Enjeux numériques

Compliance et nouvelles régulations

N°30 - JUIN 2025

Notre site

les Annales des mines Depuis 1794

Publiées avec le soutien de l'Institut Mines-Télécom

les Annales des mines
Depuis 1794

ENJEUX NUMÉRIQUES

ISSN 2781-1263 (en ligne)
ISSN 2607-9984 (imprimé)
Série trimestrielle - N°30 - Juin 2025

Rédaction

Conseil général de l'Économie
Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique
120, rue de Bercy
Télédoc 797
75572 Paris Cedex 12
Tél. : 01 53 18 52 68
http://www.annales-des-mines.org

Grégoire Postel-Vinay
Directeur de la publication et Rédacteur en chef

Alexia Kappelmann
Secrétaire générale

Daniel Boula
Secrétaire général adjoint

Magali Gimon
Assistante de rédaction et Maquettiste

Nuria Gorris
Webmestre et Maquettiste

Publication

Photos de couverture
Le Tricheur à l'as de carreau, Photo © RMN-Grand Palais (musée du Louvre) / Adrien Didierjean

Iconographie
Daniel Boula

Mise en page
Magali Gimon

Impression
Dupliprint Mayenne

Compliance et nouvelles régulations

Introduction

Panorama des différentes régulations

Régulation européenne : protection ou frein ?

Compliance : outil adapté au numérique ou dérive ?

Hors Dossier

Ce numéro a été coordonné par
Pierre BONIS et Lucien CASTEX

Réguler le numérique, ou Sisyphe heureux

Par Pierre BONIS
Directeur général de l'Association française
pour le nommage internet en Coopération (Afnic)

Et Marie-Anne FRISON ROCHE
Professeure de Droit de la Régulation
et de Droit de la Compliance

« Il faut imaginer Sisyphe heureux ». C'est ainsi qu'Albert Camus conclut son essai[1], nous invitant à garder en tête et dans notre cœur que toute entreprise est inachevée, que notre goût pour l'achevé nous la fait toujours recommencer et que de cela pourtant nous devons être heureux. De ce mouvement vers un système parfait, qui serait l'œuvre vers laquelle le travail doit recommencer à tendre, toujours le même, toujours à refaire, il n'en est pas moins gratifiant. Il est toujours en état futur d'achèvement.

C'est donc ainsi que nous pourrions imaginer les législateurs et les gouvernements du monde, heureux d'avoir mis en place des règles pour un numérique insaisissable, mais conscients qu'il leur sera nécessaire, dès la plume posée, de s'atteler à l'élaboration de nouvelles règles. Ces écritures qui portent toujours l'ambition de mieux faire, qui s'accumulent et se croisent, le numérique les appelle.

En cela, le numérique, comme il est notre ambition de le montrer dans ce numéro d'*Enjeux numériques* intitulé « Compliance et nouvelles régulations », nous invite à envisager un changement profond de paradigme dans l'approche régulatoire d'un secteur puissant et divers, que ces écritures multiples portent. Un système numérique, dirons-nous, plutôt qu'un secteur, tant il recouvre aujourd'hui le monde dans lequel chacun vit, qui renouvelle les catégories classiques de la souveraineté au sein de laquelle peut se déployer traditionnellement le droit.

Le numérique en effet, par le fonctionnement même d'Internet qui l'a transformé en fait social et économique mondial, se déploie dans le monde entier et désormais dans l'espace proche de la planète[2]. Ainsi, il aurait fallu pour que ce système numérique devînt un sujet de droit international, qu'il fût, précisément, aussi univoque que peuvent l'être les océans et les eaux internationales qui se déploient au-delà des zones économiques exclusives. Le droit international de la mer existe. Un droit international du numérique s'est-il pareillement construit ?

Ce n'est pas le cas. Un traité international du numérique, tant ses composantes sont diverses et évolutives, et pour certaines d'entre elles, relèvent de la régulation des infrastructures, quand d'autres relèvent du droit de la presse, rendrait Sisyphe malheureux, puisqu'il fixerait trop les choses, bloquant notre personnage qui ne vit que pour toujours recommencer son ascension. On sait que les approches d'une nation à l'autre sont distinctes en matière de liberté d'expression et de droit de la presse, mais également

[1] Albert CAMUS, *Le mythe de Sisyphe*, 1942.

[2] On pourra lire avec intérêt à ce propos le numéro 25 d'*Enjeux numériques*, de mars 2024, « La Terre vue d'en haut », https://www.annales.org/enjeux-numeriques/2024/en_25_03_24.html

en matière de protection des données personnelles et de confidentialité. Les conceptions sont à ce point diverses et ancrées dans chaque nation que trouver une régulation positive commune est un vœu pieux. Jamais, tant le numérique couvre de champs distincts, un traité international complet ne pourrait voir le jour, et le rocher resterait désespérément au pied de la falaise.

Ce numérique est également insaisissable car la notion recouvre des sujets de droit tellement différents qu'une régulation globale est inenvisageable.

Les acteurs techniques et économiques qui font fonctionner Internet et qui proposent puis parfois imposent des services numériques peuvent être purement nationaux, internationaux, « globaux », ce dernier terme évoquant des positions oligarchiques ou hégémoniques. Or, le sujet de la régulation quand il s'agit d'une modeste PME, peut-il être soumis aux mêmes obligations qu'un Léviathan membre du club des Gafam[3] ?

Malgré ces difficultés à réguler le numérique, la nécessité d'encadrer son déploiement et ses acteurs a donné naissance à de nombreuses lois, parfois au niveau national, plus souvent à l'échelle de l'espace économique et politique de l'Union européenne. Chacun apporte donc son petit rocher. Il ne peut en être autrement, il peut être efficace qu'il en soit ainsi. Les pratiques, les contrats et les juges les ajusteront.

Ces régulations, toujours remises sur le métier, ne cessent de s'ajouter les unes aux autres, comme on pourra s'en apercevoir dans ce numéro. Le dialogue entre les sujets du droit, que sont les acteurs du numérique, et ceux qui l'élaborent, peut pourtant devenir difficile. D'un côté, l'impression d'être soumis à des règlements pointilleux, perçus comme non pertinents techniquement et susceptibles d'entraîner des effets de bord nocifs. De l'autre, le sentiment que les acteurs du numérique font système pour échapper à toute contrainte, instrumentalisant le caractère supranational de certains services qu'ils rendent pour décliner toute responsabilité et s'affranchir de la recherche du bien commun.

On notera à ce propos que l'opposition ne se résume pas à un face-à-face entre régulateurs et entrepreneurs. Elle s'étend géopolitiquement, et met aux prises des visions concurrentes de la régulation, notamment entre les États-Unis et l'Europe[4].

Il n'est que se pencher sur la lettre écrite par le nouveau régulateur américain aux entreprises américaines majeures du secteur qu'il régule :

« J'ai une certaine inquiétude à l'égard de l'approche que l'Europe adopte sur le DSA en particulier. Il y a un risque que ce régime réglementaire impose des règles excessives en matière de liberté d'expression. La censure qui pourrait potentiellement découler du DSA est incompatible à la fois avec notre tradition de liberté d'expression en Amérique et avec les engagements que les entreprises technologiques ont pris sur la diversité d'opinions ».

Si l'expression virulente de l'opposition au DSA peut être mise sur le compte d'une administration Trump s'exprimant parfois sans nuance, il n'en reste pas moins que la différence d'approche entre l'Amérique et l'Europe en matière de régulation du numérique n'est pas nouvelle. Elle sera d'ailleurs montrée dans ce numéro.

Mais revenons aux craintes exprimées par plusieurs acteurs du numérique face à la multiplication des régulations ; DSA, DMA, NIS1, NIS2, RGPD, DORA, etc.

D'un côté, le risque perçu d'une régulation trop intrusive sur les moyens techniques et les méthodes à déployer, au point qu'elle pourrait entraîner un danger de rupture de service. La recherche permanente d'une conformité chaque jour plus lourde à mettre en œuvre se

[3] L'acronyme pointant les Google, Amazon, Facebook (Meta), Apple, Microsoft devrait lui-même évoluer pour intégrer, au moins X, TikTok, et OpenAI.

[4] https://www.fcc.gov/sites/default/files/Chairman-Letter-to-Big-Tech-on-Digital-Services-Act.pdf

ferait au détriment de l'innovation et de la vocation première des acteurs qui opèrent les infrastructures du numérique : permettre la continuité du service, quoi qu'il arrive, et dans toutes circonstances. En outre, comme les lois et règlements ne sont pas mondiaux, s'ajoute à cette crainte presque ontologique de la rupture du service celle, plus économique, d'un déclassement possible d'acteurs régulés face à d'autres qui échapperaient à ces régulations. Ces distorsions pouvant avoir pour effet de limiter paradoxalement l'effet des régulations elles-mêmes, puisqu'elles ne s'appliqueraient *in fine* qu'à des sujets rendus moribonds sous le poids de la paperasse et de la disponibilité de preuves, tandis que des géants de la tech libres comme les renards dans le poulailler atteindraient une taille si critique qu'ils deviendraient *de facto* les souverains, maîtres édictant les règles à la place des législateurs.

De l'autre, des pouvoirs publics au sens large (exécutif, législatif, autorité judiciaire) se percevant comme empêchés dans leur action par des technologies qui non seulement leur échappent, mais encore protègent les malfaiteurs, et sont utilisées par ceux-ci pour échapper à la Loi. Les récents débats sur le chiffrement de bout en bout à l'occasion de la discussion de la proposition de loi « visant à sortir la France du piège du narcotrafic » en sont une illustration édifiante, montrant la complexité de ce dialogue entre technologies et régulations. En effet, le problème rencontré ici est que la légitime volonté d'efficacité des forces de l'ordre en matière de lutte contre le narcotrafic se heurte à la tout aussi légitime nécessité de sécurisation de bout en bout des communications, dans un contexte de menace cyber grandissante. On voit ainsi, au sein même de l'État, et même de la représentation nationale, des points de vue antagonistes entre les départements cyber de l'administration et ceux de la police et des enquêteurs. La technologie du chiffrement de bout en bout, en protégeant la confidentialité des échanges, y compris vis-à-vis des plateformes qui offrent ce service, semble ne pouvoir être efficace que dans l'absolu. Créer des exceptions, des *back doors*, ce serait affaiblir l'ensemble du système de protection de la confidentialité, ces mêmes *back doors* pouvant tout aussi bien être créées par des agents malveillants.

On aurait tort cependant de déduire de ce qui vient d'être décrit que les régulations du numérique sont vaines. Depuis 1978 et la Loi *Informatique et libertés,* le législateur a su encadrer le développement de l'informatique, puis du numérique, sans toutefois obérer les capacités d'innovation et la contribution des opérations à la croissance de l'économie. Pour ce faire, un subtil mélange de règles imposées et de bonnes pratiques consenties et co-élaborées avec l'ensemble des parties prenantes a permis d'accompagner l'essor d'un numérique dont on ne peut pas, du moins au sein de l'espace européen, qualifier les opérateurs d'irresponsables. Ainsi, la Loi de 2004 de Confiance dans l'économie numérique a, par exemple, posé les fondements d'exceptions à la responsabilité des acteurs, affirmant en creux la responsabilité de l'hébergeur, de l'intermédiaire technique et de l'éditeur. Toutes sont limitées, justement pour que la société puisse les tenir pour responsables dans leur champ de compétence propre.

Les chartes élaborées par les parties prenantes, au sein d'organismes de concertation tels que l'Association française pour le Nommage Internet en Coopération (Afnic) telles que la charte de nommage de l'extension nationale française .fr, ont fini par avoir force de contrat, voire de règlement selon l'interprétation du Conseil d'État. Des organismes mixtes, rassemblant magistrats, parlementaires, fonctionnaires de l'administration centrale, régulateurs indépendants et acteurs privés et associatifs ont vu le jour, pour préparer au mieux les évolutions des règles et régulations. Ce fut dès le début des années 2000 le Forum des droits sur l'internet, remplacé par le Conseil national du Numérique (CNnum). À l'international, à travers le Sommet Mondial sur la Société de l'Information dont les Nations Unies célèbreront les 20 ans cette année 2025, une structure hybride comme le Forum sur la Gouvernance de l'Internet (FGI) a également vu le jour et complète un dispositif d'organismes divers traitant de la gouvernance d'Internet de manière

décentralisée et multi-acteurs. On citera notamment à ce propos l'*Internet Corporation for Assigned Names and Numbers (ICANN)* ou encore l'*Internet Engineering Task Force (IETF).*

On le voit, le numérique est si vaste et touche tant de parties prenantes que la prise en compte des buts sociétaux par les acteurs économiques et techniques qui le font fonctionner se fait avec d'autant plus d'efficacité que ces derniers sont impliqués, et non seulement sujets des régulations.

C'est à travers cette approche, celle de la responsabilité des acteurs, de la transparence de leur pratique, de l'intégration par ceux-ci, et en fonction de leur pouvoir technique, des obligations et des contraintes rendues nécessaires par les attentes de nos sociétés, que se rencontrent l'exigence sociétale et l'efficacité technique et économique. Si le législateur fixe un cap et des règles, il revient aux sujets de ces législations d'intégrer en leur sein propre, dans leurs processus, leur stratégie, leur mode de fonctionnement et leur mission, les attentes exprimées par le législateur.

C'est ainsi que la régulation de l'espace numérique se transforme à travers la compliance, qui constitue son nouveau paradigme, le rocher qui paraît plus que jamais écrasant sur les épaules des seuls législateurs et autorités de régulation pouvant enfin être partagé avec les opérateurs, voire les internautes. En effet, qu'il s'agisse des nouveaux dispositifs en matière de cybersécurité, de contrôle des contenus ou d'intelligence artificielle, la régulation se déploie désormais selon une nouvelle organisation normative que le droit de la compliance exprime, reposant sur un inter-maillage où chacun a son rôle, de l'internaute jusqu'aux organisations internationales, en passant par les États et les organisations professionnelles.

Les autorités politiques et publiques fixent les buts à atteindre, notamment la sécurité, la continuité du service, la fiabilité du système technique, l'Europe insistant sur la protection des personnes. Les moyens par lesquels ces buts, dont certains sont techniques, d'autres sont davantage politiques, sont atteints, sont choisis et maniés par les opérateurs économiques cruciaux du système, dont les contours ne sont pas forcément les mêmes que ceux des États. Cette internalisation des buts, parfois de force, parfois de gré, responsabilisant ainsi les opérateurs et donnant aux personnes concernées, principalement l'internaute, des droits d'action, renvoie aux mécanismes de compliance sur lesquels les nouveaux règlements européens précités, par exemple DSA, AIAct, NIS2 ou DORA, sont construits.

La régulation de l'espace numérique se prolongeant ainsi d'une façon nouvelle par la compliance, à la fois technologiquement mais aussi politiquement, elle présente par certains aspects des points communs entre toutes les régulations des zones du monde, par exemple sur l'information et la durabilité du système lui-même, tandis qu'elle traduit aussi des visions politiques différentes, notamment quant à l'emprise des autorités publiques, plus ou moins présentes en *ex ante*, plus ou moins en supervision sur les entreprises.

Dans ces équilibres qui sont forcément instables et évolutifs dans le temps, non seulement parce que les technologies évoluent mais aussi parce que les visions politiques changent (et s'affrontent) et que les attentes des personnes évoluent (et s'affrontent), la figure du juge va apparaître de plus en plus. Il dira, dans des contentieux dont l'ampleur sera à la dimension du système lui-même (« contentieux systémique émergent »), à propos des délits, des sanctions, des illégalités, des droits de propriété intellectuelle, des contrats ou des responsabilités qui des uns ou des autres doit porter ce très lourd rocher de la régulation du numérique car du fléau c'est toujours lui qui tient la balance.

Bonne lecture.

Droit des données personnelles, plateformes et transparence algorithmique

Par Julien ROSSI
Maître de conférences à l'Université Paris VIII

Les plateformes en ligne instituent des rapports de pouvoir au sein de la société, en particulier entre les différentes catégories de publics qu'elles mettent en relation. Cette intermédiation repose souvent sur la mise en œuvre d'algorithmes au fonctionnement opaque, tant au regard de l'individu concerné que de la collectivité. Le droit d'accès aux données à caractère personnel, aujourd'hui consacré à l'article 15 du RGPD, a été pour partie institué pour remédier à de pareilles situations d'asymétrie informationnelle.

Dans cet article, nous verrons que des évolutions jurisprudentielles récentes ouvrent la voie vers le développement des usages individuels, mais aussi collectifs, de ce droit d'accès, au service d'une meilleure transparence individuelle et d'une compréhension collective du pouvoir des plateformes.

Ce papier s'inscrit dans le cadre de travaux financés par l'Agence nationale de la recherche – projet DATARights, ANR-24-CE53-2287-01.

Le terme de « plateforme » recouvre une grande variété de services différents qui ont pour point commun d'offrir un service d'intermédiation en ligne dont l'efficacité repose sur la capacité de collecte, traitement et valorisation de données (Srnicek, 2019). Leurs algorithmes produisent de nombreux effets de pouvoir (Rouvroy et Berns, 2013 ; Nieborg *et al*., 2024). Il existe ainsi des algorithmes qui décident de la censure ou, au contraire, de la promotion d'un contenu sur un réseau social (Badouard, 2020). D'autres encore affectent significativement les relations de travail (Pidoux, Dehaye et Gursky 2024). Tout ceci, souvent, dans des relations marquées par une grande opacité (Bruns 2019) au profit du pouvoir des plateformes, soulevant des questions telles que : comment des créateurs de contenus peuvent-ils savoir les critères selon lesquels leurs productions seront – ou non – mises en avant, suggérées et découvrables par des utilisateurs d'une plateforme de *streaming* musical ? Comment des chauffeurs de VTC peuvent-ils savoir comment se voir attribuer plus de courses, ou des courses plus rentables, par l'algorithme de la plateforme qui les met au travail ? Peut-on comprendre les raisons qui gouvernent les personnes avec qui nous sommes mis en relation par des applications de rencontre ?

Nous verrons ici qu'il existe plusieurs modalités prévues par le droit de l'Union européenne qui devraient permettre de trouver des réponses individuelles et collectives à ces questions. L'une d'entre elles repose sur la mise en œuvre du droit d'accès aux données à caractère personnel, renforcé d'abord par l'adoption du RGPD, puis par des évolutions récentes de la jurisprudence de la Cour de justice de l'Union européenne (CJUE), qui ouvrent la voie à une compréhension collective des relations de pouvoir construites par les plateformes numériques.

Plateformes numériques, droit d'accès aux données personnelles et portabilité

La grande diversité des services que l'on désigne par le terme de « plateforme » rend difficile la rédaction d'une définition permettant de tout inclure sans perdre de vue ce qui fait la spécificité de ce type de service. Airbnb, Deliveroo, Facebook, Instagram, Shein, Spotify, Tinder, TikTok, X… ces services n'ont pas tout à fait le même modèle d'affaires, ni le(s) même(s) public(s). Cette diversité se reflète dans celle des définitions différentes que l'on trouve dans le Droit, en fonction des secteurs qui ont fait, à partir de la fin des années 2010, l'objet d'une réglementation croissante. Dès 2016, la loi pour une République numérique[1] introduisait dans notre droit national la définition – désormais abrogée[2] – de la notion d'« opérateur de plateforme en ligne ». Plus tard, l'UE adoptait le règlement dit Plateform-to-Business[3], s'appliquant aux « services d'intermédiation en ligne » ; puis le Règlement sur les marchés numériques[4] (Digital Markets Act – DMA) encadrait les plateformes désignées par la Commission comme « contrôleurs d'accès » en raison de leur capacité à conditionner l'accès aux marchés sur lesquels elles assurent l'intermédiation. Enfin, le Règlement sur les services numériques[5] (Digital Services Act, DSA) définit quant à lui une plateforme comme étant « un service d'hébergement qui, à la demande d'un destinataire du service, stocke et diffuse au public des informations ». Le considérant 13 du DSA permet de mieux comprendre la distinction opérée entre un simple hébergeur, tel qu'on le connaît depuis la directive sur le commerce électronique de 2000[6], et la plateforme : cette dernière ne se contente pas de stocker, mais aussi de diffuser l'information au public. Cette diffusion – et, pourrions-nous ajouter, le contrôle des modalités de cette diffusion – n'y est pas une caractéristique mineure, mais le cœur de son activité.

