du sujet en adoptant des législations interdisant les propos haineux et racistes sur Internet.

L'Allemagne a été précurseur avec l'adoption en 2018 de la loi *NetzDg*[21]. Elle impose aux plates-formes numériques de retirer les contenus haineux signalés par les utilisateurs en 24 heures, sous peine d'amende. Cette loi a suscité des critiques, d'une part quant à la responsabilisation des GAFA, (Google, Apple, Facebook, Amazon) puisque ce sont eux qui doivent apprécier si un contenu est haineux ou non, l'État donnant l'impression de déléguer ses fonctions aux opérateurs privés ; et d'autre part quant à une crainte de dérive liberticide avec un risque de censure de propos non conformistes. L'observation pratique révèle un bilan mitigé[22], alors que le bilan officiel est attendu pour 2021.

La France emprunte la même voie sans attendre, avec un texte de loi en cours d'examen. Le contenu est similaire en obligeant les plates-formes à retirer les contenus « manifestement haineux », sous peine de sanction du Conseil supérieur de l'audiovisuel, actuellement évaluée à 4 % du chiffre d'affaires mondial[23]. La même solution reçoit les mêmes critiques quant au risque liberticide, de délégation indue aux opérateurs privés, et de difficultés de mise en œuvre. Ce d'autant plus que des normes répriment déjà les

20. Voir « Code of Practice on Disinformation », 26 septembre 2018, disponible sur : <https://ec.europa.eu>.
21. Loi du 1er janvier 2018 « Netzwerkdurchsetzungsgesetz ».
22. En 2018, 166 072 contenus ont été retirés par Facebook, Twitter et Google, soit 17 % seulement des contenus signalés. M. Untersinger, « L'Allemagne a déjà fait une loi pour lutter contre la haine en ligne, son efficacité est incertaine », *Le Monde*, 4 juillet 2019, disponible sur : <www.lemonde.fr>.
23. Le texte vise les contenus contrevenant manifestement aux lois liées à l'apologie des crimes contre l'humanité, des actes de terrorisme, à une incitation à la haine, à la discrimination, etc. Voir le texte actuellement soumis à l'examen du Sénat : <www.senat.fr>.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

propos haineux ou racistes exprimés sur des supports plus habituels. La nécessité d'une nouvelle loi est donc discutable, même si les craintes liées à la propagation rapide de tels discours sont réelles, et exigent l'implication des opérateurs du Net.

Vie privée

La protection de la vie privée sur Internet n'est pas aisée. Les utilisateurs plébiscitent souvent les réseaux précisément pour exposer certains aspects de leur vie privée, sans prendre garde aux dérives possibles. Pendant longtemps, aucune protection n'était assurée pour les données personnelles dès lors qu'elles entraient dans le réseau. Compte tenu de la mine d'or que constituent ces données, et des conséquences de la diffusion d'informations sur la vie privée des utilisateurs, il a été nécessaire de réglementer leur usage.

Le droit à l'oubli a été consacré dans l'Union européenne en 2014[24]. Par un arrêt, la Cour de Justice de l'Union européenne reconnaît un droit au déréférencement de données privées : l'exploitant d'un moteur de recherche (Google en l'espèce) est responsable de la demande de suppression de données personnelles contenues sur les pages de tiers, dont le lien apparaît dans la liste de résultats obtenus. La Cour vient de limiter la portée géographique de cette obligation aux référencements issus des extensions européennes du moteur de recherche (google.fr, google.de, etc.), et non au reste du monde (google.com)[25]. La difficulté technique qui aurait résulté d'une position inverse inquiétait Google et les autres moteurs de recherche. Par ailleurs, cela suscitait une difficulté d'articulation avec les normes juridiques relatives aux États non-membres de l'Union européenne, où la législation est moins protectrice, notamment aux États-Unis. Cette protection de la vie privée doit être proportionnée avec l'exercice de la liberté d'expression et d'information, certains utilisateurs cherchant parfois à effacer ainsi les données relatives à une condamnation judiciaire pour pédophilie, alors que d'autres considèrent qu'elle doit être portée à la connaissance de tous.