Or, nombre de données traitées par les plateformes revêtent le caractère de données à caractère personnel, définies à l'article 4 (1) du RGPD comme recouvrant « toute information se rapportant à une personne physique identifiée ou identifiable […] directement ou indirectement ». Dès lors, et sans même aborder la question d'éventuelles données collectées sur des personnes non-utilisatrices[7], les plateformes sont responsables du traitement de ces données, et doivent notamment garantir aux personnes concernées par le traitement de leurs données un certain nombre de droits, dont le droit d'y accéder en vertu de l'article 15 de ce règlement, dans un délai d'un mois (hors exception tenant compte de la complexité de la demande ; art. 12 (3) du RGPD). Lorsque la demande d'accès

[1] Article 49 de la loi n°2016-1321 du 7 octobre 2016.

[2] Le paragraphe I. de l'article L.111-7 du Code de la consommation a été abrogé par l'article 52 de la loi 2024-449 du 21 mai 2024 visant à sécuriser l'espace numérique, dans le cadre de l'adaptation du droit français au DSA et au DMA.

[3] Règlement 2019/1150.

[4] Règlement 2022/1925.

[5] Règlement 2022/2065.

[6] Directive 2000/31.

[7] Google avait fait l'objet de sanctions en France pour avoir collecté de manière illicite des données sur des internautes non-utilisateurs de leurs services (Cnil, Délibération 2013-420 du 3 janvier 2014). En Belgique, l'injonction contre Facebook obtenue en référé en 2018 par l'Autorité de Protection des données et l'obligeant à arrêter le pistage des internautes non-inscrits doit encore faire l'objet d'un jugement suite à la cassation en 2023 d'une première décision d'appel (Cour de cassation belge, 10 mars 2023, arrêt C.22.0271.N).

est faite sous une forme électronique, le demandeur peut demander à ce que la réponse prenne la même forme, lorsque c'est possible.

Le droit d'accès de l'article 15 du RGPD est complété par son article 20, qui consacre le droit d'une personne concernée de recevoir les données qu'il a lui-même fournies dans un format structuré et lisible par la machine et de les transférer ainsi, le cas échéant, d'une plateforme à une autre. Mais ce droit à la portabilité ne concerne pas les données qui auraient par exemple été inférées par un algorithme. L'article 6 (9) du Règlement sur les marchés numériques (Digital Markets Act – DMA) complète alors ce droit en imposant à certains services de plateforme essentiels désignés par la Commission européenne en raison de leur poids dans le marché intérieur d'intégrer les données « générées par l'activité de l'utilisateur final » dans cette portabilité. Enfin, le Règlement sur les données (Data Act) prévoit, dans son article 3 (1), un droit d'accès aux données produites par les objets connectés que l'on possède, que celles-ci soient à caractère personnel ou non.

De l'accès individuel à la compréhension collective des données des plateformes

Le droit d'accès ne revêtirait qu'un piètre intérêt du point de vue de la transparence algorithmique s'il ne s'étendait pas aux données inférées, ni si son exercice était trop étroitement conditionné. Or, un arrêt de la CJUE de 2014 avait d'abord considérablement affaibli le droit d'accès[8]. Interprétant la directive de 1995 aujourd'hui remplacée par le RGPD, la Cour avait jugé qu'une analyse juridique portant sur les données personnelles du demandeur d'un titre de séjour n'était pas une donnée à caractère personnel. Elle avait alors distingué les données sur lesquelles portaient l'analyse de l'analyse elle-même, et, partant, dit pour droit qu'une demande d'accès formulée par un tel demandeur pouvait être satisfaite par un simple « aperçu complet des [ses] données sous une forme intelligible[9] ». L'accès à l'analyse (donc aux inférences) n'était pas nécessaire. De plus, la CJUE suivit à cette occasion un raisonnement téléologique qui semblait subordonner l'exercice du droit d'accès à une justification fondée sur l'utilité de la demande pour évaluer la licéité d'un traitement de données à caractère personnel. Bart Custers et Helena Vrabec (2024) en ont conclu que cet arrêt limiterait à l'avenir la possibilité d'accéder à ses données lorsque celles-ci sont inférées par un algorithme, ses inférences pouvant s'assimiler alors à des analyses détachables des données à caractère personnel. La CJUE semble toutefois avoir adopté, au cours d'une série d'arrêts récents, un virage en matière de droit d'accès.

Une « donnée à caractère personnel » se conçoit comme une « toute information » (art. 4 (1) RGPD) relative à une personne physique identifiée ou identifiable, directement ou indirectement. Une fois son identité vérifiée (pour éviter que la demande d'accès se transforme en faille de sécurité béante) cette personne physique doit pouvoir accéder à ces informations qui la concernent de manière claire et intelligible. La CJUE a ainsi admis en 2023 que cela pouvait inclure y compris « une reproduction fidèle et intelligible de l'ensemble de ces données[10] ». La même année, la Cour précisait que le demandeur devait pouvoir accéder aux données qu'il a lui-même transmises, mais aussi à toutes les métadonnées associées à celles-ci, à toutes les données qu'un responsable du traitement aurait récupérées par des tiers et à toutes les données inférées algorithmiquement[11]. D'ailleurs, pour aider à

[8] CJUE 17 juillet 2014, Y.S. contre Minister voor Immigratie, Integratie en Asiel, aff. j. C141/12 et C372/12.

[9] CJUE 17 juillet 2014, Y.S. contre Minister voor Immigratie, Integratie en Asiel, aff. j. C141/12 et C372/12, art. 2.

[10] CJUE 4 mai 2023, CRIF, aff. C-487/21, art. 1.

[11] CJUE 7 décembre 2023, SCHUFA Holding, aff. C-634/21, pts. 23, 56 et 63.

la compréhension de ces dernières, l'alinéa 1 sous h) de l'article 15 du RGPD permet de connaître les « informations utiles concernant la logique sous-jacente » des algorithmes de décision automatisée ou de profilage. Enfin, en octobre 2024, la CJUE a jugé que « l'obligation de fournir à la personne concernée, à titre gratuit, une première copie de ses données à caractère personnel faisant l'objet d'un traitement s'impose au responsable du traitement même lorsque cette demande est motivée dans un but étranger[12] » à la vérification de la licéité d'un traitement ou de l'exactitude des données.

Le droit d'accès n'est pas pour autant absolu. L'article 23 du RGPD permet aux États membres d'adopter des restrictions, par exemple pour la sécurité ou la défense nationale. Même en dehors de ces domaines, il est possible de refuser les demandes « manifestement infondées ou excessives » (art. 12 (5) du RGPD). La communication de la copie des données doit en outre tenir compte des droits des tiers : droit, notamment à la vie privée, des autres personnes concernées par le même jeu de données ; mais aussi droit de la propriété intellectuelle ou secret des affaires. Néanmoins, un responsable du traitement est alors « tenu de communiquer [l]es informations prétendument protégées à l'autorité de contrôle ou à la juridiction compétente, auxquelles il incombe de pondérer les droits et les intérêts en cause aux fins de déterminer l'étendue du droit d'accès de la personne concernée[13] ». Enfin, l'article 15 (3) du RGPD permet de facturer les « frais […] basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée », mais ceux-ci doivent demeurer « raisonnables » et cela ne concerne de toute façon pas les nouvelles demandes pouvant intervenir à « intervalles raisonnables » (cons. 63 du RGPD).

La principale limite reste que l'accès transparent à ses propres données ne permet pas toujours une véritable compréhension des enjeux collectifs soulevés par les rapports de pouvoir institués par les algorithmes des grandes plateformes, même si elle reste intéressante. En 2019, Judith Duportail (2019) publiait par exemple une enquête sur l'algorithme de l'application de rencontre Tinder, à partir de l'exégèse des seules données associées à son propre profil. Mais comme l'ont rappelé la Cnil et le Défenseur des Droits (DDD) dans un rapport conjoint de 2020 : « les effets discriminatoires des algorithmes ne sont bien souvent mesurables par les chercheurs qu'à l'échelle des groupes » (Cnil et DDD, p. 6). Une solution est que des individus se constituent en collectifs pour partager leurs données – récupérées par le droit d'accès de l'article 15 du RGPD, ou l'un des autres mécanismes d'accès aux données précédemment discutés – pour en examiner et en comprendre ensemble les effets (Mahieu, Ashgari et van Eeten, 2018). Cela peut se faire, le cas échéant, avec l'appui d'organisations de la société civile et de laboratoires de recherche, comme l'ont fait, en Suisse, un collectif de chauffeurs travaillant pour la plateforme Uber (Pidoux, Dehaye et Gursky, 2024), leur permettant notamment de calculer le ratio entre le temps passé à travailler sans être payé (entre deux courses) et le temps rémunéré.

Conclusion

Le droit d'accès aux données personnelles permet donc aujourd'hui, compte tenu de l'évolution des textes et de la jurisprudence, d'ouvrir des pistes pour, au-delà de la transparence que ce droit offre aux individus, construire une compréhension collective des rapports de pouvoir institués par les plateformes. Cette démarche pourra être utilement appuyée par la poursuite de la stratégie des autorités de protection des données européennes, qui ont publié, début 2025 (CEPD, 2025), un rapport sur des actions coordonnées de contrôle du respect du droit d'accès. Enfin, l'entrée en application à venir des dispositions du DSA permettant l'accès à des chercheurs agréés aux données des très grandes plateformes en

[12] CJUE 26 octobre 2023, FT contre DW, aff. C-307/22, art. 1.

[13] CJUE 27 février 2025, Dun & Bradstreet Austria GmbH, aff. C-203/22, art. 2.

ligne devrait compléter le dispositif existant et faciliter cette compréhension collective du pouvoir des plateformes, renforçant ainsi pour les plus puissantes d'entre elles les possibilités déjà offertes par le RGPD.

Références citées

BADOUARD R. (2020), *Les nouvelles lois du web : modération et censure*, La République des idées. Paris, Seuil.

BRUNS A. (2019), "After the 'APIcalypse': Social media platforms and their fight against critical scholarly research", *Information, Communication & Society*, vol. 22, n°11, pp. 15441566.

CEPD (Comité européen de protection des données) (2025), "2024 Coordinated Enforcement Action. Implementation of the right of access by controllers", Adopté le 16 janvier.

CNIL (Commission nationale de l'informatique et des libertés) et DDD (Défenseur des droits) (2020), « Algorithmes : prévenir l'automatisation des discriminations ».

CUSTERS B. & VRABEC H. (2024), "Tell me something new: data subject rights applied to inferred data and profiles", *Computer Law & Security Review*, vol. 52,105956.

DUPORTAIL J. (2019), *L'amour sous algorithme*, Paris, Éditions Goutte d'or.

MAHIEU R., ASHGARI H. & VAN EETEN M. (2018), "Collectively exercising the right of access: individual effort, societal effect", *Internet Policy Review*, vol. 7, n°3.

NIEBORG D., POELL T., CAPLAN R. & VAN DIJCK J. (2024), "Introduction to the Special Issue on locating and theorising platform power", *Internet Policy Review*, vol. 13, n°2.

PIDOUX J., DEHAYE P-O. & GURSKY J. (2024), "Governing work through personal data: The case of Uber drivers in Geneva", *First Monday*, vol. 29, n°2.

ROUVROY A. & BERNS T. (2013), « Gouvernementalité algorithmique et perspectives d'émancipation : Le disparate comme condition d'individuation par la relation ? », *Réseaux*, n°177, pp. 163-196.

SRNICEK N. (2019), *Platform Capitalism*, Cambridge Malden, Polity.

Les acteurs visés par la législation européenne sur la cybersécurité

Par Michel SÉJEAN
Professeur agrégé de droit privé et sciences criminelles,
Université Sorbonne Paris Nord, IRDA (UR 3970)

Il est impossible de dresser une liste exhaustive, ou même une simple typologie des acteurs visés par les douze textes sur la cybersécurité qui marquent la première moitié de la Décennie numérique. Ces acteurs sont si nombreux, que les architectes de ce monument normatif sont loin d'avoir tout anticipé. Des impensés apparaissent, tant au niveau de la qualification des acteurs concernés que du régime juridique qui correspond.

« Droit et passion du droit sous la Décennie numérique » : si l'on s'autorisait à pasticher le titre du célèbre ouvrage paru il y a trente ans sous la plume du Doyen Carbonnier[1], ce pourrait être l'intitulé d'une monographie à propos de l'emballement législatif qui s'aggrave depuis 2020 en droit de la cybersécurité. Bien malin qui pourrait dresser une liste exhaustive, ou même une simple typologie des acteurs visés par cette ardeur législative : cet exercice relève de la gageure ! Ces acteurs sont si nombreux, que les architectes de ce monument normatif sont loin d'avoir tout anticipé. Des impensés apparaissent, tant au niveau de la qualification des acteurs concernés que du régime juridique qui correspond.

La Décennie numérique est une stratégie de l'Union européenne qui vise à atteindre un objectif numérique en 2030 : « L'Europe veut donner aux entreprises et aux citoyens les moyens d'agir dans un avenir numérique durable, centré sur l'humain et plus prospère », écrit la Commission européenne sur son site internet[2]. En réalité, l'avenir numérique que propose l'Union européenne va de pair avec un risque accru de cyberattaques et d'incidents de sécurité informatique[3]. Une illustration parmi d'autres : lorsque l'Union européenne vise l'adoption de technologies qui transforment l'activité numérique des entreprises, elle fixe comme objectif que « 75 % des entreprises de l'UE utilisent l'informatique en nuage, l'IA ou les mégadonnées »[4]. La surface d'exposition au risque cyber a donc vocation à augmenter de manière continue, et la production de règles préventives et curatives ne

[1] J. Carbonnier, *Droit et passion du droit sous la V^e^ République*, coll. « Forum », Flammarion, 1996, 273 pages.

[2] Site de la Commission européenne, dernière consultation le 10 mai 2025, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr

[3] Les cyberattaques sont des menaces volontaires à la cybersécurité, tandis que les incidents de sécurité informatique renvoient plutôt aux événements involontaires qui mettent en danger la cybersécurité (pannes, négligences, avaries, catastrophes naturelles, etc.).

[4] Site de la Commission européenne, préc., https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr

pouvait que s'emballer. Nous voici donc au mitan de cette Décennie numérique 2020-2030, et trois ans seulement après la déclaration européenne sur les droits et principes numériques du 15 décembre 2022, aux termes de laquelle les États membres s'engagent notamment à « garantir un environnement numérique sûr et sécurisé » (art. 11, a)[5].

Quel est l'état d'esprit des acteurs visés par la législation européenne qui incarne la stratégie de la Décennie numérique ? Reconnaissons-le, ce sont actuellement la lassitude, la surcharge cognitive et la perte de sens qui dominent. Dans les trois dernières années, douze textes aussi fondateurs que la Loi des Douze Tables ont fait leur irruption dans l'organisation interne d'entités[6] déjà mises à l'épreuve par le déploiement du RGPD (2016), de la première directive sur la sécurité des réseaux d'information (dite directive SRI, ou NIS, 2016) et du règlement européen sur la cybersécurité (2019)[7]. Les douze textes entrés en vigueur entre 2022 et 2025 forment ainsi un véritable monceau législatif sans équivalent dans l'histoire récente. Les acteurs concernés ne savent cependant pas toujours qu'ils sont assujettis à certains textes, et l'on peut citer au moins un cas où une règle importante fait la démonstration de ses limites au moment d'être mise en œuvre. C'est dire que des impensés affaiblissent l'opération de qualification juridique et la mise en œuvre du régime juridique applicable aux acteurs concernés.

Un labyrinthe de qualifications juridiques

Qui est concerné ? Les mots se font de plus en plus abstraits pour capturer la variété croissante d'acteurs que vise cet amas de textes, alors que le risque systémique de cyberattaques est, lui, toujours plus concret. Un texte incarne mieux que d'autres la difficulté de l'opération de qualification juridique : le règlement sur la cyberrésilience, qui porte principalement sur la cybersécurité des produits connectés[8]. Non seulement les définitions des acteurs concernés forment un catalogue de qualifications juridiques abstraites juxtaposées les unes à côté des autres, mais ces définitions s'emboîtent, se ramifient, et se renvoient parfois l'une à l'autre, laissant au lecteur la charge de se rendre dans une directive pour trouver le texte de la définition contenue dans un règlement.

Voyez l'article 3 du règlement sur la cyberrésilience : il comporte cinquante et une définitions. Au paragraphe 12 de cet article 3, l'« opérateur économique » est défini comme étant « le fabricant, le mandataire, l'importateur, le distributeur ou une autre personne physique ou morale soumise à des obligations liées à la fabrication de produits comportant des éléments numériques ou à la mise à disposition sur le marché de produits comportant des éléments numériques conformément au présent règlement ».

---

[5] Déclaration européenne des droits et principes numériques pour la Décennie numérique, 2023/C 23/01, 15 décembre 2022, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32023C0123(01)

[6] « Entité » : voir spéc. Directive (UE) n°2022/2555 du Parlement européen et du Conseil, 14 décembre 2022, concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2), dont l'article 6 point 38 définit une « entité » comme étant « une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations ». Cela renvoie concrètement aux entreprises, aux associations, aux administrations, aux hôpitaux, ou encore aux collectivités locales.

[7] Pour une présentation des quinze textes de législation européenne entre 2016 et 2025, voir le tableau, réalisé par l'auteur de ces lignes.

[8] Règlement du Parlement européen et du Conseil concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n°168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience).

Mais qu'est-ce qu'un fabricant, un mandataire, un importateur, ou encore un distributeur ? Les paragraphes 13 et suivants de l'article 3 ramifient la définition de l'opérateur économique. Par exemple, un fabricant est « une personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et les commercialise sous son propre nom ou sa propre marque, à titre onéreux, monétisé ou gratuit » (art. 3§13). Sur le même mode, les définitions du mandataire, d'importateur et de distributeur sont données aux paragraphes 15, 16 et 17. Après ce fastidieux inventaire, l'on aurait tort de se croire au bout de sa peine : il faut encore digérer la définition d'un « intendant de logiciels ouverts » (art. 3§14) ou encore d'un « organisme d'évaluation de la conformité » (art. 3§28), d'un « organisme notifié » (art. 3§29) ou encore d'un « CSIRT désigné comme coordinateur » (art. 3§51). Les lectrices et les lecteurs des *Annales des Mines* seront certainement plus à l'aise avec les CSIRT que ne le sont les juristes en charge du déploiement des mesures prévues par ce règlement[9]. Si ces mêmes juristes voulaient trouver un éclairage dans la définition du « CSIRT désigné comme coordinateur », avertissons-les sans tarder : ils seront déçus ! En effet, la définition qu'en donne l'article 3§51 semble tout droit sortie des Douze Travaux d'Astérix, où l'irréductible Gaulois se trouve piégé dans un labyrinthe administratif qui le renvoie de bureau en bureau : c'est ainsi qu'un « CSIRT désigné comme coordinateur » est défini comme « un CSIRT désigné comme coordinateur conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555 » (art. 3§51). Autrement dit : débrouillez-vous !

À côté des cas où il est ardu de rattacher la situation d'une entité à une ou plusieurs qualifications juridiques, un problème d'une autre nature se dessine à l'horizon. Une catégorie d'entreprises n'est pas toujours au courant qu'elle est assujettie à certains textes : il s'agit des entreprises qui contribuent à la « chaîne d'approvisionnement » des entités essentielles (EE) importantes (EI) d'après la directive SRI 2[10], ou qui sont des « prestataires tiers de services numériques » au sens du règlement DORA sur la cybersécurité des services financiers.

L'article 21 de la directive SRI 2 énonce, en effet, que les entités essentielles et importantes doivent prendre des mesures de gestion des risques en matière de cybersécurité concernant « la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs » (art. 21§2, d). Si la réglementation du risque cyber dans les chaînes d'approvisionnement est une des questions les plus sensibles de la Décennie numérique[11], c'est sans aucun doute parce que les entreprises de la chaîne d'approvisionnement sont difficiles à identifier : jusqu'à quel rang une entreprise sous-traitante ou prestataire tierce à l'entité assujettie doit-elle être aspirée dans le champ d'application de la directive SRI 2 ? Le rang 1 ? Sans aucun doute ! Mais ensuite ? Jusqu'au rang 10 ? 100 ? Il faudra sans doute que des lignes directrices précisent qui fait partie des acteurs concernés par la directive SRI 2, à moins que ce ne soit le contentieux qui s'en occupe.

---

[9] Voir spéc. pour plus d'informations sur les CSIRT, M. Séjean, « Tiers de confiance numérique et centres de réponse aux incidents de sécurité informatique (CSIRT) », Dalloz IP/IT, décembre 2024, p. 641 s, https://shs.hal.science/halshs-04836188v1

[10] Voir l'article 3 (« Entités essentielles et importantes ») de la Directive (UE) n°2022/2555 du Parlement européen et du Conseil, 14 décembre 2022, préc.

[11] Voir, pour aller plus loin, E. Buisson, *La réglementation relative au risque de cyberattaques au sein des chaînes d'approvisionnement*, Thèse dactyl., Université Bretagne-Sud, Chaire Cyber de l'IHEDN, avril 2025, dir. M. Séjean, 309 pages.

Présentation des quinze textes de législation européenne entre 2016 et 2025

	Nom du texte	Type	Date d'entrée en vigueur	Textes d'application adoptés par l'UE ?
1	Règlement général sur la protection des données (RGPD) (UE 2016/679)	Règlement	24 mai 2016	Aucun règlement d'application spécifique, mais actes délégués/exécution sur points précis
2	Directive sur la sécurité des réseaux et des systèmes d'information (NIS 1) (UE 2016/1148)	Directive	8 août 2016	N/A
3	Règlement sur la cybersécurité (Cybersecurity Act) (UE 2019/881, création de l'ENISA)	Règlement	27 juin 2019	Oui : schémas européens de certification (EUCC, EUCS, etc.)
Début de la Décennie numérique 2020-2030				
4	Règlement sur la gouvernance des données (Data Governance Act) (UE 2022/868)	Règlement	23 juin 2022	Oui : actes d'exécution et délégués sur l'enregistrement, etc.
5	Règlement sur les services numériques (Digital Services Act, DSA) (UE 2022/2065)	Règlement	16 novembre 2022	Oui : actes d'exécution sur rapports de transparence, coopération
6	Directive sur la résilience des entités critiques (REC) (UE 2022/2557)	Directive	16 janvier 2023	N/A
7	Directive sur des mesures destinées à assurer un niveau élevé commun de cybersécurité (NIS 2) (UE 2022/2555)	Directive	16 janvier 2023	N/A

	Nom du texte	Type	Date d'entrée en vigueur	Textes d'application adoptés par l'UE ?
8	Règlement sur la résilience opérationnelle numérique du secteur financier (DORA) (UE 2022/2554)	Règlement	16 janvier 2023	Oui : actes délégués, normes techniques (RTS/ITS)
9	Directive sur la résilience opérationnelle numérique du secteur financier (DORA) (UE 2022/2556)	Directive	16 janvier 2023	N/A
10	Règlement sur les données (Data Act) (UE 2023/2854)	Règlement	11 janvier 2024	Oui : actes d'exécution attendus, non encore adoptés
11	Règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (UE/Euratom 2023/2841)	Règlement	7 janvier 2024	Oui : actes d'exécution attendus, non encore adoptés
12	Règlement sur l'intelligence artificielle (AI Act) (UE 2024/1689)	Règlement	11 juillet 2024	Oui : actes délégués/exécution prévus, encore en préparation
13	Directive sur la responsabilité du fait des produits défectueux (UE 2024/2853)	Directive	9 décembre 2024	N/A
14	Règlement sur la cyberrésilience (Cyber Resilience Act, CRA) (UE 2024/2847)	Règlement	10 décembre 2024	Oui : actes délégués/exécution attendus, non encore adoptés
15	Règlement sur la solidarité en matière de cybersécurité (Cyber Solidarity Act, CSA)	Règlement	4 février 2025	Oui : actes d'exécution attendus, non encore adoptés

La directive SRI 2 aurait pu s'inspirer du mécanisme mis en place par le règlement DORA sur la cybersécurité des services financiers[12]. Ce règlement comporte, lui aussi, des dispositions spéciales sur les « prestataires tiers de services TIC [Technologies d'Information et de Communication] ». Mais son article 28§1, a) énonce clairement que l'assujetti à DORA est responsable des vulnérabilités de sa chaîne d'approvisionnement : « 1. Les entités financières gèrent les risques liés aux prestataires tiers de services TIC en tant que partie intégrante du risque lié aux TIC dans leur cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1, et conformément aux principes suivants : a) les entités financières qui ont conclu des accords contractuels pour l'utilisation de services TIC dans le cadre de leurs activités restent à tout moment pleinement responsables du respect et de l'exécution de toutes les obligations découlant du présent règlement et du droit applicable aux services financiers ». Pourquoi ne pas l'avoir indiqué également dans la directive SRI 2 ? La chaîne d'approvisionnement d'une entité essentielle ou importante – l'on parle de 100 000 entités dans toute l'Union européenne – aurait dû faire l'objet de précisions sur ce point, car si une entreprise ne sait pas qu'elle est concernée par un texte, il y a peu de chances qu'elle s'y conforme. À ces difficultés concernant la qualification juridique des acteurs concernés par la législation de droit de la cybersécurité en Union européenne, il faut ajouter un impensé au niveau du régime juridique.

Un impensé dans le régime juridique applicable aux acteurs concernés

Bien que la France n'ait pas encore transposé dans son droit interne la directive SRI 2, les entreprises ont commencé à s'organiser avec les textes dont elles disposent. Le point d'entrée pour une entité concernée par la directive, c'est l'enregistrement auprès de l'autorité compétente : par exemple, si une entreprise française, établie en France, est une entité essentielle ou importante, elle doit s'enregistrer auprès de l'ANSSI. Mais le texte qui impose cet enregistrement, l'article 26 de la directive SRI 2, n'a pas été pensé pour les multinationales qui opèrent dans plusieurs États membres de l'Union européenne.

Il dispose que : « Les entités relevant du champ d'application de la présente directive sont considérées comme relevant de la compétence de l'État membre dans lequel elles sont établies, à l'exception des cas suivants : (…) ». Une multinationale ayant des activités dans tous les pays de l'Union européenne doit-elle donc s'enregistrer vingt-sept fois ? Peut-elle centraliser tous les enregistrements auprès de l'ANSSI, si le siège de ses activités est en France ? Oui, elle le peut, mais seulement dans trois séries de cas exceptionnels (art. 26§1 a), b) et c). Or, de nombreuses entreprises de la Base Industrielle et Technologique de Défense (BITD) sont dans une situation administrative difficile : elles remplissent parfois les critères de l'exception qui permettrait de centraliser les enregistrements auprès de l'ANSSI, mais pas pour toutes leurs activités, si bien qu'elles doivent à la fois enregistrer leurs activités auprès des vingt-sept ANSSI européennes, et parfois centraliser certains enregistrements auprès de l'ANSSI française pour les activités qui remplissent les critères des exceptions.

Dans ces conditions, l'Union européenne est en train de créer ce contre quoi elle prétend lutter dans le cadre de ses compétences de protection du marché intérieur (art. 114 TFUE). L'Union européenne était censée protéger les entreprises naissantes de la prédation par les mastodontes qui ont tant de fois racheté leurs concurrents pour neutraliser

[12] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, spéc. Chapitre V « Gestion des risques liés aux prestataires tiers de services TIC ».

les produits qui menaçaient les leurs. Mais avec douze textes gigantesques sur le droit de la cybersécurité entrés en vigueur en trois ans, quel est l'intérêt, pour une entreprise naissante, de croître jusqu'à être assujettie à certains de ces textes européens sur la cybersécurité. Ne vaut-il pas mieux que ces jeunes pousses se fassent racheter par une grande entreprise à la puissance administrative capable de soulever une montagne juridique, en espérant que la montagne n'accouche pas d'une souris économique ?

Le Droit de la Compliance, clé de voute de la Régulation de l'intelligence artificielle

Par Alex NICOLLET
Junior Editor du *Journal of Regulation & Compliance* (JoRC)
Doctorant en Droit à l'Université Jean Moulin Lyon 3

Face aux risques inhérents à l'espace numérique en général et à l'intelligence artificielle en particulier, s'est progressivement constitué, brique par brique, un *corpus* de règles visant à détecter et prévenir ces risques. Cette construction, émanant principalement de l'Union européenne, s'inscrit dans un ensemble plus vaste : le Droit de la Compliance. Les règles qui le composent ont en commun des méthodes et outils, et surtout une finalité : préserver les systèmes et/ou les améliorer afin que les êtres humains impliqués soient préservés.

L'Europe a ainsi constitué un modèle reposant sur un équilibre entre liberté et protection des personnes, c'est-à-dire un modèle de Régulation. Cette Régulation est intégrée directement dans les opérateurs contrôlant les systèmes en cause, leur imposant de détecter, prévenir, et le cas échéant réparer et remédier aux risques générés, faisant de cette Régulation non seulement un élément mais encore un exemple du Droit de la Compliance.

La création par les opérateurs de systèmes incorporels, détachés de toute emprise territoriale, déployés à l'échelle mondiale

Après la révolution des technologies de l'information et de la communication (TIC), qui a permis la création par les entreprises d'espaces virtuels, par nature a-territoriaux, dont elles ont l'entière maîtrise[1], la révolution de l'intelligence artificielle (IA)[2] aboutit à la création de modèles et systèmes d'intelligence artificielle déployés dans cet espace numérique à une échelle mondiale. Ces technologies ne sont pas neutres ; leur conception, leur développement et leur utilisation sont vecteurs d'externalités négatives, notamment de risques pour les personnes.

Le choix européen de réguler l'IA, conciliant liberté et protection de la personne

Face à cet état de fait et à ces risques, plusieurs options s'offrent aux autorités publiques. Ne pas encadrer ces innovations, les laissant se développer librement, engendrer des

[1] Voir notamment M.-A. Frison-Roche (dir.) (2016), *Internet, espace d'interrégulation*, Dalloz, coll. « Thèmes & Commentaires », série « Régulations », 208 pages.

[2] Sur la révolution de l'IA, voir la Commission de l'intelligence artificielle, présidée par Ph. Aghion et A. Bouverot, « IA : notre ambition pour la France », Rapport remis au Premier ministre, mars 2024, p. 20.

risques, causer des dommages, puis les réparer de manière plus ou moins satisfaisante ; en soutenant notamment qu'il ne serait pas raisonnable d'encadrer par anticipation un objet nouveau n'ayant pas atteint son plein développement. L'approche américaine en relève. À l'inverse, les autorités peuvent décider que ces dommages ne peuvent survenir, car trop graves, notamment en ce qu'ils affectent les personnes. Il faut alors encadrer, en *ex ante*, le développement et l'utilisation de ces innovations. Tel est le choix fait par l'Europe, laquelle repose sur un projet humaniste, plaçant la personne humaine en son centre[3]. Se pose alors la question de l'équilibre entre la liberté d'une part, notamment la libre concurrence, et la protection des personnes d'autre part. Cette conciliation entre la concurrence et un principe a-concurrentiel, inhérente à la Régulation[4], laquelle est prolongée et dépassée par la Compliance[5], est au cœur du dispositif encadrant l'IA[6].

L'encadrement de l'intelligence artificielle : une superposition de textes spéciaux propres à l'IA, de textes spéciaux concernant indirectement l'IA et du droit commun

Trois catégories de textes forment le cadre juridique. D'abord, des textes ayant pour objet l'IA, tel que le règlement sur l'intelligence artificielle (RIA)[7], qui constitue une sorte de « droit commun de l'IA »[8], ou la nouvelle directive sur les produits défectueux[9]. Ensuite, des textes concernant indirectement l'IA, qu'ils la visent expressément, comme le règlement Cyberrésilience[10], ou non, comme le RGPD[11]. En effet, l'IA ne pouvant fonctionner qu'en intégrant une masse importante de données, tous les textes ayant trait aux données (RGPD, Data Act, etc.) s'appliquent indirectement à l'IA. De plus, son utilisation peut

[3] M.-A. Frison-Roche (dir.) (2019), *Pour une Europe de la Compliance*, Dalloz, coll. « Thèmes & Commentaires », série « Régulations & Compliance », 124 pages.

[4] M.-A. Frison-Roche (2001), « Le droit de la régulation », *Recueil Dalloz, Chronique*, 2001, pp. 610-616.

[5] M.-A. Frison-Roche (dir.) (2017), *Régulation, Supervision, Compliance*, Dalloz, coll. « Thèmes & Commentaires », série « Régulations », 148 pages.

[6] Le RIA dispose par exemple dans son article 1er, définissant son « objet », que : « L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle (IA) axée sur l'humain et digne de confiance, tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, notamment la démocratie, l'État de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation ».

[7] Règlement (UE) 2024/1689, 13 juin 2024, établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle – RIA ; en anglais Artificial Intelligence Act – IA Act).

[8] S. Merabet (2024), « Des vertus et des vices du règlement sur l'intelligence artificielle », *Recueil Dalloz* 2024, pp. 2017-2020.

[9] Directive (UE) 2024/2853, 23 octobre 2024, relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil. Bien que s'appliquant au-delà de l'IA, la nouvelle version de ce texte a été pensée spécifiquement pour saisir l'IA, ce qui justifie son classement dans cette catégorie.

[10] Règlement (UE) 2024/2847, 23 octobre 2024, concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques (règlement sur la cyberrésilience), art. 12.

[11] Règlement (UE) 2016/679, 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 (RGPD).

relever de règles spécifiques, comme le *Digital Services Act*[12]. Enfin, l'IA n'étant qu'un objet comme un autre, le Droit commun, par exemple des contrats ou de la responsabilité, s'applique. L'ensemble forme le « droit de l'intelligence artificielle »[13]. L'on se concentrera ici sur le premier *corpus*, part du Droit de la Compliance, part de ce « puzzle européen »[14], consistant en *ex ante* à détecter et prévenir les risques et en *ex post* à les réparer s'ils se sont matérialisés en dommages et à y remédier afin qu'à l'avenir ils ne se reproduisent plus.

Le dispositif encadrant l'intelligence artificielle : élément du Droit de la Compliance

De l'impératif de distinguer Compliance et conformité, condition pour appréhender les obligations pesant sur les opérateurs

Bien que souvent confondues – certains expliquant que la conformité serait la traduction française du mot anglais « *compliance* » –, la Compliance et la conformité sont deux notions distinctes. La « conformité » consiste pour un opérateur à respecter en permanence l'ensemble de la réglementation qui lui est applicable et à le démontrer en *ex ante*[15]. À cet égard, l'intelligence artificielle joue un double rôle. D'abord, en tant qu'outil de conformité : cette obligation, de fait impossible, de conformité nécessitant dans un premier temps une connaissance parfaite de l'ensemble des réglementations applicables, puis dans un second temps une mise en œuvre mécanique de celles-ci, laquelle ne pourrait être réalisée que par le biais d'algorithmes réduisant ces réglementations en masses de données et détectant de possibles non-conformités[16]. Ensuite, en tant qu'objet de conformité : d'aucuns réduisant le « droit de l'intelligence artificielle » à des réglementations auxquelles il conviendrait de se conformer. S'il est vrai que les opérateurs doivent respecter les règles de Droit auxquelles ils sont assujettis en matière d'IA, cela est vrai de l'ensemble des règles de Droit et ne renseigne pas sur l'objet de ces règles, ce qui en conséquence ne permet pas de rendre compte de la substance des obligations pesant sur les opérateurs. Si la technique de conformité existe et est un élément important du RIA, celle-ci n'est précisément qu'un outil, permettant aux opérateurs, de gré ou de force, de satisfaire à leurs obligations substantielles.

[12] Règlement (UE) 2022/2065, 19 octobre 2022 relatif à un marché unique des services numériques (en anglais *Digital Services Act* - DSA).

[13] Sur la constitution d'un « droit de l'intelligence artificielle » au-delà de la réglementation, voir S. Merabet, *Vers un droit de l'intelligence artificielle*, préface H. Barbier, Dalloz, coll. « Nouvelle Bibliothèque de Thèses », vol. 197, 2020, 592 pages.

[14] M.-A. Frison-Roche, « La vigilance, pièce d'un puzzle européen », *in* I. Grossi (dir.), dossier *« La société vigilante »*, JCP E, 3 août 2023, n°31-35, étude 1247, pp. 57-58.

[15] M.-A. Frison-Roche (2024), « Compliance et conformité : les distinguer pour les articuler », *Recueil Dalloz, Chronique*, 2024, pp. 497-499.

[16] *Ibid*.

Droit de la Compliance et *corpus* encadrant l'IA : des caractéristiques communes

Loin de se résumer à la « conformité », le Droit de la Compliance constitue une branche du Droit substantielle, trouvant son unité dans ses « Buts Monumentaux »[17], visant à détecter et prévenir les risques systémiques afin qu'à l'avenir les systèmes ne s'effondrent pas (« Buts Monumentaux négatifs »), voire s'améliorent (« Buts Monumentaux positifs »)[18]. Il repose sur l'internalisation dans les opérateurs en position d'agir de l'obligation de tendre à la concrétisation de ces buts, afin que les systèmes s'inscrivent dans le temps (durabilité), impliquant une analyse systémique. Le droit de l'IA l'illustre.

Le *corpus* encadrant l'IA : un Droit de nature systémique

Le Droit de la Compliance est par nature systémique, en ce qu'il a pour objet les systèmes[19]. Ce caractère systémique est inhérent à la régulation de l'IA, les textes appréhendant principalement celle-ci à travers la notion clé de « système d'intelligence artificielle » (SIA)[20]. En outre, le RIA prévoit des obligations particulières pour les « modèles d'IA à usage général »[21], obligations renforcées lorsque ceux-ci présentent des « risques systémiques »[22]. Le Droit cherche ainsi à agir sur ces systèmes, en obligeant les opérateurs à les renforcer, notamment au regard des exigences de cybersécurité, à éliminer les risques de biais, etc., afin que les personnes qu'ils impliquent (dont les données sont traitées par ces systèmes ou qui risquent de subir les conséquences de l'utilisation de ces systèmes, etc.) soient préservées.

Le *corpus* encadrant l'IA : le recours aux Outils de Compliance pour réguler l'IA

Le RIA a recours à de nombreux Outils de Compliance[23]. En premier lieu, le texte impose par exemple aux fournisseurs de SIA à haut risque (SIAHR) de mettre en place un « système de gestion des risques », lequel implique d'identifier, analyser et évaluer les risques liés au système[24], c'est-à-dire de réaliser une cartographie des risques, outil

---

[17] M.-A. Frison-Roche (2022), « Les Buts Monumentaux, cœur battant du Droit de la Compliance », *in* M.-A. Frison-Roche (dir.), *Les Buts Monumentaux de la Compliance*, JoRC et Dalloz, coll. « Régulations & Compliance », 2022, pp. 21-44.

[18] *Ibid*.

[19] M.-A. Frison-Roche (2016), « Le Droit de la compliance », *Recueil Dalloz, Chronique*, 2016, pp. 1871-1874.

[20] RIA, article 3, 1) : « un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels ».

[21] La notion de modèle d'IA a été introduite dans la version finale du RIA et vise un élément d'un SIA, un logiciel de base ensuite auxquels doivent être ajoutés d'autres composantes pour constituer un SIA ; voir en ce sens Th. Bonneau (2024), « Le règlement IA du 13 juin 2024 », *Revue de Droit bancaire et financier*, novembre-décembre 2024, n°6, étude 10, pp. 31-36.

[22] RIA, art. 51 et s.

[23] Sur cette notion, voir M.-A. Frison-Roche (dir.) (2021), *Les outils de la Compliance*, JoRC et Dalloz, coll. « Régulations & Compliance », 2021, 323 pages.

[24] RIA, art. 9.

premier du Droit de la Compliance[25]. En considération de celle-ci, les opérateurs doivent adopter des « mesures appropriées » c'est-à-dire des mesures propres à prévenir ces risques. La technique du *comply or explain* est également mobilisée par le texte, avec des normes techniques, dites « normes harmonisées », dont le respect engendre une présomption de conformité aux exigences essentielles[26]. Le RIA impose par ailleurs aux fournisseurs de SIAHR de mettre en place « un système de gestion de la qualité garantissant le respect du […] règlement », lequel se matérialise notamment par des politiques, des procédures et des instructions écrites[27]. Ce faisant, il ne fait rien d'autre qu'obliger cette catégorie d'opérateur à mettre en place des programmes de compliance[28]. La formation, outil central du Droit de la Compliance[29], est également mobilisée par le RIA, les personnels utilisant l'IA devant disposer des compétences et de la formation nécessaires pour maîtriser l'IA[30], cette formation pouvant le cas échéant être réalisée par le fournisseur lui-même au profit du déployeur[31].