Le traitement des données personnelles fait l'objet d'une protection particulière sur le territoire européen depuis l'entrée en vigueur du Règlement général sur la protection des données (RGPD) en 2018. Afin de se prémunir contre les utilisations commerciales, souvent à l'insu des utilisateurs, ou frauduleuses, des normes juridiques rigoureuses s'imposent désormais à tous ceux qui sont amenés à traiter des données personnelles,

24. CJUE, Grande chambre, 13 mai 2014, arrêt C-131/12 « Google Spain ».
25. CJUE, Grande chambre, 24 septembre 2019, arrêt C-507/17, « Google LLC ».

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

ce qui permet d'harmoniser les législations à l'échelle européenne. Cela concerne tout organisme (privé ou public) qui réside ou cible des utilisateurs résidant sur le territoire de l'Union européenne, dès lors qu'il traite des données personnelles[26]. D'importantes obligations s'imposent : recueil du consentement de la personne en lui expliquant la finalité de l'obtention de ses données, tenue d'un registre précis confidentiel, désignation d'un délégué à la protection des données, droit à la portabilité des données, etc. Les changements considérables entrepris pour respecter cette réglementation doivent permettre une meilleure protection des droits des personnes et une certaine confidentialité des données. Le RGPD est unique à l'échelle mondiale, mais certains États envisagent de s'en inspirer. Les opérateurs privés transnationaux le souhaitent, en dépit des contraintes inhérentes, afin de pouvoir élaborer des procédés identiques quel que soit le lieu concerné.

Le RGPD est unique mais certains États envisagent de s'en inspirer

Le terrain des données est devenu un enjeu de rivalités entre États. La plupart d'entre eux développent des législations visant à sécuriser leur stockage et leur contrôle[27]. Le *Cloud Act* adopté par les États-Unis oblige les fournisseurs de services détenant des données réclamées par les autorités à les livrer, même si elles sont stockées à l'étranger à partir du moment où ces fournisseurs sont soumis aux lois américaines. La Chine a adopté une loi imposant aux entreprises de stocker physiquement les données sur des serveurs localisés en Chine, une autre loi permettant aux responsables de la sécurité de surveiller Internet au nom de la protection de la sécurité nationale et de la vie privée. La Russie, pour sa part, exige que les données des ressortissants russes soient stockées sur son sol, et soient fournies aux organes de sécurité dans le cadre de la lutte anti-terroriste. Il en résulte des conflits de normes considérables que les opérateurs doivent gérer, avec difficulté, et dont l'utilisateur n'a bien souvent pas conscience. Le droit devient ici outil de confrontation géopolitique au détriment de la protection des utilisateurs.

Taxer les revenus des géants du numérique

Le pouvoir de lever l'impôt relève de l'État. Mais dans un espace virtuel sans frontières, les modalités de taxation d'activités numériques devenues

26. On entend par données à caractère personnel, toute information se rapportant à une personne physique identifiée ou identifiable : nom, numéro d'identification, données de localisation, identifiant en ligne, éléments propres à son identité physique, génétique, psychique, économique ou sociale (article 4 du RGPD, 27 avril 2016).
27. G. Longuet (rapporteur), *Le devoir de souveraineté numérique*, rapport n° 7, Paris, Sénat, octobre 2019, disponible sur : <www.senat.fr>.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

lucratives ne vont pas de soi. À titre d'exemple, le chiffre d'affaires de Google en 2017 aurait été de 95 milliards de dollars, dont 80 % issus des revenus publicitaires[28]. Les disparités de politiques fiscales permettent à certains États d'utiliser ce levier pour attirer l'implantation d'entreprises. Le principe étant celui de l'imposition dans le lieu de l'établissement, les GAFA implantent leurs sièges dans les États où le taux est le plus faible. Un projet d'harmonisation fiscale européenne a échoué en 2018, compte tenu de la concurrence entre certains États membres[29]. La France a donc fait le choix d'instaurer, seule, une « taxe GAFA » pour imposer les sociétés numériques à partir du lieu de l'activité de l'utilisateur et non du siège[30].