Le *corpus* encadrant l'IA : le rôle central de l'information dans la Régulation de l'IA

L'information est un élément central dans la régulation de l'IA et ce à un double titre. En premier lieu, l'information est l'objet même d'un SIA, lequel est entraîné à partir de quantités massives de données, afin dans un second temps d'être en mesure de produire un résultat à partir de données d'entrée. Cette information est encadrée, en ce qu'elle permet indirectement de réguler le SIA lui-même. C'est à ce titre que plusieurs obligations consistent à imposer aux opérateurs de contrôler les données implémentées, afin que celles-ci soient pertinentes, suffisamment représentatives et exemptes d'erreurs[32]. Lorsque ces informations relèvent de la catégorie des données personnelles, non-seulement le Droit propre à celles-ci trouve à s'appliquer, mais en outre le RIA prévoit des obligations supplémentaires[33], en raison des risques pour les personnes inhérents à ce type d'information. En second lieu et au-delà, l'information est au cœur des obligations imposées par le RIA aux opérateurs, que celle-ci porte sur le SIA, les risques qu'il génère ou même l'information des tiers, durant l'ensemble des stades de vie du système (développement et fonctionnement) ; ces obligations étant tournées vers une même finalité : détecter afin de prévenir les risques générés par le SIA. Ainsi, en amont de la mise sur le marché ou en service, le fournisseur doit identifier les risques liés au SIAHR[34] – en collectant et traitant de l'information, en vue dans un second temps d'agir en considéra-

[25] M.-A. Frison-Roche, « Théorie juridique de la cartographie des risques, centre du Droit de la Compliance », *Recueil Dalloz, Chronique*, 2019, pp. 2432-2434.

[26] RIA, art. 40.

[27] RIA, art. 17.

[28] Sur l'analyse des textes qui, sous différentes appellations (plan, programme, code de conduite), imposent une telle obligation à l'entreprise, voir M.-A. Frison-Roche, « Obligation de Compliance : construire une structure de compliance produisant des effets crédibles au regard des Buts Monumentaux visés par le Législateur », *in* M.-A. Frison-Roche (dir.), *L'Obligation de Compliance*, JoRC et Dalloz, coll. « Régulations & Compliance », 2025.

[29] M.-A. Frison-Roche, « La formation : contenu et contenant de la Compliance », *in* M.-A. Frison-Roche (dir.), *Les outils de la Compliance*, *op. cit*., pp. 227-244.

[30] Voir notamment RIA, art. 4 et 26, 2.

[31] RIA, art. 9, 5., c)

[32] Voir par exemple RIA, art. 10 (pour les fournisseurs) art. 26, 4. (pour les déployeurs).

[33] Voir par exemple RIA, art. 10, 5.

[34] RIA, art. 9 ; voir *infra*.

tion de celle-ci –, ou bien encore générer de l'information à destination de tiers dans une démarche de transparence[35]. Cette information a également des conséquences en aval, certaines obligations pesant sur les déployeurs dépendant de celle-ci. Par exemple, le déployeur doit prendre des mesures appropriées afin de garantir que le SIAHR est utilisé conformément aux notices d'utilisation établies par le fournisseur[36], ou encore surveiller le fonctionnement du SIA « sur la base de la notice d'utilisation »[37]. Plusieurs obligations d'information se déclenchent au stade de fonctionnement du SIA. Ces obligations peuvent porter sur le SIA lui-même, le fournisseur comme le déployeur devant par exemple assurer la tenue des journaux générés automatiquement par les SIA qu'ils contrôlent et retraçant leur fonctionnement[38], ou bien concerner des tiers, l'employeur déployant un SIAHR devant informer ses salariés et leurs représentants[39]. L'information collectée en aval peut par la suite avoir des conséquences sur l'amont, le déployeur devant informer le fournisseur s'il constate un risque supplémentaire ou un incident grave[40]. L'on retrouve ici la démarche de progrès permanent et d'adaptation continue aux risques, inhérente au Droit de la Compliance.

Le *corpus* encadrant l'IA : une « approche par les risques »

Le Droit de la Compliance vise à détecter et prévenir les risques systémiques. Pour ce faire, il impose aux opérateurs d'identifier ces risques puis d'agir en conséquence, afin que ceux-ci ne se matérialisent pas. Cette méthode est au cœur du *corpus* encadrant l'IA, lequel, tout comme plus généralement le Droit du numérique, relève d'une « approche par les risques »[41]. Ainsi, le RIA classe les SIA selon les risques qu'ils présentent et ventile les obligations en fonction de ceux-ci : les SIA à risque intolérable sont interdits *per se*[42], les SIA à haut risque sont autorisés mais particulièrement encadrés[43], les SIA à risque modéré sont autorisés mais encadrés et enfin les modèles et systèmes d'IA à usage général présentant un risque systémique justifient l'application d'obligations particulières[44].

Le *corpus* encadrant l'IA : la recherche de l'opérateur « en position » d'agir au sein de la « chaîne de valeur de l'IA »

Le Droit de la Compliance s'appuie sur les opérateurs disposant de la puissance nécessaire pour agir, transformant cette puissance en pouvoir[45], en internalisant en leur sein

[35] Voir en ce sens RIA, art. 11, qui impose l'établissement d'une documentation technique, et art. 13, qui met à la charge du déployeur des obligations de transparence.

[36] RIA, art. 26, 1.

[37] RIA, art. 26, 5.

[38] RIA, art. 19 et 26, 6.

[39] RIA, art. 26, 7.

[40] RIA, art. 26, 5.

[41] A. Latil (2024), *Le droit du numérique. Une approche par les risques*, 2e éd., Dalloz, 2024, 296 p.

[42] RIA, art. 5.

[43] RIA, art. 6 et s.

[44] RIA, art. 51 et s.

[45] Sur la notion de pouvoir, voir E. Gaillard (1985), *Le pouvoir en droit privé*, préface G. Cornu, Economica, coll. « Droit civil », série « Études et Recherches », 1985, 250 pages. ; M.-A. Frison-Roche (2021), « Concevoir le pouvoir », document de travail, décembre 2021, https://www.mafr.fr/fr/article/le-pouvoir-pour-mieux-servir/

l'obligation de participer à la réalisation des Buts Monumentaux. Les textes encadrant l'intelligence artificielle recherchent également l'opérateur idoine, afin de faire peser sur celui-ci la charge de la détection, la prévention et la réparation des risques générés par les SIA sur lesquels ils sont en position d'agir. Ainsi, le RIA impose des obligations à une série d'opérateurs composant la « chaîne de valeur de l'IA »[46] : du fournisseur de celle-ci à son déployeur et ce dans une perspective a-territoriale. Sont ainsi concernés au titre du RIA : le « fournisseur », qui crée le système d'IA et le met à disposition du public ; le « déployeur », qui utilise le SIA sous son autorité dans le cadre d'une activité à caractère professionnel ; le « mandataire », qui est désigné par le fournisseur pour s'acquitter en son nom de ses obligations ; l'« importateur », qui met sur le marché un SIA qui porte le nom ou la marque d'une personne établie dans un pays tiers ; et enfin le « distributeur », qui met le SIA à disposition sur le marché intérieur[47]. L'objectif est de saisir l'opérateur disposant effectivement du contrôle du SIA, et donc en position d'agir. Ainsi, l'opérateur concerné n'est pas nécessairement l'opérateur de grande taille, mais celui dont le comportement est susceptible d'affecter, en bien ou en mal, le système, et disposant de suffisamment de puissance pour agir effectivement pour prévenir les risques générés. Dans le même sens, la nouvelle directive sur les produits défectueux relève de cette logique, en prévoyant à titre principal la responsabilité des fabricants et assimilés (fournisseur, importateur, mandataire) et à titre subsidiaire celle des distributeurs *lato sensu*[48].

Le dispositif encadrant l'intelligence artificielle : illustration du *continuum* de Compliance

Le cadre juridique portant sur l'intelligence artificielle : alliance de l'*ex ante* et de l'*ex post*

Le *corpus* applicable à l'IA est composé de deux types de dispositions : les premières imposent aux opérateurs des obligations visant à prévenir les risques de dommages en lien avec le développement ou le fonctionnement d'un SIA, les secondes portent sur l'obligation pesant sur les opérateurs de réparer les dommages en lien avec un SIA, dommages résultant notamment de la matérialisation des risques que les opérateurs ne seraient pas parvenus à prévenir. À cet égard, le dispositif européen a été pensé en deux temps : le RIA réglant l'*ex ante*, les directives sur la responsabilité l'*ex post*[49].

Ex ante, imposer aux opérateurs de détecter et prévenir les risques générés par les SIA

Il résulte de ce qui précède que le *corpus* encadrant l'intelligence artificielle se saisit des opérateurs en position d'avoir un impact sur les SIA, et internalise en leur sein des obligations structurelles et comportementales[50] visant à prévenir les risques générés par le développement et l'utilisation de ces systèmes. Il le fait par une série d'obligations

[46] RIA, art. 25.

[47] Pour les définitions, voir RIA, art. 3.

[48] Directive (UE) 2024/2853, 23 oct. 2024, préc., art. 4.

[49] Voir en ce sens G. Loiseau (2022), « Le droit de la responsabilité civile s'adapte aux systèmes d'intelligence artificielle », novembre 2022, *Communication - Commerce électronique*, n°11, comm. 75.

[50] Sur la définition de l'Obligation de Compliance comme obligation de mettre en place des structures et comportements de Compliance, voir M.-A. Frison-Roche, « Obligation de Compliance : construire une structure de compliance produisant des effets crédibles au regard des Buts Monumentaux visés par le Législateur », préc.

s'appliquant cumulativement à raison du niveau de risque du système en cause et à raison du type d'opérateur (fournisseur, déployeur, etc.).

Ainsi, pour les SIA à risque modéré, c'est-à-dire ceux destinés à interagir avec des personnes physiques, une information spéciale doit être délivrée à l'utilisateur afin qu'il comprenne qu'il interagit avec un SIA[51].

Pour les SIA à haut risque, se superposent des obligations propres à ces systèmes et des obligations propres aux différents opérateurs. Ainsi, le RIA prévoit que dans leur conception même les SIAHR doivent respecter une série « d'exigences », comprenant : un système de gestion des risques (art. 9) ; un système de gouvernance des données d'entraînement, de validation et de test (art. 10) ; une documentation technique démontrant le respect des obligations du texte (art. 11) ; un système d'enregistrement automatique des évènements (journal) (art. 12) ; un fonctionnement transparent pour l'utilisateur (art. 13) ; un « contrôle humain », c'est-à-dire un contrôle effectif par des personnes physiques au stade de l'utilisation du SIA (art. 14) ; et, enfin, un niveau approprié d'exactitude, de robustesse et de cybersécurité (art. 15). Ces obligations, sont renforcées et complétées par des obligations s'attachant aux opérateurs, selon la catégorie à laquelle ils appartiennent. Le fournisseur d'un SIAHR doit ainsi respecter les exigences essentielles précitées, mais encore mettre en place un système de gestion de la qualité (art. 17), des mesures permettant d'enregistrer les journaux générés automatiquement par les SIA qu'ils contrôlent (art. 19) et des mesures correctives et d'information (art. 20). Les déployeurs doivent quant à eux adopter « des mesures techniques et organisationnelles appropriées », assurant le respect des notices d'utilisation, un contrôle humain effectif et efficace, un contrôle des données d'entrée, une surveillance du fonctionnement du SIAHR, la tenue des journaux, etc.[52]. Ces diverses obligations ont en commun d'être tournées vers un même objectif : détecter et prévenir les risques générés par les SIAHR.

Enfin, la mise sur le marché, la mise en service et l'utilisation de SIA à risque intolérable sont quant à elles purement interdites[53]. Il s'agit donc, en *ex ante*, de prohiber *per se* tout développement et/ou tout usage de ceux-ci. Sont ici visés des SIA particulièrement néfastes pour les personnes, portant atteinte à des droits fondamentaux et donc contraires aux valeurs de l'UE. Ils font l'objet d'une liste limitative, comprenant notamment les SIA ayant recours à des techniques subliminales, délibérément manipulatrices ou trompeuses, ceux réalisant de la notation sociale ou bien encore permettant la reconnaissance des émotions sur le lieu de travail et dans les établissements d'enseignement, etc.

Toutefois, nonobstant la mise en œuvre de l'ensemble de ces dispositions, un dommage peut survenir. *Ex post*, il doit être effectivement réparé.

Ex post, les difficultés du Droit de la responsabilité à permettre une réparation effective des dommages liés à des SIA

Les instruments traditionnels du Droit de la responsabilité civile, spéciaux comme généraux, peinent à se saisir pleinement de l'IA. Pour la responsabilité du fait des

[51] RIA, art. 50, 1.

[52] RIA, art. 26.

[53] RIA, art. 5.

produits défectueux, la possibilité même de qualifier un SIA de produit fait débat[54], sans compter que les difficultés probatoires et les exonérations de responsabilité pour risque-développement et modification postérieure à la mise sur le marché sont autant d'obstacles à la mise en œuvre de cette responsabilité spéciale. L'immatérialité du SIA nécessiterait une adaptation de la jurisprudence sur le critère de la chose, l'anormalité de sa position et sa garde[55]. Enfin, même la plasticité de la responsabilité civile délictuelle de Droit commun bute *a priori* sur l'autonomie et l'opacité de l'IA (« effet boîte noire »). La Commission européenne avait donc proposé une nouvelle version de la directive dite « produits défectueux »[56] et une directive sur l'adaptation de la responsabilité civile délictuelle à l'IA[57]. Seule la première a été adoptée, la seconde ayant été retirée dans le mouvement en faveur de la « dérégulation »[58].

Ex post, réparer les dommages générés par les SIA : la nouvelle responsabilité du fait des produits défectueux

La nouvelle version de la directive produits défectueux de 2024[59] vise donc à combler les lacunes du texte de 1985, afin d'appréhender l'IA. Les notions de produit et objet dommageable ont été élargies[60], celle de défectuosité a été étendue[61], ainsi que le nombre de responsables potentiels. Surtout, la charge de preuve de la victime est allégée par la création d'un mécanisme de divulgation réciproque[62] et des présomptions de défectuosité et de lien de causalité[63]. Enfin, elle apporte des exceptions à l'exonération pour défaut-postérieur et risque-développement[64]. L'objectif est clair : permettre une réparation effective des dommages causés par un SIA. Toutefois, outre des incertitudes quant à sa portée et des limites intrinsèques, notamment le fait qu'il ne s'applique qu'en présence

[54] Contre la qualification de produit, voir notamment J.-S. Borghetti, « L'accident généré par l'intelligence artificielle autonome », *in Le droit civil à l'ère du numérique. Actes du colloque du Master 2 Droit privé général et du Laboratoire de droit civil – Paris II – 21 avril 2017*, LexisNexis, 2017, pp. 23-28, spéc. n°29, p. 37 ; pour cette qualification voir notamment M. Bacache, « Intelligence artificielle et droit de la responsabilité et des assurances », *in* A. Bensamoun & G. Loiseau (dir.) (2019), *Droit de l'intelligence artificielle*, LGDJ, coll. « Les intégrales », 2019, p. 69 et s., spéc. n°131, p. 84.

[55] Voir sur ces points S. Lequette, *Droit du numérique*, LGDJ, coll. « Précis Domat », série « Droit privé », 2024, 858 pages, spéc. § 1495 et s.

[56] Directive (UE) 2024/2853, 23 octobre 2024, préc.

[57] Proposition de directive, relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (directive sur la responsabilité en matière d'IA), 28 septembre 2022, COM(2022) 496 final.

[58] Comm., Annexes to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission work programme 2025. Moving forward together: A Bolder, Simpler, Faster Union, 11 février 2025, COM(2025) 45 final, annexe IV.

[59] Pour une analyse du texte, C. Mangematin (2023), « Responsabilité du fait des produits défectueux et intelligence artificielle : une proposition presque parfaite », *Responsabilité civile et assurance*, juin 2023, n°6, étude 8, pp. 8-12.

[60] Directive (UE) 2024/2853, 23 octobre 2024, préc., art. 4.

[61] *Ibid*., art. 7.

[62] *Ibid*., art. 9.

[63] *Ibid*., art. 10.

[64] *Ibid*., art. 11.

d'un dommage causé à une personne physique, le texte n'a vocation qu'à concerner les produits, et donc les SIA, mis sur le marché ou en service à compter du 9 décembre 2026[65].

Ex post, réparer les dommages générés par les SIA : la responsabilité civile délictuelle pour faute

Si la directive portant adaptation de la responsabilité civile délictuelle[66] a certes été abandonnée, cela ne signifie pas pour autant une « irresponsabilité » des opérateurs. Si cette réparation ne sera pas aisée, car la responsabilité n'est plus facilitée par un texte spécial, le Droit commun demeure et implique de réparer ces dommages. En effet, la proposition de directive ne visait qu'à alléger le système probatoire. Or le juge peut de sa propre initiative procéder à un tel allégement, par des présomptions qu'il construit par des raisonnements. Il le fait depuis toujours, par exemple en concurrence déloyale où, hors de tout texte spécial, il présume l'existence d'un dommage puis affirme que la faute se déduit du préjudice, afin d'aider la victime. Qui l'empêcherait de faire de même en matière d'IA s'il pense que cela est juste ? Il peut aussi ordonner des mesures d'ordre probatoire.

Ex post, remédier aux risques et dommages générés par les SIA

L'*ex post* ne se limite pas à la réparation, il implique aussi la remédiation, c'est-à-dire l'adoption de mesures de nature à faire en sorte que le risque ou le dommage ne surviennent pas à nouveau à l'avenir. C'est à ce titre que le RIA impose aux déployeurs de SIAHR d'informer sans délai les fournisseurs s'ils constatent un risque ou un incident grave[67]. Les obligations de coopération des opérateurs avec les autorités publiques vont également dans ce sens. Il s'agit prioritairement d'agir, afin que le système soit renforcé à l'avenir et les personnes concernées indirectement préservées.

Il apparaît ainsi que l'Europe a construit un modèle qui lui est propre. Une Régulation pragmatique de l'IA, s'appuyant sur la puissance des entreprises, que celles-ci soient ou non européennes, pour que l'innovation se déploie au bénéfice des êtres humains, objectif que le Législateur est maître d'imposer, tandis que les entreprises demeurent maîtresses des moyens. Le système repose donc sur une alliance entre ces deux types d'acteurs, exprimée par des mécanismes de Compliance, dans une démarche de progrès permanent, garantissant qu'à l'avenir l'innovation se développe et les personnes soient préservées. En cela, il constitue un vecteur de souveraineté européenne.

[65] *Ibid*., art. 2.

[66] Proposition de directive sur la responsabilité en matière d'IA, préc.

[67] RIA, art. 26, 5.

ENJEUX NUMÉRIQUES

Pour une IA responsable et éthique

N°29 - Mars 2025

Ce numéro a été coordonné par
Nicolas CHAGNY

Ce numéro peut être consulté et téléchargé gratuitement
sur notre site ***http://www.annales-des-mines.org***

Droit du numérique : vers l'effacement du juge ?

Par Olivier ITEANU
Avocat à la cour d'appel de Paris

Les États membres de l'Union européenne ont abandonné aux institutions de l'Union, le privilège de réglementer le secteur du numérique. Cela aboutit depuis trente ans, à la mise en place d'une structure de réglementation qui invisibilise le système judiciaire, peuplant la réglementation d'autorités administratives indépendantes et d'organismes en tous genres. Cet article en fait le constat au travers de deux textes communautaires populaires que sont le RGPD de 2016 entré en application en 2018 et l'IA Act de 2024. Pourtant, le juge judiciaire reste toujours accessible, dans une sphère d'intervention différente. Cet article plaide pour que cette invisibilité des juges ne se transforme pas en effacement.

Introduction

Le droit du numérique[1] n'est pas une branche du droit à part entière, comme le sont notamment le droit du travail, le droit civil ou le droit pénal. Il est composé de textes épars autour de cinq thématiques : la propriété intellectuelle avec le droit du logiciel, des bases de données et les créations numériques, le droit de la donnée y compris à caractère personnel, la liberté d'expression dans le cyberspace, la cybersécurité et le commerce électronique.

Le point commun entre ces différents textes est la nécessité de composer avec un environnement technique imposé, nouveau et évolutif. L'intelligence artificielle est la dernière illustration d'un droit bousculé par le numérique. L'autre point commun est que la création de ce droit a été abandonnée par les États membres au profit des institutions de l'Union. Le droit du numérique étant récent, l'Union européenne a cherché à édicter dès l'abord des règles harmonisées au sein de l'Union[2]. Quatre conséquences sont attachées à cette évolution significative.

En premier lieu, ces textes sont négociés et rédigés en langue anglaise, ensuite traduits en français. Il n'est pas rare que les praticiens soient contraints de revenir au texte originel anglais pour l'interpréter. En second lieu, la rédaction est fleuve car le législateur communautaire doit aboutir à un consensus avec un grand nombre d'interlocuteurs, aujourd'hui au nombre de 27. Ces textes longs et verbeux sont alors souvent source de

[1] Le vocable a lui-même évolué dans le temps. Le droit de l'informatique puis, avec la libéralisation des télécommunications, le droit de l'informatique et des télécoms, avant de devenir le droit des nouvelles technologies de l'information et des communications (NTIC) puis le droit des technologies de l'information et des communications (TIC).

[2] La première norme juridique communautaire est la Directive n°91/250/CEE du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur qui avait été précédée de Lois nationales. On trouve cependant encore quelques rares textes de Lois votés par le Parlement français comme la Loi n°2016-1321 du 7 octobre 2016 pour une République numérique votée sous la présidence de François Hollande.

débats et donc d'insécurité juridique. Il est loin le temps de la rédaction précise et concise à la française qui constituait un cadre clair pour tout citoyen, laissant ensuite aux juges le soin d'en préciser ses contours au moyen de la casuistique. En troisième lieu, les observateurs attentifs constatent une dérive lente et continue du droit communautaire vers des concepts juridiques anglo-saxons[3]. Enfin, on ne peut manquer d'observer l'invisibilité du juge judiciaire.

Pour illustrer notre dernier propos, nous proposons l'étude et l'analyse de deux textes communautaires récents et très populaires, pour ensuite déceler les causes et conséquences de ce mouvement.

Le constat, par l'analyse de deux grands textes communautaires, le RGPD et l'IA Act

Le RGPD est le texte star de la Commission européenne. Il est entré en application dans les 27 États membres le 25 mai 2018. Le Règlement sur l'intelligence artificielle dit IA Act[4] date quant à lui du 13 juin 2024. Il devrait entrer en application progressivement sur 36 mois[5].

Le RGPD ou le triomphe de la Cnil et des autorités administratives indépendantes (AAI)

Le RGPD est consacré tout entier à la défense des droits des personnes physiques et d'un des attributs de leur personnalité, à savoir les informations susceptibles de les identifier directement ou indirectement. Le niveau de sanction prévu par le texte en cas de non-conformité a fait son succès. Ces sanctions peuvent s'élever jusqu'à 4 % du chiffre d'affaires mondial total du contrevenant et 20 millions d'euros d'amende[6]. Le prononcé des sanctions de même que les opérations de contrôle qui les précèderont immanquablement, sont confiées à une autorité de contrôle, en France, la Commission nationale de l'Informatique et des Libertés (Cnil).

Créée par la Loi dite « informatique et libertés » de 1978[7], la Cnil est la première autorité administrative indépendante (AAI) créée dans notre droit contemporain. Elle a fait depuis des émules, puisque le droit français accueille désormais près de 50 AAI[8], les plus connues aujourd'hui étant l'Arcom et l'Autorité de la Concurrence. La Cnil est le « gendarme » des données personnelles, avec des moyens juridiques considérablement renforcés. Elle dispose d'un droit d'accès aux données au sein des organismes contrôlés quasi équivalent à un droit de perquisition, d'un droit d'auditionner toutes personnes en ses locaux, d'un

[3] ITEANU Olivier, *Quand le digital défie l'État de droit*, Paris : Eyrolles, 2017, 188 pages.

[4] Règlement UE 2024/1689 du 13 juin 2024 du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle dit règlement sur l'intelligence artificielle.

[5] ITEANU Alexandra, « Intelligence artificielle : zoom sur l'IA Act bientôt adopté », *Solutions Numériques*, 24 janvier 2024.

[6] Article 83 5) du RGPD.

[7] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[8] Rapport du Sénat n°126 (2015-2016), déposé le 28 octobre 2015, « Un État dans l'État : canaliser la prolifération des autorités administratives indépendantes pour mieux les contrôler ».

pouvoir d'injonction, de limitation voire même d'interdiction des traitements[9]. La Cnil fonctionne et se considère aussi comme un juge, même si organiquement, elle ne l'est pas[10]. Étant autorité administrative, sa chambre de recours est le Conseil d'État. Une nombreuse jurisprudence rappelle régulièrement que les AAI sont soumises aux grands principes directeurs des procès, tels que le respect des droits de la défense, le principe du contradictoire, et l'impartialité notamment.

Ainsi, dans le RGPD, on ne trouve aucune trace d'un juge judiciaire ou du système qui l'accompagne. Le pouvoir de contrôle et de sanction est tout entier dévolu aux autorités de contrôle et de sanction. Le droit français, depuis l'origine de cette réglementation spéciale en 1978, comporte pourtant un volet pénal qui vient sanctionner les contrevenants à la Loi à des peines d'amende et de prison. On le trouve aux articles 226-16 à 226-24 du Code pénal. Dans le souci d'éviter les risques de contradiction entre le volet pénal et les décisions de la Cnil, le législateur français a dû voter une Loi accompagnant le RGPD dans ses effets[11], qui prévoit que lorsqu'une « … sanction pécuniaire [par la Cnil] devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce. ».

Cependant, depuis 47 ans, ce sont au plus quelques dizaines de procès pénaux seulement qui ont pris place. Les plaintes déposées au Parquet ne sont d'ailleurs pas souvent suivies d'enquêtes, et les praticiens ont dès lors très peu recours au volet judiciaire. Le juge judiciaire est donc invisibilisé dans le RGPD, mais il reste accessible, même si cette place est résiduelle.

Le règlement IA Act ou le sacre de la gouvernance

L'intelligence artificielle, dite « IA » en français, est au-devant de l'actualité. Il faut dire qu'elle amène avec elle un certain nombre de fantasmes mais aussi de rêves de jours meilleurs. L'IA Act définit l'IA comme « un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement [pour] … à partir des entrées qu'il reçoit (…) générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels. »[12].

L'ambition du texte est de favoriser l'innovation dans un cadre éthique et de protéger les droits fondamentaux face aux risques liés à certaines utilisations. Ainsi, l'IA Act classe les systèmes en fonction de leur niveau de risque. Certaines IA sont interdites car causant des risques qualifiés d'inacceptables, d'autres, dites à haut risque sont réglementées, celles à risque limité sont soumises à de simples obligations de transparence et d'information ; enfin, celles dits à risque minimal sont hors règlement.

La question qui nous paraît majeure est celle du régime de responsabilité appliqué à l'IA. L'IA peut tromper intentionnellement ou commettre des erreurs qui causent préjudice, et bousculer les droits de tiers en propriété intellectuelle ou en matière de protection de la

[9] Article 58 du RGPD.

[10] Conseil Constitutionnel Décision n°2009-580 DC du 10 juin 2009 sur la Loi favorisant la diffusion et la protection de la création sur Internet, sur l'Hadopi (téléchargement illégal), une autre AAI absorbée depuis par l'Arcom.

[11] Article 7 de la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles.

[12] Article 3 1).

vie privée. Or, le Règlement européen ne traite pas de la responsabilité[13]. Une proposition de Directive relative à l'adaptation des règles en matière de responsabilité civile extra-contractuelle était bien prévue aux côtés de l'IA Act mais elle a été étonnamment retirée du programme de travail de la Commission européenne[14]. Quelques jours plus tôt, lors du sommet sur l'IA organisé à Paris, le vice-président américain James David Vance avait dit tout le mal qu'il pensait d'une réglementation européenne[15]. Du fait de cette absence de texte spécial, la question des responsabilités reviendra dès lors naturellement au juge judiciaire appliquant le droit de la responsabilité civile de droit commun.

S'agissant des manquements à l'IA Act, c'est-à-dire essentiellement au classement des systèmes en fonction des risques, des sanctions sont bien prévues jusqu'à 35 millions d'euros d'amende ou 7 % du chiffre d'affaires mondial total. Mais le système de contrôle et sanction élaboré par l'IA Act confirme notre perception. Ce système est appelé « gouvernance » par le Règlement quand le droit français connaît la réglementation et la régulation[16]. L'IA Act est en effet un festival d'organes en tous genres chargés de cette gouvernance. Un bureau de l'IA est créé auprès de la Commission flanqué de divers groupes d'experts et de travail. Un Comité européen de l'IA est créé, qui supervise l'application du Règlement, et chaque État doit désigner des autorités nationales de supervision et de sanction.

En France, on murmure que la Cnil et la DGCCRF seraient pressentis, mais le texte ménage une certaine souplesse, prévoyant à son article 99, point 9, que les amendes administratives pourront être « … appliquées de manière à ce que les amendes soient imposées par les juridictions nationales compétentes ou par d'autres organismes, selon ce qui est applicable dans ces États membres… ».

Enfin, la Commission européenne se réserve certaines sanctions, par exemple à l'encontre des fournisseurs d'IA dits à usage général contrevenant à l'IA Act, soit jusqu'à 15 millions d'euros ou 3 % du chiffre d'affaires annuel mondial total.

Causes et conséquences ?

Comment peut-on dès lors expliquer ce mouvement que nous décrivons et en évaluer les conséquences. Pour cela, nous allons recenser les principaux motifs qui ont poussé les institutions communautaires et les États à emprunter cette voie.

Une réponse au temps du numérique et à sa complexité

C'est la critique la plus directe adressée au service public de la justice. Le temps judiciaire n'est pas le temps du numérique. Le premier est un temps long, parfois très long, quand le numérique exige une réponse souvent rapide. De surcroît, le système judiciaire est occupé essentiellement par le juge seul, pouvant éventuellement s'entourer d'avis techniques

[13] Sauf par allusions, par exemple à l'article 60 9 du Règlement sur les essais de systèmes d'IA à haut risques en dehors de milieux fermés, dits bacs à sable, qui « Le fournisseur ou le fournisseur potentiel sont responsables, en vertu du droit de l'Union et du droit national de tout préjudice causé... ».

[14] ITEANU A., Avis de recherche : où est passée la Directive sur la responsabilité de l'IA, Solutions Numériques, 18 février 2025.

[15] Wulff Wold J. & Bourgery-Gonse Théo, JD Vance veut démanteler les réglementations européennes en matière d'IA, EURACTIV.FR, consultable sur https://www.euractiv.fr/section/intelligence-artificielle/news/jd-vance-veut-demanteler-les-reglementations-europeennes-en-matiere-dia/

[16] Marie-Anne FRISON-ROCHE (ouvrage collectif sous la direction de), Internet, espace d'interégulation, Paris, Dalloz, 2016.

mais non décisionnaires. Les différentes autorités conçues par l'UE et impliquées dans ce domaine en constante évolution sont capables de fédérer des compétences techniques, économiques et juridiques dans leurs formations de contrôle et de sanction. C'est une supériorité certaine de ces dernières à la condition que le droit, norme démocratique, soit bien supérieur à la technique tout en composant avec lui dans un subtil souci d'équilibre. De ce point de vue, les chambres de recours de ces différentes autorités doivent impérativement rester des juridictions de l'ordre administratif ou judiciaire[17], pour que la force reste au droit. Il s'ajoute que les premières décisions de ces autorités pourront exposer le cas traité en experts et décrire l'environnement technique éventuellement économique en question, faisant ainsi œuvre pédagogique pour les juges d'appel qui pourront s'appuyer sur cette expertise pour se concentrer sur le droit.

L'exigence de l'indépendance

La Cnil a été créée dans le but d'être le gendarme des données personnelles pour tous, y compris la sphère publique et en premier lieu l'État. De ce fait, cette autorité devait être indépendante à l'égard de l'État lui-même, ce qui est le cas au regard des règles de désignation de ses membres, de l'impossibilité de révoquer leurs mandats avant terme, et des décisions qu'elle prend sans en référer à aucune tutelle.

Cependant, les autorités en charge du numérique sont constituées d'un petit nombre de personnes. Celles-ci étant facilement identifiées sont la cible des lobbyistes qui ne manquent pas à Bruxelles et plus généralement dans le numérique au regard des enjeux. À cela s'ajoute le fait que les AAI ou les Commissions administratives ont souvent une activité réglementaire ou doctrinale qui les fait rencontrer dans un cadre amical, toutes sortes de représentants des acteurs du numérique. Ce mélange des genres est toujours à risque sur le terrain du conflit d'intérêts.

À l'inverse, les juges judiciaires et administratifs sont de l'ordre de 8 000 en France, ce qui rend le travail d'influence difficile. La décision de sanction peut venir de partout sur le territoire et de tout juge à tout niveau. Le monde des affaires anglo-saxon est d'ailleurs terrifié par le juge français et sa loi locale, de sorte qu'il refuse souvent sa désignation pour interpréter ou gérer les litiges nés de l'exécution des contrats qu'il conclut.

Un enjeu de pouvoirs ?

Enfin, nous considérons que la situation que nous décrivons est la conséquence de l'état de développement inabouti de l'Union européenne. À ce jour, l'institution européenne produit de la norme juridique sans jamais l'appliquer elle-même. Par la création de ces diverses autorités auxquelles s'ajoutent souvent des groupes d'experts, de travail ou de coordination plus ou moins formalisés, qui réunissent des représentants des 27 États membres[18], la Commission européenne vient ainsi pallier l'organisation actuelle de l'Union européenne. Elle participe à sa façon à contrôler l'application des textes communautaires qu'elle promeut et joue de son influence pour que la lettre et l'esprit de ces textes soient respectés. Ceci est particulièrement vrai dans le numérique peuplé d'oligopoles essentiellement américains avec notamment, mais pas seulement, les fameux Gafam[19]. Il faut dire

[17] C'est le cas de l'AAI qu'est l'Autorité de la Concurrence avec la cour d'appel de Paris quand de nombreuses autres AAI répondent de leurs décisions devant le Conseil d'État.

[18] En matière de données à caractère personnel, c'est le Comité européen pour la Protection des Données dit CEPD, qui regroupe les « Cnil » des 27 États membres.

[19] Au-delà de Google Amazon Facebook Apple et Microsoft (GAFAM), on pourrait aussi y ajouter Oracle, Salesforce, et bien d'autres encore, ainsi que l'émergence des acteurs chinois (Baidu, Alibaba, Tencent, Xiaomi, TikTok…).

enfin que face aux États-Unis et à la Chine, le bon niveau de riposte des Européens est l'Union, et non l'échelon national.

Conclusion

Au-delà des deux constats que nous avons opérés au travers du RGPD et de l'IA Act, nous aurions pu évoquer d'autres réglementations promues par l'Union européenne. Prochainement, un paquet cybersécurité autour de la Directive NIS2 s'annonce[20], bâti sur une structure réglementaire proche du RGPD. Cette répétition nous fait penser que ce qui émerge est un nouveau système. Ce système se dessine devant nous sans crier gare, mais il modifie en profondeur notre État de droit appliqué au secteur du numérique.

Deux ordres d'autorités se partagent désormais sa régulation. Le premier est le système judiciaire tel que nous le connaissons depuis la Révolution française. Le second fait essentiellement appel à des autorités administratives et se réclamerait plutôt de la gouvernance. Ce second système a des vertus et une utilité certaine : sa multidisciplinarité nécessaire, une ouverture vers la société et ses usages, et enfin son efficacité. Ceci explique pourquoi le juge judiciaire est invisibilisé par les grands textes communautaires du droit du numérique.

Mais ce juge n'est pas effacé. Il est bien présent, et cette présence est une nécessité, car il est le garant de notre État de droit. Ces juges judiciaires sont non seulement formés au droit, mais aussi aux procédures contentieuses, ce qui ne s'improvise pas. Ils apportent ainsi aux citoyens de réelles garanties. Non seulement le juge judiciaire n'est pas effacé, mais surtout, il ne doit pas l'être et doit se voir réserver une place dans ce double système. Ce devrait être un souci constant de tous les législateurs européens désormais.

Bibliographie

FERAL-SCHUHL C. (2024), *Cyberdroit – Le droit à l'épreuve de l'internet* (8e édition), Paris, Dalloz.

FRISON-ROCHE MA. (ouvrage collectif sous la direction de) (2016), *Internet, espace d'interégulation*, Paris, Dalloz.

GAUDRAT P. & SARDAIN F. (2015), *Traité de droit civil du numérique*, Bruxelles, Larcier.

ITEANU O. (1996), *Internet et le Droit – Aspects juridiques du commerce électronique*, Paris, Eyrolles.

ITEANU O. & VORMES M. (1998), *Le nouveau marché des télécoms – Conseils juridiques pratiques pour l'entreprise*, Paris, Eyrolles.

ITEANU O. (2004), *Tous cybercriminels : la fin d'internet ?*, Paris, Jacques-Marie Laffont

ITEANU O. (2008), *L'identité numérique en question – 10 scénarios pour une bonne gestion juridique de son identité sur internet*, Paris, Eyrolles.

ITEANU O. (2016), *Quand le digital défie l'État de droit*, Paris, Eyrolles.

[20] Directive (UE) 2022/255 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. Le même jour, une autre directive a été prise sur la résilience des entités critiques (dite directive « REC ») et un Règlement sur la résilience opérationnelle numérique du secteur financier (DORA).

MATTATIA F. (2013), *Loi et internet – Un petit guide civique et juridique*, Paris, Eyrolles.

MATTATIA F. (2021), *RGPD et droit des données personnelles* (5e édition), Paris, Eyrolles.

MATTATIA F. (2023), *Internet et les réseaux sociaux : que dit la loi ?* (5e édition), Paris, Eyrolles.

VIVANT M., WARUSFEL B., MALLET-POUJOL N. & MADI C. (2025), *Le Lamy droit du numérique* (Édition 2025), Saint Ouen, Lamy Liaisons.

La place de la normalisation dans la politique européenne du numérique

Par Louis MORILHAT
Service de l'Économie numérique
de la direction générale des Entreprises

Alors que les normes et standards techniques dans le domaine des télécommunications et du numérique s'autonomisent progressivement du seul registre technique pour investir des sujets de gouvernance, d'éthique et de souveraineté, les instances de normalisation apparaissent comme des espaces de configuration des rapports de forces technologiques entre les acteurs.

Par une réaffirmation de la normalisation comme instrument de compétitivité technologique et son intégration comme outil d'autonomie stratégique ouverte, l'Union européenne s'empare fortement de ce levier pour façonner son cadre réglementaire grâce à une architecture inédite de gouvernance fondée sur une hybridation entre législation et spécifications techniques.

L'objectif de cet article est d'analyser les enjeux spécifiques au domaine du numérique dans la normalisation, l'intégration de ce champ dans la politique européenne sur le numérique et la transformation progressive des normes et standards en outils d'influence technologique.

Longtemps reléguée à la périphérie des grands instruments de politique publique, la normalisation technique s'impose progressivement comme un espace de reconfiguration des rapports de force industriels et technologiques : soit parce qu'ils n'ont pas été arbitrés au niveau politique et réglementaire, soit parce qu'ils émergent directement des innovations techniques. Ce changement de paradigme est particulièrement perceptible dans le domaine des télécommunications et du numérique, où les normes et standards techniques[1] ne se contentent plus de faciliter la compatibilité entre les dispositifs, mais structurent les modalités de gouvernance et d'interopérabilité des différentes couches techniques d'un système d'information. Dans ce contexte, la capacité d'un acteur à définir, imposer ou diffuser ses standards devient une forme de puissance, une faculté à façonner le marché selon ses préférences commerciales, industrielles et technopolitiques.