Ainsi, elle vise les interfaces permettant à un utilisateur du territoire d'entrer en contact avec d'autres pour la fourniture de services et la vente de services publicitaires ciblés s'appuyant sur les données récoltées lors des visites d'utilisateurs. L'efficacité d'une loi isolée n'est pas évidente et la disparité normative au sein même du territoire européen, peu propice à l'unité du marché économique cher aux institutions européennes, inquiète. Pourtant, le mouvement semble enclenché car d'autres États européens veulent emprunter cette voie et des négociations ont été engagées au sein du G7 et de l'OCDE pour réformer les règles fiscales.

***

L'évolution de la relation entre Internet et le droit révèle que le cyberespace est devenu un lieu de tensions entre acteurs de la société internationale, que ce soit entre les États eux-mêmes ou entre États et opérateurs privés. D'une part, Internet est devenu un nouveau moyen d'affrontements entre États (cyberattaques contre un autre État, ingérence dans la vie démocratique, outil de guerre industrielle) et un objet de leur affrontement (détermination du droit applicable aux cyberattaques, lois permettant l'exploitation ou la protection des données). Le droit est ici un outil d'expression de confrontations entre États, sans constitution de blocs unis mais avec des coalitions à géométrie variable. D'autre part, Internet bouleverse la relation entre États et société civile internationale. Alternant entre incitation au développement économique et scientifique, répression de comportements (non-respect de la vie privée avec les affaires Google ou exploitation de données avec le scandale Cambridge Analytica), instrumentalisation dans les confrontations étatiques (par les entreprises stockant les données) et délégation de fonctions régaliennes (en leur confiant

28. « Google fête ses 20 ans : chiffre d'affaires, requêtes, amendes... Le géant du web résumé en quatre chiffres (vertigineux) », France TV Info, 24 septembre 2019, disponible sur : <www.francetvinfo.fr>.
29. Voir sur : <www.touteleurope.eu>.
30. Loi du 24 juillet 2019 portant création d'une taxe sur les services numériques.

Institut français des relations internationales | Téléchargé le 07/07/2026 sur https://shs.cairn.info (IP: 37.60.190.132)

le contrôle des contenus haineux ou terroristes), l'attitude des États à leur égard n'est pas linéaire. La réciproque est vraie. Les GAFA se plaignent régulièrement des contraintes résultant des législations relatives aux données, des pressions exercées pour livrer des données, des obligations de contrôle des contenus et des difficultés techniques et économiques qui en résultent. Pourtant, depuis 2017, ils réclament une régulation étatique du réseau par l'appel à une Convention de Genève digitale ou par la voix de Mark Zuckerberg qui s'est prononcé en faveur d'un « rôle plus actif des gouvernements et des régulateurs »[31].

C'est que ces opérateurs privés ont besoin de prévisibilité, de stabilité, et de rassurer des utilisateurs désormais conscients de leurs vulnérabilités. Les autorités semblent entendre et recevoir ces demandes. Ainsi l'Appel de Paris de 2018[32], co-signé par des États et des acteurs privés, révèle une prise de conscience d'un besoin de régulation sur Internet afin de sécuriser les activités numériques. Cette régulation doit être co-construite entre les acteurs d'Internet, États, organisations internationales et opérateurs privés, au bénéfice des utilisateurs. Reste à trouver comment répondre à ce besoin. À défaut, les opérateurs pourraient bien être tentés d'entreprendre seuls cette fonction normative, comme les projets de création de monnaie et de juridiction internes à Facebook le montrent. Sur Internet comme ailleurs, le droit est un outil qu'il faut utiliser à bon escient.

PE

Mots clés
Cyberespace
Gouvernance de l'Internet
Droit du numérique
Régulation des technologies

31. Voir son compte Facebook le 30 mars 2019, disponible sur : <www.facebook.com>.
32. Appel de Paris pour la confiance et la sécurité dans le cyberespace, novembre 2018, avec 564 soutiens dont 67 États, 358 entités privées et 139 organisations internationales et de la société civile. Voir sur : <www.diplomatie.gouv.fr>.