À l'échelle européenne, cette évolution s'inscrit dans un double mouvement : d'une part, la réaffirmation de la normalisation comme instrument de compétitivité technologique, et d'autre part, son intégration progressive au sein d'un projet d'autonomie stratégique ouverte, fondé sur la maîtrise des infrastructures critiques et des standards régulateurs. Dans une compétition largement disputée au niveau mondial, à l'ISO-IEC et à l'UIT,

[1] On parle de « normes », pour désigner les documents techniques rédigés par les organismes de normalisation officiels (tels que ISO-IEC au niveau international, CEN-Cenelec au niveau européen et l'Afnor au niveau français). Les « standards » désignent tout autre référentiel, notamment ceux rédigés par des consortiums tels que l'ETSI ou l'IEEE. Dans le langage courant – ou en anglais – les deux termes se confondent.

l'Union européenne bénéficie d'un échelon régional unique grâce à son système européen de normalisation, constitué de l'ETSI – initialement spécialisé dans les sujets de télécommunications – et du CEN-Cenelec – les deux organismes de normalisation historiques représentant la filière générale d'une part et la filière électro-technologique d'autre part, travaillant conjointement sur les sujets numériques.

L'objectif de cet article est d'analyser les enjeux spécifiques au domaine du numérique dans la normalisation, et de montrer comment celle-ci s'autonomise progressivement du seul registre technique pour investir des sujets de gouvernance, d'éthique et de souveraineté.

Le « droit souple » de la technique

L'inclusivité comme vecteur de compétitivité

À rebours des modalités d'élaboration de textes réglementaires, les processus de normalisation et de standardisation offrent des caractéristiques particulièrement structurantes pour les sujets numériques.

En premier lieu, ces référentiels sont élaborés selon des mécanismes de concertation multipartite, associant industriels, chercheurs, société civile et pouvoirs publics. Ce fonctionnement ascendant et collaboratif, bien qu'imparfait, garantit l'ancrage industriel et la flexibilité des futures exigences techniques, rédigées par ceux qui les adopteront.

Aussi, dans un environnement technologique évolutif marqué par des cycles d'innovation rapides, les normes et standards assurent une certaine adaptabilité des exigences techniques. Néanmoins, l'accélération technologique observée – notamment en matière d'Intelligence artificielle ou de technologies immersives – provoque une pression croissante sur les comités techniques : les travaux de normalisation se retrouvent tiraillés entre la nécessité de se maintenir à l'état de l'art pour éviter une obsolescence rapide des référentiels et l'enjeu de préserver les exigences à un niveau de maturité suffisant pour faciliter leur adoption dans l'industrie.

Enfin, en permettant d'orienter les trajectoires d'innovation, de fixer les cadres d'interopérabilité et d'anticiper les exigences réglementaires futures, les normes et standards facilitent l'encadrement de la concurrence selon des critères de confiance, tout en nourrissant une dynamique de compétitivité pour les entreprises.

La spécificité numérique

Plusieurs propriétés fondamentales affectent la manière dont s'élaborent et se diffusent les normes et standards techniques dans le domaine des technologies de télécommunications et du numérique : l'interopérabilité systémique, les externalités de réseau aboutissant à des logiques oligopolistiques, et les enjeux de concurrence liés à l'intégration des brevets dans les standards.

Alors que les enjeux de sécurité, de qualité ou de fiabilité représentent habituellement les exigences techniques prioritaires dans la normalisation d'un produit : la notion d'interopérabilité s'impose comme une clé de voûte pour les technologies numériques. Dans les écosystèmes numériques, les systèmes complexes centrés sur les usages et les systèmes d'information reposent sur l'interaction constante entre des couches hétérogènes – des infrastructures aux logiciels en passant par les équipements et les interfaces. Dans ce cadre, les standards ne sont plus de simples normes facilitant la conformité, mais des dispositifs d'orchestration technique, garantissant la circulation des données, la portabilité des services et la compatibilité entre couches logicielles.

Les externalités de réseau jouent également un rôle structurant : la valeur technologique (ou financière) d'une technologie croissant avec le nombre d'utilisateurs l'ayant adoptée, cette dynamique favorise l'émergence de standards dominants fondés sur des effets de

masse, parfois indépendamment de leur supériorité technique (Katz et Shapiro, 1985). Ces standards *de facto*, imposés par les grands acteurs industriels, concurrencent directement les processus classiques de standardisation basés sur le consensus multipartite (standard de *jure*). Cette logique du "winner-takes-all" caractéristique des marchés numériques, dans laquelle le premier acteur à imposer son standard peut bénéficier d'un verrouillage de marché durable (Besen et Farrell, 1994) confère une dimension particulièrement stratégique à la normalisation, qui permet ainsi de casser des monopoles et d'ouvrir le marché.

Enfin, l'intégration de brevets dans les standards de télécommunications soulève des enjeux juridiques et concurrentiels majeurs. Les « brevets essentiels aux normes » (BEN) sont rendus indispensables à la mise en œuvre technique d'un standard (par exemple pour les technologies 4G, 5G, ou *wifi*). Afin de prévenir tout abus de position dominante d'acteurs possédant des technologies propriétaires, d'encourager leur partage de connaissances dans des travaux de normalisation et de favoriser l'applicabilité technique d'un standard, des organismes comme l'ETSI permettent aux détenteurs de ces BEN de les concéder sous des licences dites FRAND (Fair, Reasonable and Non-Discriminatory).

Toutefois, les pratiques de *licensing* agressif, les injonctions judiciaires ou la rétention stratégique d'informations sur les brevets peuvent perturber l'accès équitable aux standards et fausser la concurrence (Contreras, 2013). Dans le domaine de la 5G par exemple, des litiges opposant des acteurs majeurs comme Qualcomm, Huawei ou Ericsson ont mis en lumière la tension entre incitation à l'innovation et verrouillage technologique des marchés (Galetovic, Haber et Zaretzki, 2015).

Des normes techniques aux normes éthiques

En prolongement des normes et standards portés sur la sécurité, la qualité et l'interopérabilité, le champ de la normalisation du numérique s'élargit progressivement pour répondre à des risques systémiques liés à l'usage des technologies. Ces nouvelles considérations apparaissent particulièrement visibles sur le sujet de l'Intelligence artificielle, pour lequel les risques portent autant sur le produit lui-même que sur les effets de ses usages. Cette configuration conduit ainsi à une volonté d'encadrer le déploiement de ces nouvelles technologies en introduisant des principes de transparence, de justice, de responsabilité et de non-discrimination (Jobin, Ienca et Vayena, 2019).

Deux types de normes éthiques peuvent être distingués (Gornet et Maxwell, 2023) : les normes de gouvernance traitant des mécanismes nécessaires à une entreprise pour intégrer une technologie dans un contexte social et assurer un respect des principes éthiques (gestion des risques et de la qualité, processus d'intégration, gestion du cycle de vie). Les normes de mesure, quant à elles, visent à répondre à des exigences éthiques par des critères techniques (définition technique de la transparence, de l'équité, de la fiabilité).

Ce type de normes, souvent aligné derrière des objectifs réglementaires (en soutien à des législations européennes) ou politiques (en déclinaison des objectifs de développement durable onusiens par exemple), est toutefois contesté. Sur un volet technique d'une part, au regard de la complexité de définir, mesurer et évaluer des aspects éthiques au sein d'une technologie ; et, sur un volet idéologique d'autre part, certaines parties prenantes considérant que les normes et standards doivent se borner à des considérations purement techniques.

Néanmoins, que les considérations éthiques soient explicitement prises en compte ou non, les normes et standards sur les technologies numériques ne sont pas neutres : en encapsulant des méthodes techniques, ils déploient des paradigmes technologiques, donc des visions technopolitiques.

Intégration des normes dans la politique européenne sur le numérique

La nouvelle approche européenne : de l'harmonisation à l'outil d'influence

Afin d'harmoniser les spécifications industrielles à travers l'Europe pour construire le marché unique naissant, l'Union européenne adopte en 1985 la Nouvelle approche[2], introduisant une architecture inédite de gouvernance fondée sur une hybridation entre législation et spécifications techniques. Mise à jour et développée dans le "New Legislative Framework[3]" publié en 2008, cette approche repose sur un dispositif en deux étapes :

- la définition, par les institutions européennes, d'exigences obligatoires à travers une législation, réglementation ou politique publique (par exemple la sécurité et la protection des droits fondamentaux) ;
- la déclinaison technique de ces exigences par les organismes de normalisation européens (CEN, Cenelec, ETSI), chargés d'élaborer des normes harmonisées en réponse à une « demande de normalisation » de la Commission européenne.

Ces normes, bien que volontaires dans leur application, sont citées au *Journal officiel de l'Union européenne* et représentent la méthodologie préférentielle pour répondre aux exigences fixées par la loi : la conformité d'un produit ou d'un service à une norme harmonisée confère une présomption de conformité à la réglementation correspondante.

Initialement pensée comme un dispositif technico-réglementaire communautaire, cette approche s'est progressivement muée en un vecteur d'influence externe, dans une forme singulière de *soft power* normatif (M. Egan, 2001 ; J. Pelkmans, 2001). Du fait de sa taille, de son attractivité et de son intégration dans les flux internationaux, le marché européen agit comme un levier normatif incitant les acteurs extérieurs à adapter leurs pratiques à son cadre technique pour pouvoir l'intégrer, jusqu'à entraîner, par répercussion, l'adoption extraterritoriale de standards techniques européens[4] : c'est le "Brussels Effect" (A. Bradford, 2020).

Conçue à l'origine pour les biens industriels – où la conformité aux normes harmonisées européennes devient une condition d'accès aux chaînes de valeur mondiales et à la circulation des produits – cette nouvelle approche s'est progressivement étendue au domaine du numérique, constituant un élément incontournable de son cadre politique européen.

La déclinaison technique des politiques européennes du numérique

Les domaines des radiocommunications et des télécommunications utilisent depuis des années déjà les normes harmonisées pour répondre à l'enjeu de cohérence réglementaire et technique au sein du marché unique.

C'est en particulier à l'ETSI que sont développées les normes portant sur les caractéristiques de compatibilité, d'interconnexion de sécurité et de qualité des transmissions des

[2] La nouvelle approche – France Normalisation, https://www.francenormalisation.fr/les-acteurs-de-la-normalisation/la-nouvelle-approche/#:~:text=La%20r%C3%A9glementation%20de%20type%20Nouvelle,mis%20sur%20le%20march%C3%A9%20europ%C3%A9en

[3] New legislative framework – European Commission, https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

[4] La directive RoHS (2002) sur la restriction des substances dangereuses dans les équipements électroniques a imposé des normes de fabrication reprises à l'échelle mondiale.

technologies de télécommunication. Dans le cadre de la directive RED, les normes harmonisées développées à l'ETSI soutiennent l'évaluation de la conformité des équipements radio en ce qui concerne l'utilisation efficace du spectre et la compatibilité électromagnétique[5]. S'agissant des réseaux de communications mobiles, le travail de normalisation s'appuie sur une articulation singulière avec le 3GPP[6], partenariat international chargé de développer des spécifications techniques communes pour les réseaux de communications mobiles (initialement la 3G, puis la 4G, la 5G et désormais la 6G). Ainsi, si le 3GPP constitue le forum d'élaboration technique des standards mobiles à l'échelle mondiale, l'ETSI assure un rôle de transcription, d'adaptation normative et de légitimation réglementaire dans le cadre européen.

Pour les technologies numériques, alors que la dernière mandature de l'Union européenne a été marquée par la mise en place d'un cadre réglementaire ambitieux, un certain nombre de ces réglementations prévoient de s'appuyer sur des normes harmonisées pour en assurer l'implémentation.

En particulier, le Règlement sur l'Intelligence Artificielle[7] requiert la conduite d'évaluation de conformité *ex ante*, pour les systèmes à haut risque, dont les exigences seront adossées aux normes harmonisées actuellement développées par le CEN-Cenelec[8,9]. Dans une approche « produit », les normes en cours d'élaboration portent autant sur les exigences d'intégration d'un système d'IA dans une organisation (système de gestion de la qualité, gestion des risques) que sur la définition, les métriques et les contre-mesures d'une exigence de confiance (transparence, fiabilité, robustesse et qualité des jeux de données…).

Également, s'agissant du Règlement sur la Cyber résilience (CRA)[10], la demande de normalisation[11] envoyée au CEN-Cenelec et à l'ETSI requiert un corpus impressionnant d'exigences portant sur la cybersécurité relative aux produits comportant des éléments numériques, et au traitement des leurs vulnérabilités. Enfin, pour le Règlement sur les données (Data Act)[12], la Commission européenne rédige actuellement une demande de normalisation visant à détailler les exigences nécessaires à l'interopérabilité des données et les modalités de leur partage entre différents espaces de données.

Ces nombreux travaux de normalisation menés en parallèle soulèvent ainsi plusieurs enjeux : l'identification d'un bon niveau de profondeur entre exigences génériques et

[5] Par exemple, la norme EN 300 328 traite du bon usage du spectre radioélectrique et détaille les exigences nécessaires pour la mise sur le marché des équipements fixes et mobiles dédiés à la transmission de données dans la bande 2,4 GHz (par exemple *wi-fi*, *bluetooth*).

[6] Créé en 1998, le 3GPP (Third Generation Partnership Project) regroupe sept organismes de standardisation régionaux appelés Organizational Partners, parmi lesquels figure l'ETSI, représentant les intérêts européens. À ce titre, l'ETSI assure le lien institutionnel entre le 3GPP et l'Union européenne.

[7] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401689

[8] L'ETSI n'a pas été intégré à la demande de normalisation portant sur l'Intelligence artificielle.

[9] Register of Commission Documents - C(2023)3215, https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en

[10] Regulation - 2024/2847 – EN - EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

[11] Registre de documents de la Commission - C(2025)618, https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=fr

[12] Regulation - EU - 2023/2854 - EN - EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1704709568425

sectorielles d'une part, afin de disposer de référentiels applicables aux différents usages et aux différentes industries, pour des technologies par nature transverses. D'autre part, l'articulation entre ces différents corpus normatifs pose un défi de coordination et d'harmonisation important entre les différents comités techniques qui les rédigent. Ce qui se joue ici constitue non seulement la cohérence du cadre technique européen sur le numérique, mais également, par effet de projection, la définition proactive des normes mondiales dans des domaines considérés comme stratégiques.

Enjeux de gouvernance et soutien des acteurs publics

La Commission européenne, en affirmant dans sa stratégie européenne de normalisation[13] publiée en 2022 que cette dernière est un « enjeu de souveraineté technologique », explicite ainsi un tournant stratégique : la normalisation devient un prolongement de la souveraineté régulatoire, un outil de projection de ses valeurs – transparence, sécurité, protection des données – dans la définition technique des technologies numériques au niveau mondial. Pour cela, elle s'inscrit pleinement dans l'ambition d'autonomie stratégique ouverte de l'Union européenne[14].

De ce fait, les enjeux de gouvernance des organismes européens de normalisation et l'alignement des travaux avec les politiques industrielles des États membres s'en trouvent rehaussés.

En matière de gouvernance, le modèle multilatéral non-gouvernemental du CEN-Cenelec et de l'ISO-IEC, pour lesquels les entreprises participent aux travaux par l'intermédiaire de leur organisme national (AFNOR pour la France, DIN pour l'Allemagne, SAC pour la Chine, etc.), diffère du modèle multipartite caractéristique de l'ETSI, pour lequel chaque acteur participe en son nom propre. Alors que le premier modèle se traduit théoriquement par une assurance de représentativité et de traçabilité, les inégalités de ressources, d'expertise et de capacité d'influence entre les différents pays sont sources de déséquilibres. Concernant l'ETSI, les asymétries d'influence et de représentativité inhérentes à un modèle multipartite ont suscité une réforme de la gouvernance de l'organisation à partir de 2022, fortement impulsée par les États membres, pour renforcer le poids de ces derniers dans les processus de décision aux dépens des entreprises multinationales, pour la plupart extra-européennes.

Outre la définition des activités de normalisation – par la rédaction des textes réglementaires organisant le système français[15] et européen[16] – l'action publique, portée par la direction générale des Entreprises, consiste également dans la participation active aux instances de dialogue et de gouvernance européennes chargées de la déclinaison du cadre réglementaire (les projets de demandes de normalisation sont soumises au vote des États membres) et de définir les orientations stratégiques de l'Union (*High Level Forum, Plateforme multipartite sur la normalisation du numérique).* L'action de la DGE porte également sur la mobilisation des filières, l'alignement entre les politiques publiques

[13] https://ec.europa.eu/docsroom/documents/48598

[14] Ambition et leviers pour une autonomie stratégique de l'Union européenne dans le domaineéconomique, https://www.lecese.fr/sites/default/files/pdf/Avis/2022/2022_13_autonomie_strategique_UE.pdf

[15] Décret n°2009-697 du 16 juin 2009 relatif à la normalisation – Légifrance, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020749979

[16] Règlement - 1025/2012 - EN - EUR-Lex, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32012R1025

et les travaux normatifs mais également sur l'intégration de la normalisation dans les stratégies nationales pour les technologies numériques. Ainsi, la mise en place d'une stratégie de normalisation sur l'Intelligence Artificielle (Grand Défi IA, 2020-2025) et sur les technologies quantiques (MetriQs-France, 2022-2027), témoigne de la prise en compte du levier normatif dans les stratégies industrielles de l'État.

Bibliographie

KATZ M. L. & SHAPIRO C. (1985), "Network externalities, competition, and compatibility", *The American Economic Review*, 75(3), pp. 424-440.

BESEN S. M. & FARRELL J. (1994), "Choosing how to compete: Strategies and Tactics in standardization", *The Journal of Economic Perspectives*, 8(2), pp. 117-131.

CONTRERAS J. L. (2013), "Patent pledges", *Arizona State Law Journal*, 47(3), pp. 543-608.

GALETOVIC A., HABER S. & ZARETZKI L. (2015), "An empirical examination of patent holdup", *Journal of Competition Law and Economics*, 11(3), pp. 549-578.

JOBIN A., IENCA M. & VAYENA E. (2019), "The global landscape of AI ethics guidelines", *Nature Machine Intelligence*, 1(9), pp. 389-399.

GORNET M. & MAXWELL W. (2023), « Normes techniques et éthique de l'IA », CNIA 2023 - Conférence nationale en Intelligence artificielle, Juillet 2023, Strasbourg, France.

EGAN M. (2001), "Constructing a European market: The EU and the politics of regulatory convergence", *Journal of European Public Policy*, 8(3), pp. 293-315.

PELKMANS J. (2001), *European integration: Methods and economic analysis*, Longman.

BRADFORD A. (2020), *The Brussels effect: How the European Union rules the world*, Oxford University Press.

COMMISSION EUROPÉENNE (2017), "Setting out the EU approach to standard essential patents", Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, COM(2017) 712 final.

L'action des opérateurs

Par Dominique WURGES
Orange

Après avoir rappelé des considérations générales sur l'intérêt de la normalisation pour les opérateurs de télécommunications, l'auteur détaille dans cet article les éléments spécifiques de ce secteur et décrit les grands principes guidant l'action des opérateurs dans leurs activités de normalisation et les moyens qu'ils y allouent.

Cet article présente notamment le domaine d'activités de plus en plus large des instances du secteur des TIC dédiées à la normalisation, leurs spécificités, et expose les principaux enjeux de la participation dans ces activités pour un opérateur majeur. Il est complété par l'analyse de deux exemples concrets. Enfin, l'article élargit le propos à des considérations connexes à la normalisation et pose la question de son futur face à la montée de l'*open source*.

Considérations générales : de l'intérêt des activités de normalisation pour les opérateurs

L'intérêt des opérateurs de télécommunications pour la normalisation s'est manifesté très tôt, quasiment dès le développement des réseaux téléphoniques, pour lesquels il a fallu fixer des règles, normes et standards afin de permettre les interconnexions et communications télégraphiques, téléphoniques ou électroniques et assurer un développement coordonné. L'action des opérateurs est également caractérisée par la nécessité de prendre en compte la dimension internationale, ne limitant de fait pas la normalisation au seul cadre national. Le secteur des télécommunications fut ainsi le premier à être doté d'une organisation intergouvernementale technique de coordination, l'Union Internationale du Télégraphe, d'ailleurs créée à Paris en 1865, et qui deviendra par la suite l'Union Internationale des Télécommunications (UIT), dont le rôle a été reconnu par son rattachement aux Nations Unies après la Seconde Guerre mondiale. Dès 1924, cette organisation avait ainsi créé une branche spécialisée dédiée à la normalisation, le Comité Consultatif International Téléphonique (CCIT), devenu par la suite l'UIT-T, ou secteur de la normalisation de l'UIT. L'UIT-T joue aujourd'hui un rôle déterminant dans le secteur des télécommunications, en demeurant le seul organisme véritablement mondial de normalisation des technologies de l'information et de la communication (TIC).

L'Intérêt de la normalisation pour les opérateurs est caractérisé par un intérêt général pour la valeur ajoutée générique de la normalisation, renforcé par la spécificité du secteur des télécommunications, ou plus globalement aujourd'hui de l'infrastructure mondiale des technologies de l'information et de la communication.

Du point de vue générique, la normalisation est un facteur de compétitivité pour les entreprises : elle favorise la création de nouveaux marchés en assurant l'interopérabilité des produits, ou permet de structurer des marchés vers des offres de produits et services de qualité. La normalisation permet d'établir un cadre de confiance, reconnu par tous : elle renforce la confiance entre les acteurs économiques, entreprises de produits, de services, les financeurs et les consommateurs, car les normes leur donnent l'assurance qu'un bien ou un service est adapté à l'utilisation prévue, qu'il est sûr et qu'il ne portera préjudice

ni aux personnes ni à l'environnement. Très souvent également, la normalisation permet des transferts d'innovation et de bonnes pratiques entre entreprises, même si cette acceptation doit être nuancée avec une tendance au développement de normes propriétaires, particulièrement dans le secteur des télécommunications. En d'autres termes, elle aide les constructeurs à garantir l'interopérabilité des produits et des services, à réduire les coûts, à améliorer la sécurité et à stimuler l'innovation. Au final, la valeur ajoutée de la normalisation est reconnue, car elle permet aux entreprises participant aux activités de normalisation d'exercer une influence sur les technologies et constitue l'un des éléments d'une compétitivité mondiale. Enfin, la normalisation a un impact économique directement mesurable, en permettant d'importantes d'économies d'échelle, et *in fine* de coûts plus bas pour les équipementiers, les opérateurs comme pour les consommateurs.

L'Intérêt général des opérateurs de télécommunications pour la normalisation est donc motivé par une série de bénéfices issus de cette activité. La normalisation leur permet d'abord d'encourager l'innovation, souvent en avance de phase, en étant sur le chemin critique entre la recherche/développement et le déploiement à grande échelle de biens et services. Elle est également justifiée car elle permet de répondre à des objectifs de qualité, en contribuant à améliorer la qualité des produits et services, avec des critères clairs et partagés entre les acteurs, et à des objectifs de sécurité, en renforçant la sécurité des produits, et en garantissant le respect de standards minimaux. La normalisation permet aussi et surtout une meilleure interopérabilité, critère essentiel aux activités des opérateurs au regard de la nécessité d'avoir des systèmes et des produits fonctionnant ensemble sur un large périmètre géographique.

À ces caractéristiques générales s'ajoutent les éléments spécifiques du secteur des télécommunications, qui renforcent la valeur perçue de la normalisation. En effet, dans ce secteur plus que dans tout autre peut-être, les normes sont essentielles à l'interopérabilité des TIC, et permettent d'assurer des communications dans le monde entier, en faisant communiquer ensemble réseaux et dispositifs de tous les pays. Les normes constituent ainsi un élément central de l'infrastructure mondiale des technologies de l'information et de la communication (TIC). Les normes sont essentielles à l'interopérabilité des TIC et à la capacité d'échanger des messages vidéo, vocaux ou de données.

Pour les opérateurs, les activités de normalisation portent donc avant tout sur le développement de normes techniques ou standards. Ces normes peuvent parfois avoir pour objet l'application d'une réglementation, *i.e.* l'application de décisions prises par les pouvoirs publics nationaux, par des instances régionales (par exemple au niveau européen) ou internationales. Mais dans la majorité des cas, la normalisation est une activité « volontaire », résultant d'une démarche proactive des acteurs socioéconomiques membres d'un écosystème très large : elle est ainsi le résultat d'un consensus entre entreprises, fédérations professionnelles, universités, académies, associations de consommateurs, centres de recherche, organisations de contrôle, utilisateurs et prescripteurs publics et privés, consensus qui associe aussi les pouvoirs publics, dont les représentants participent souvent aux activités de normalisation et à leurs instances de gouvernance.

Un dernier point de principe doit également être clarifié, celui de la distinction entre « normes » et « standards ». Certains experts justifient cette distinction en se basant sur des différences entre les modes d'élaboration, les premières émanant d'un organisme officiel et les secondes plutôt de *forums* de normalisation, ou des critères de délais, les contraintes étant parfois plus lourdes et les délais plus longs pour l'adoption par consensus de normes.

Du point de vue des opérateurs, cette distinction reste assez sémantique. En pratique, on constate une grande porosité, car certains standards peuvent devenir ensuite des « normes » au sens propre (*cf. European Normes*, on EN, publiées au *JOCE*), ou par la pratique du "rubber stamping" : celui-ci permet de faire endosser quasi automatiquement

et sans grand ou pas de changement le contenu d'une spécification ou d'un standard développé dans un forum, ou une instance adéquate, par un organisme officiel. La distinction entre « normes » et « standards » n'a d'ailleurs pas grande importance dans le monde anglo-saxon. *In fine*, ce qui importe le plus aux acteurs du secteur est le contenu même du texte, et ce quelle que soit l'appellation de l'enveloppe : standard, norme, norme harmonisée, ou recommandation, qui est l'appellation des standards dans le système UIT.

En dernier ressort, seule la distinction entre « standards, normes » et « régulation » mérite d'être prise en compte : les premiers sont en effet élaborés par des experts du secteur, tandis que les régulations sont élaborées par des autorités gouvernementales. Les standards et normes peuvent être volontaires, tandis que les régulations sont obligatoires et comprennent parfois des références à des normes.

En matière de règlementation, l'Europe reste aussi un cas particulier, dans la mesure où une valeur particulière est accordée aux normes européennes harmonisées. Ce type de normes est élaborée sur demande de la Commission européenne, par le biais d'une demande de normalisation (mandat) ou *Standardisation request*, adressée à une organisation européenne de normalisation reconnue (CEN, Cenelec, ou ETSI). Une fois acceptées, ces normes deviennent partie intégrante du droit de l'Union européenne et apportent aux fabricants qui les utilisent dans l'ensemble du marché unique une présomption de conformité de leurs produits aux exigences de la législation de l'UE. La conformité à ces normes garantit notamment la présomption de conformité aux exigences essentielles de santé et de sécurité, conformité qui est nécessaire et obligatoire pour obtenir le marquage CE des produits et la libre circulation sur le marché européen.

Ce processus européen spécifique d'élaboration de la norme associe de fait l'ensemble des acteurs de la normalisation, dans un cadre de principe défini par le Règlement 1025/2012 relatif à la normalisation, régulièrement révisé.

Les grands principes qui guident l'action des opérateurs

L'action des opérateurs en normalisation consiste à établir des normes et des standards pour garantir la qualité, l'interopérabilité, la sécurité et l'efficacité des produits, services ou processus.

Dans son principe, la normalisation est une activité volontaire, largement basée sur l'implication active du secteur privé (constructeurs et fabricants, opérateurs, etc.). Il est coutume de dire que la normalisation est faite par l'industrie. Ces acteurs financent ainsi une grande partie des travaux de normalisation : dans la filière générale, ce financement se fait par le paiement de cotisations aux organismes de normalisation, de participation dans les commissions de normalisation (montant unitaire à multiplier par le nombre de commissions) et aussi par l'achat des normes que ces acteurs ont contribué à élaborer.

Dans la filière des télécommunications, la contribution des opérateurs est prévisible et stable pour un exercice donné. Le coût de l'adhésion, fixe et connu à l'avance, évite ainsi aux entreprises de devoir négocier des budgets supplémentaires en cours d'exercice budgétaire, afin de pouvoir participer à des nouveaux travaux de normalisation engagés en cours d'année. Ce système présente un énorme avantage pour les entreprises, dans l'élaboration de leur budget annuel et leur contribution à la normalisation. Par ailleurs, la participation aux comités techniques est gratuite. Surtout, ce système de fonctionnement est vertueux pour les organisations de normalisation elles-mêmes, en les obligeant à respecter le cadre financier préalablement établi, et permet donc une gestion saine des finances.

Concernant l'accès aux normes, la philosophie de principe est totalement différente dans la filière des télécommunications : les normes sont en effet d'accès gratuit et libre, car elles ne sont qu'un moyen de développement des produits et services au service des acteurs et non une finalité en elles-mêmes. Cette approche de gratuité pourrait d'ailleurs s'étendre : un premier pas a récemment été franchi par la Cour de Justice de l'Union européenne (CJUE) dans une décision du 5 mars 2024 (affaire dite "Malamud"), par laquelle l'accès aux normes européennes harmonisées devient gratuit. Cette décision est tout particulièrement applicable aux normes du CEN et du Cenelec, organisations qui depuis s'emploient à en atténuer la portée, en essayant par exemple d'en limiter l'application à la seule consultation en ligne, sans possibilité de téléchargement ou d'impression.

Pour les opérateurs de télécommunications, et plus globalement les acteurs des TIC, la norme représente donc un moyen, et non une finalité, au service de l'innovation des produits et services pour le bénéfice des clients, entreprises et particuliers. La finalité du travail de leurs activités en normalisation consiste en l'élaboration de normes ou de spécifications, dont le succès se mesure par l'implémentation dans les différents produits et services, et non au nombre de téléchargements, comme cela peut souvent être le cas dans les autres filières.

Au niveau des principes, les opérateurs accordent aussi une importance particulière à un autre principe de base appliqué dans les travaux de normalisation, le principe FRAND, pour "Fair, Reasonable, and non-discriminatory" : afin de garantir un accès effectif à la norme, un accord de normalisation ne restreint pas la concurrence dès lors que la politique en matière de propriété intellectuelle exige que les participants qui souhaitent voir leurs droits de propriété intellectuelle inclus dans la norme s'engagent, de manière irrévocable et par écrit, à accorder des licences concernant leurs droits de propriété intellectuelle essentiels à l'ensemble des tiers dans les conditions du principe FRAND.

Au-delà de ces principes, les activités des opérateurs sont aussi motivées par les bénéfices induits de la participation à l'élaboration de normes qui, tout en définissant les exigences techniques et les critères de performance, permettent un contrôle de la conformité. Le secteur des TIC est aussi caractérisé par une évolution technologique et une innovation constante, se diffusant à grande vitesse sur la planète. D'où l'importance toute particulière de deux autres principes, celui de la mise à jour régulière des normes pour s'adapter aux évolutions technologiques et aux besoins du marché et celui de collaboration internationale, par le moyen d'une participation à des organisations de normalisation pour harmoniser les normes à l'échelle mondiale. En effet, les marchés des opérateurs ne sont plus depuis longtemps limités à un périmètre géographique national, et sont devenus internationaux au fur et à mesure de la libéralisation des télécommunications et de l'adhésion de la majorité des pays aux principes définis par l'Organisation Mondiale du Commerce.

L'existence de normes internationales dans le secteur des TIC est ainsi d'autant plus importante qu'elle permet d'éviter la fragmentation des marchés : pour les opérateurs, les normes dites « propriétaires » sont en effet antinomiques avec les principes de développement, d'interopérabilité et de connexion des réseaux et des produits et services.

Les moyens des opérateurs

Le *graal* historique des opérateurs de télécommunications reste le succès de la norme GSM (*Global System for Mobile Communication*) que les opérateurs aimeraient rééditer d'une façon ou d'une autre. Cette norme avait été développée par les opérateurs et les constructeurs à la fin des années 1980 au sein d'un groupe spécialisé (le Groupe Spécial Mobile, premier acronyme de GSM) au sein d'une instance de la CEPT (Conférence Européenne des Postes et Télécommunications), qui deviendra l'ETSI (European Télécommunications Standardisation Institute) par la suite. Il s'agissait alors d'une norme

numérique de seconde génération (2G) de téléphonie mobile, prédécesseur historique des normes de communication 3G, puis des évolutions ultérieures. Cette première norme avait connu un succès important en étant devenue la référence en Europe, mais aussi en Afrique, au Moyen-Orient et en Asie.

Le succès de ce travail normatif a convaincu les opérateurs d'allouer des moyens conséquents aux activités de normalisation, tant pour le développement des réseaux fixes et mobiles que pour celui des produits et services associés.

Ces moyens se traduisent tout d'abord par une implication directe dans les travaux des instances de normalisation de la filière et notamment dans les deux principales d'entre elles, l'UIT et l'ETSI. Ces deux organisations ont la compétence de principe pour les télécommunications et les fréquences de radiocommunications. Leurs travaux sont basés sur les contributions des experts, sous la propre casquette de leur entreprise : elles autorisent en effet la participation directe des entreprises, sans aucun intermédiaire ou structure de coordination, et permettent donc aux opérateurs ainsi qu'aux constructeurs d'être parties prenantes du processus de décision pour l'élaboration des standards et de participer au vote à la majorité qualifiée si un consensus n'a pu être atteint.

Le focus sur les organisations de la filière des télécommunications est aussi justifié par une séparation des tâches entre les organisations internationales : l'ISO a une compétence pour la normalisation dite générale, et deux instances plus techniques, l'une pour les électrotechnologies, l'IEC, et l'autre pour les télécommunications (UIT) complètent ce dispositif. La déclinaison au niveau régional (par exemple européen) ou national, découle de cette structure. Comme l'UIT et l'ETSI autorisent une participation directe des entreprises, le passage par une organisation nationale comme l'Association française de normalisation (AFNOR) ne s'impose pas, contrairement à la filière générale dans laquelle les normes sont élaborées sous le pilotage de cette instance ainsi que des vingt bureaux de normalisation agréés. De fait, il n'y a pas de bureau de normalisation dédié aux télécommunications ou au numérique dans l'organigramme du Système français de Normalisation (SFN).

Les moyens des opérateurs sont aussi mis en œuvre dans le cadre d'une coopération étroite, ayant pour objectif d'identifier des problématiques communes, de faire prendre en compte les spécificités de leurs activités dans les travaux de normalisation, voire parfois de lancer un travail prénormatif. Depuis l'époque du premier groupe GSM, l'action commune des opérateurs s'est ainsi structurée soit par la constitution de groupes dédiés au sein des instances reconnues, comme le collège « Opérateurs » de l'ETSI, soit par la constitution d'entités dédiées, comme la GSMA, ou le NGMN (Next Generation Mobile Networks Alliance), voire Connect Europe (ex-ETNO) pour les travaux en lien avec la réglementation européenne. Certaines de ces instances, comme la GSMA, sont ainsi devenues des références mondialement reconnues, ce que ne dément pas le succès de leur manifestation emblématique, le Mobile World Congress, organisé chaque année à Barcelone.

Un périmètre d'activités de plus en plus élargi

La participation aux activités de normalisation ne se limite pas seulement à la participation aux deux organisations emblématiques que sont l'UIT et l'ETSI mais se focalise aujourd'hui sur une multitude d'organisations et de *forums* plus ou moins spécialisés dans un domaine technique, qui est souvent le reflet de l'évolution des technologies.

Tout d'abord l'UIT et l'ETSI restent les organisations historiques de référence ayant respectivement développé la normalisation des réseaux fixes et mobiles. Aujourd'hui leur champ d'activité s'élargit considérablement.

Ainsi, l'UIT développe des travaux dans différents domaines importants pour les opérateurs de télécommunications, dont :

- les réseaux d'accès et les réseaux domestiques, notamment les réseaux du futur ou de prochaines générations, et leurs paramètres de fonctionnement ;
- les exigences, architectures, capacités fonctionnelles et interfaces de programmation d'applications des futurs réseaux ;
- les réseaux d'accès à fibre optique ;
- les communications multi-protocoles (par exemple les profils de transport : MPL-TP) ;
- les spécifications des protocoles et les exigences de signalisation ;
- la performance, la qualité de service (QoS), la qualité d'expérience (QoE) ;
- la qualité de fonctionnement du réseau pour les services, sur le protocole Internet ;
- la qualité vidéo et le codage des médias ;
- le développement du chargeur universel ;
- les ressources de numérotage ;
- les questions de tarification et de comptabilité ;
- les services *cloud* ;
- l'Internet des objets (IoT) ;
- la compatibilité électromagnétique ;
- le système de transport intelligent ;
- et enfin les questions de sécurité et de cybersécurité.

Les travaux de l'UIT-T ne se limitent pas aux considérations techniques des réseaux et produits, mais se sont aussi étendus à des domaines en phase avec les aspirations de la société et notamment l'impact des TIC sur le changement climatique. Les TIC sont à la fois une partie du problème, en étant émetteurs de gaz à effet de serre, et de la solution, en offrant des alternatives à des solutions plus énergivores. La Commission d'études 5 est en charge des travaux sur les TIC et les changements climatiques, et élabore des normes pour les deux aspects de cette problématique, dans le cadre d'un mandat très large incluant notamment l'environnement, l'action climatique, l'économie circulaire et le traitement des déchets électroniques.

Dans le détail, la participation aux travaux de la Commission d'études 5 (CE 5) permet aux opérateurs de répondre à plusieurs objectifs :

- permettre une utilisation sûre et durable des produits des technologies de l'information et de la communication (TIC) ; téléphones portables, équipements (adaptateurs, câbles, fibre optique, réseaux d'accès radio) et des installations (petites stations de base, centres de données) ;
- garantir l'efficacité énergétique et les économies d'énergie des réseaux, y compris pour les appareils domestiques (par exemple, les box Internet) ;
- élaborer les trajectoires de décarbonation pour le secteur des TIC, y compris l'ensemble de la chaîne de valeur avec les fournisseurs ;
- définir des indicateurs clés de performance et les méthodologies d'évaluation de l'impact environnemental, notamment sur le changement climatique ;

- mettre au point les indicateurs d'économie circulaire pour les réseaux mobiles et les équipements informatiques ;
- prendre en compte les effets des ondes électromagnétiques sur la santé.

Il est à noter que les normes élaborées par la CE 5, et notamment celles de la série de recommandations UIT-T L.1400 sur les méthodologies d'évaluation des TIC et des trajectoires de CO_2, sont souvent utilisées dans les cadres politiques, en France et en Europe par la Commission européenne. D'ailleurs, le travail sur ces sujets se fait le plus souvent en liaison avec les travaux d'autres organismes de normalisation (IETF, ISO, etc.). En ce domaine, la coopération la plus étroite est celle existant entre l'UIT-T CE5 et le TC EE (Environmental Engineering) de l'ETSI, qui se traduit par la publication de standards techniquement alignés, c'est-à-dire ayant le même contenu, élaboré en commun. Le TC EE a la charge de la définition des aspects environnementaux et d'infrastructures de tous les équipements de télécommunication et informatiques dans différents types d'installations, de l'amélioration de l'efficacité énergétique des équipements et de la réduction de la consommation d'énergie de refroidissement.

Concernant le second organisme historique du secteur, l'ETSI, les travaux les plus importants des comités techniques concernent d'abord l'héritage du groupe GSM, et les travaux actuels du Mobile Standards Group (MSG) consistant à :

- élaborer des normes harmonisées couvrant les exigences essentielles de la Directive sur les équipements radioélectriques et les livrables ETSI associés pour le GSM, les systèmes internationaux de télécommunications mobiles et les technologies qui en découlent ;
- identifier les exigences réglementaires européennes spécifiques aux systèmes cellulaires à développer par le 3GPP et répondre aux mandats pertinents de la Commission européenne.

D'autres travaux des comités techniques de l'ETSI présentent un intérêt manifeste pour les opérateurs, comme ceux portant sur :

- l'accès, les terminaux, la transmission et le multiplexage ;
- le domaine de la radiodiffusion (normes DVB) ;
- la cybersécurité, et notamment l'élaboration de normes relatives à la sécurité des infrastructures, des appareils, des services et des protocoles, ainsi qu'aux mécanismes de sécurité pour la protection de la vie privée ;
- les tests d'interopérabilité, consistant en l'élaboration de spécifications de test pour le réseau central (interopérabilité, conformité, performance, sécurité) ;
- les communications d'urgence ;
- les travaux sur l'interception légale, en soutien aux autorités publiques, et consistant à développer des normes soutenant les exigences du droit national et international en matière d'interception légale et de divulgation légale des communications électroniques.

À côté de ces deux organisations, l'UIT et l'ETSI, une multitude d'organisations et de *forums* se sont développés. Elles élargissent considérablement le périmètre d'activités des opérateurs. Le groupe Orange, par exemple, participe aux travaux de près de quarante organisations de standardisation, à commencer par les plus importantes pour les activités d'opérateurs : outre l'UIT et l'ETSI, figurent dans cette liste ;

- le 3GPP, en charge du développement des normes techniques 5G et 6G pour la téléphonie mobile ;
- le Broadband Forum ;

- la GSMA ;
- l'IETF (Internet Engineering Task Force) ;
- le TM Forum (Telemanagement Forum) ;
- l'ICANN, le RIPE NCC pour les aspects relatifs à Internet.

D'autres organisations de standardisation, le plus souvent dédiées à des thématiques plus spécialisées, font aussi l'objet d'une mobilisation des opérateurs : on peut citer par exemple :

- la Wi-Fi Alliance ;
- le FSAN (Full Service Access Network) ;
- l'IEEE (Institute of Electrical and Electronics Engineers) ;
- le NGMN (Next Generation Mobile Networks Alliance) ;
- la LoRa Alliance ;
- le DVB (Digital Video Broadcasting) ;
- ou, au plan national, les travaux de l'AFNOR et notamment certains comités miroirs de l'ISO.

Les principaux enjeux de la participation en normalisation pour Orange

Le cas d'Orange est particulièrement représentatif de la participation aux travaux de normalisation. Orange est en effet à ce jour le seul opérateur national de télécommunications à participer activement aux travaux des organisations de standardisation. Cette participation est motivée par plusieurs enjeux.

Le premier consiste à promouvoir la stratégie technologique développée par le groupe : Orange dispose en effet d'une importante équipe d'innovation, héritière du centre de recherche et de développement des télécommunications de l'ex-Centre national d'études des télécommunications (CNET).

Au travers de cet enjeu, l'objectif est de promouvoir des spécifications conformes aux priorités d'Orange en matière de réseaux, de services et des diverses fonctionnalités associées. Il consiste aussi à promouvoir un écosystème ouvert, permettant un choix de plus en plus flexible de fournisseurs et de partenaires, avec une interopérabilité efficace entre fournisseurs grâce à des interfaces ouvertes (par exemple, Open RAN – Radio Access Network). Enfin, il s'agit de garantir les meilleures performances réseau et de favoriser l'efficacité énergétique des réseaux.

Le second objectif consiste à valoriser l'expertise technique du groupe. Cet objectif est réalisable grâce à l'implication directe dans l'élaboration des spécifications techniques et la collaboration au sein d'un écosystème associant notamment les experts des fournisseurs. En ce domaine, Orange peut capitaliser sur l'expérience acquise en matière de normes pour anticiper l'évolution du réseau et accompagner les projets d'innovation, comme la définition des exigences des appels d'offres, ou répondre au challenge des implémentations des fournisseurs.

Cette expertise technique permet aussi d'accompagner les déploiements et les défis opérationnels (meilleures pratiques, résolution des problèmes opérationnels *via* les normes…) et de réduire les efforts internes de test et de validation grâce à l'adoption de schémas et procédures de test conformes aux normes.

Enfin, le troisième objectif est de garantir l'influence d'Orange et des opérateurs dans l'écosystème de la standardisation. Orange est ainsi invité à la table des négociations par d'autres opérateurs et partenaires. Cette implication précoce permet d'anticiper et de définir les réseaux de nouvelle génération, ou simplement de détecter les tendances commerciales et technologiques futures. Orange est également invité à répondre aux appels d'offres. Enfin, la participation aux activités de normalisation constitue aussi une des bases du *lobbying*, afin de développer des alliances (avec les opérateurs/partenaires) et de promouvoir des exigences communes.

Ces enjeux soutiennent une stratégie et des développements au service des clients

Au final, la participation n'est pas altruiste, mais permet de retirer à moyen terme des bénéfices importants pour les différentes activités du groupe, en particulier lorsque les développements technologiques peuvent être monétisés. Les principaux enjeux et actions sont ainsi guidés par la stratégie et les objectifs de l'entreprise.

Il s'agit tout d'abord de moderniser, simplifier et optimiser les réseaux fixes et mobiles, en passant au très haut débit : c'est le cas avec les Réseaux 2030 et « au-delà des G – Beyond G », l'évolution et l'interopérabilité des réseaux d'accès et de transport optiques, et le mouvement actuel d'automatisation et de virtualisation des réseaux. L'intégration des évolutions logicielles aux réseaux représente ainsi un challenge porteur.

Le second enjeu consiste à maîtriser l'évolution technologique afin d'apporter une valeur ajoutée significative aux clients du groupe. Aujourd'hui, un véritable mouvement de fond est engagé, conduisant à la désagrégation et à la transformation du réseau et caractérisé par une convergence industrielle sur la couche *cloud* du réseau (*cf.* travaux de l'Alliance O-RAN). Il s'agit donc d'améliorer et de développer de nouveaux services afin de créer de nouvelles opportunités commerciales.

Le troisième enjeu est plus spécifique au cœur de métier des opérateurs de télécommunications et d'infrastructure : il consiste à construire et exploiter des réseaux sécurisés. Au-delà des aspects de sécurité traditionnels, il couvre aujourd'hui de nouveaux champs issus des évolutions technologiques récentes : la sécurité post-quantique, avec *in fine* le potentiel énorme du cryptage, la prise en charge de l'eSIM pour les nouvelles activités (par exemple, l'IoT) pour la téléphonie mobile, et les nouveaux services à valeur ajoutée (par exemple, le portefeuille électronique), ou pour le réseau fixe des particuliers l'activation du mode *wifi* sécurisé WPA3 dans les réseaux domestiques.

Enfin, en référence à la problématique de l'impact des TIC sur le changement climatique, le quatrième et dernier enjeu prend en compte les questions liées à l'environnement, à l'action climatique, à l'économie circulaire et au traitement des déchets électroniques, par le biais de standards d'efficacité énergétique : le travail de normalisation s'inscrit dans l'une des priorités affichées par la directrice générale du groupe, afin de développer des réseaux et services écologiques et économes en énergie. Ces actions se traduisent à tous les niveaux, des réseaux aux services finaux, au moyen de mesures d'économies et d'efficacité énergétique (dans les appareils, dans les bâtiments ainsi que les véhicules), de mesure des émissions de type Scope 3 ou de gestion du cycle de vie des équipements. Très souvent, elles sont menées avec le concours de partenaires, comme les constructeurs, eux aussi engagés dans des démarches équivalentes et participant activement aux différents travaux de normalisation dans ce domaine.

Deux exemples concrets : SDN et le WIFI 7

Le concept de la *softwarisation* du réseau, ou "Software Defined Networking" (SDN)

Le concept de la *softwarisation* du réseau, connu sous la dénomination "Software Defined Networking" (SDN), est illustratif du travail de normalisation sur une composante clé pour les opérateurs de télécommunications, le réseau. Il est aussi symbolique de la coopération existante entre plusieurs organisations majeures de standardisation : l'UIT-T, l'IETF et l'ONF (Open Networking Foundation).

Le SDN est basé sur l'utilisation d'une couche de logiciel programmable ayant une vue globale et logique du réseau sous-jacent et de ses ressources, permettant ainsi une gestion dynamique de la connectivité à travers ce réseau. Le SDN a pour ambition de transformer la gestion des ressources, souvent hétérogènes, des réseaux en une plateforme de contrôle programmable et flexible.

Le SDN répond à plusieurs cas d'usage, comme par exemple la configuration « à la demande » de la connectivité réseau, la gestion dynamique des ressources réseau et la gestion de la connectivité réseau entre les plateformes NFV (fonctions virtuelles).

La normalisation du SDN a ainsi été effectuée au sein de plusieurs instances, dont les travaux ont finalement été complémentaires.

Ces travaux ont tout d'abord été initiés à l'UIT-T. Au début des années 2010, la commission d'études (CE) 13 de l'UIT-T a abordé le thème des réseaux du futur ("Future Networks") et dans ce cadre a publié plusieurs standards précurseurs du SDN telles que la Recommandation UIT-T Y.3001 "Future networks: objectives and design goals" (2011) et la Rec. UIT-T Y.3011 "Framework of network virtualization for future networks" (2012).

Sur la base de ces travaux sur les réseaux du futur, la CE 13 de l'UIT-T a adopté en 2014 une première définition du SDN, à savoir « un ensemble de techniques permettant de programmer, orchestrer et gérer les ressources réseau afin de faciliter la conception, la fourniture et l'opération des services réseaux de manière dynamique et évolutive » (*cf*. Rec. UIT-T Y.3300).

La Rec. UIT-T Y.3300 ("Framework of software-defined networking") fournit également une architecture de haut niveau du SDN comprenant une description de trois couches, à savoir :

- une couche de services applicatifs réseau (tels que des applicatifs permettant la gestion de VPN à la demande) ;
- une couche de contrôle contenant des fonctions d'abstraction et de programmation des ressources réseau sous-jacentes et offrant un ensemble de services comme la gestion des nœuds (routeurs et commutateurs) et des liens associés ;
- une couche de ressources comprenant les ressources réseau constituées par l'ensemble des éléments de réseaux physiques ou virtuels (routeurs et commutateurs).

En plus des activités UIT-T susmentionnées, la CE15 de l'UIT-T avait développé des normes relatives aux Réseaux de Transport de type SDN (Rec. G.7702 spécifiant l'architecture de plan de contrôle SDN pour les réseaux de transport).

D'autres travaux relatifs au SDN avaient aussi eu lieu à l'Internet Engineering Task Force (IETF) : l'IETF a notamment développé des solutions visant à faciliter la program-

mabilité des réseaux et donc, bien que ne le concernant pas directement, des standards applicables à un environnement SDN, comme notamment :

- le protocole NETCONF (et RESTCONF dans sa version HTTP) qui fournit un mécanisme pour gérer la configuration des éléments de réseau ;
- le langage de modélisation de données YANG, qui peut être utilisé pour spécifier des modèles de données de gestion de réseau transportés *via* des protocoles tels que NETCONF et RESTCONF ;
- le chaînage de fonctions de service (SFC) permettant la définition et l'instanciation d'une liste ordonnée d'instances de fonctions de service, et le contrôle du trafic s'écoulant à travers ces fonctions de service ;
- les extensions au protocole Border Gateway Protocol (BGP) comme des solutions de VPN pour utilisation dans les réseaux au sein de centres de données (*data centers*) et de solutions de VPN permettant la construction de topologies virtuelles servant de support à des services tels que le "Service Function Chaining (SFC)" ;
- la spécification des protocoles dans le cadre d'une architecture de réseau utilisant un serveur externalisé (PCE "Path Computation Element") pour le calcul des chemins dans les réseaux IP-MPLS et GMPLS.

Enfin, quasi en même temps, en 2011 un nouveau forum dénommé "Open Networking Foundation" (ONF) avait été établi avec pour objectif la spécification d'une solution SDN reposant sur la séparation des plans de transfert et de contrôle réalisée à travers l'utilisation du protocole *OpenFlow* développé en phase initiale par l'Université de Stanford.

Les principaux documents liés à l'architecture, produits par l'ONF, sont les suivants :

- SDN Architecture (TR-521, février 2016) : l'architecture décrite est agnostique aux technologies utilisées et repose sur une découpe selon trois plans, à savoir « plan applicatif », « plan de contrôle » et « plan de données », similaire à celle décrite dans la Rec. UIT-T Y.3300 ;
- Modèle d'information "Core Information Model" version 1.2 (septembre 2016 | TR-512.1) : ce document ONF fournit une représentation des ressources de « transfert » réseau indépendante des technologies d'acheminement spécifiques utilisées dans les réseaux (IP, Ethernet, optique…) ;
- Architecture SDN pour les réseaux de transport (TR-522, mars 2016) : cette spécification décrit l'application de l'architecture (TR-521) et la modélisation de l'information (TR-512.1) nécessaire pour une utilisation du SDN dans les réseaux de transport.

Par ailleurs, l'ONF avait développé les spécifications du protocole *OpenFlow* (OF). OF est un protocole de communication permettant l'accès direct et la manipulation du plan d'acheminement des éléments de réseau tels que commutateurs ou routeurs qu'ils soient physiques ou virtuels, complété ensuite par un protocole de configuration et de gestion appelé OF-CONFIG permettant la configuration à distance des commutateurs *OpenFlow*.

Ainsi, les experts des réseaux d'opérateurs doivent intégrer ces différents paramètres, issus de travaux de plusieurs organisations, en avance des déploiements qui seront opérés. La participation aux activités de normalisation permet d'anticiper les évolutions des réseaux. Aujourd'hui, sur ces bases, Orange propose à sa clientèle « entreprises » des offres dites « SD-WAN » (Sofware Defined Wireless Access Network) basées sur un *backbone* IP et permettant de relier les différents sites clients avec une excellente connectivité.

Le *wifi* 7

La norme *wifi* fait partie des normes bien connues du grand public, mais elle couvre en réalité des spécifications techniques qui ont fortement évolué ces vingt dernières années. L'adoption de la dernière évolution en avril 2025 constitue un exemple d'actualité du succès des travaux de normalisation. Cette évolution résulte du travail de normalisation opéré au sein d'une agence dédiée, la Wi-Fi Alliance. Orange est membre de l'Alliance Wi-Fi et participe aux travaux d'élaboration de la norme, reprise dans nombre de ses produits, dont les box internet (près de 10 millions en *wifi* 5). L'écosystème au sein de cette Alliance est vaste et comprend notamment des constructeurs internationaux (Apple, Huawei, ZTE, Nokia, Sagemcom, Qualcomm), des grands opérateurs américains, européens, et asiatiques, ainsi que les principaux fournisseurs de *chipset*. Cette contribution active à la Wi-Fi Alliance permet aux experts du groupe de jouer un rôle essentiel dans l'évolution des technologies *wifi*, en assurant une transition vers des normes performantes et plus sécurisées et en offrant une amélioration continue de l'expérience client.

Le développement de la nouvelle norme *wifi* 7 est ainsi illustratif de l'apport de la normalisation aux nouveaux produits et services, car elle sera immédiatement intégrée dans les nouvelles box de l'opérateur. Cette intégration du *wifi* 7 marque une étape significative dans l'évolution de la connectivité domestique sans fil, car cette technologie promet des débits plus élevés et une gestion plus efficace des appareils connecté, de plus en plus nombreux pour des usages multiples : accès à Internet et aux services vidéos (OTT, *web*, etc.), TV, *gaming*, travail, électroménager, etc. La conception d'une nouvelle box internet nécessite de prendre en compte près de 1 200 spécifications, dont un quart uniquement pour le *wifi*.

La capacité à gérer des connexions haut débit simultanées de plusieurs appareils est cruciale dans un environnement domestique moderne, où les *smartphones*, tablettes, ordinateurs portables et appareils intelligents sont omniprésents. Le *wifi* 7 permet justement une gestion plus efficace des bandes de fréquence, améliorant ainsi la couverture et la stabilité du réseau. Cette technologie va donc être particulièrement bénéfique aux foyers qui comptent de nombreux appareils connectés. La gestion efficace des bandes de fréquence permet en effet de réduire les interférences et d'optimiser la distribution du réseau, et donc d'assurer une connexion stable et rapide pour tous les appareils connectés.

Le travail normatif au sein de la Wi-Fi Alliance a ainsi nécessité la prise en compte d'intérêts divers. Orange a particulièrement axé ses efforts sur une sécurité renforcée, notamment en termes de cryptage et de gestion des clés de sécurité. Le *wifi* 7 intègre des protocoles de sécurité avancés, tels que le WPA3, qui offre une meilleure protection contre les attaques. Orange a aussi joué un rôle central dans la promotion et l'adoption du standard WPA3-Compatibility Mode et à l'adoption d'un identifiant unique (SSID) à destination des équipements *wifi*.

Dans la ligne de sa stratégie environnementale, Orange a aussi poussé au respect des normes en ce domaine. Les nouvelles box qui intègreront le *wifi* vont en effet gérer de manière dynamique certains paramètres et les adapter aux besoins réels pour réduire la consommation, en activant ou désactivant des bandes de fréquences ou des points d'accès ; certaines bandes de fréquences seront ainsi désactivées à certains moments de la journée grâce à des algorithmes pour rester proche de la consommation énergétique du *wifi* 6E, dans le respect des normes européennes imposant une consommation inférieure à 8 watts en 2025 et 7 watts en 2027.

L'exemple du *wifi* 7 pourrait devenir un cas d'école. En effet, la participation à une instance de normalisation comme la Wi-Fi Alliance permet à Orange d'améliorer la fiabilité du *wifi* (diagnostic, sécurité), mais aussi de se différencier par rapport à la concurrence. Vis-à-vis des clients, Orange développe les différents avantages perçus en termes de qualité d'expérience, d'amélioration de la couverture radio, de gestion des interférences en zone dense,

de gestion de la coexistence entre les différentes générations, de simplicité (appairage et sécurité) et de maîtrise de la consommation énergétique.

Le travail en standardisation ne constitue cependant qu'une étape sur le chemin critique de développement d'un produit : au-delà de la standardisation, le travail d'Orange Innovation commence en fait là où s'arrête les standards. Les analyses et améliorations des algorithmes en sont un exemple représentatif : le travail d'analyse nécessite de comprendre et d'influencer l'écosystème et tous ses acteurs et d'effectuer un *monitoring* et un diagnostic fin du réseau *wifi* (liste des stations, topologie, liens radio…). Les standards notamment ne précisent pas le format, la collecte, la mesure des paramètres *wifi*, qui diffèrent d'un *chipset* à l'autre (pas les mêmes API, pas les mêmes noms), d'une génération à l'autre et ont des valeurs hétérogènes. Il convient donc d'identifier, évaluer et valider les différents paramètres et algorithmes de diagnostic du *wifi*, notamment ceux assurant la gestion multi-liens (MLO) ou multi- connectivité, ou ceux assurant la gestion du spectre (*puncturing*) en mode dynamique ou statique. Enfin, le développement nécessite un travail postérieur de définition et d'analyse d'indicateurs clés rendant lisibles les indicateurs techniques de qualité de service (niveau de signal, d'interférences, débit, etc.) en qualité d'expérience perçue par le client.

Autour de la normalisation

La participation aux travaux de normalisation ne se limite pas à la participation aux seuls débats techniques, mais peut aussi comprendre une mobilisation de caractère plus institutionnel. En effet, l'évolution du cadre règlementaire fait souvent référence à des actions normatives, rendant utiles la participation à des instances qui sont sur le chemin critique du cadre légal, comme par exemple certaines instances consultatives européennes : European Commission High Level Forum for Standardisation (HLF), ICT Multi-Stakeholder Platform for ICTS Standardisation (ICTS-MSP). Les opérateurs y participent *via* leurs instances représentatives (Connect Europe, ex-ETNO). Ces instances sont notamment consultées pour l'élaboration des Standardisation Request ou demandes de normalisation qui sont émises par la Commission et adressées aux instances européennes de normalisation, et seront la base des normes européennes harmonisées.

Plus en amont, les opérateurs sont aussi force de propositions, et ont récemment proposé la création d'une agence européenne (JASTE, Joint Agency for Standards and Technology Europe), destinée à renforcer le rôle de la standardisation en faisant mieux prendre en compte les résultats des travaux de recherche européens par les différents organismes de standardisation. La Commission européenne avait aussi annoncé le lancement d'un « accélérateur de normalisation » (Standardisation Booster) pour aider les chercheurs travaillant dans le cadre des programmes « Horizon Europe » à tester la pertinence de leurs résultats pour la normalisation.

D'un point de vue sociétal, la pédagogie autour de l'apport des normes nécessite aussi d'être développée. Tout le monde a en mémoire le *bashing* sur la 5G, qui a pris une dimension émotive exacerbée et disproportionnée dans un contexte de sensibilité accru par la crise du Covid-19. Les effets démultiplicateurs des réseaux sociaux ont amplifié des réactions et des comportements ne laissant guère de place aux explications rationnelles. Des émetteurs de TV ont même été brûlés par quelques activistes persuadés de s'en prendre à des antennes 5G, dont le déploiement n'avait pas encore commencé ! Aujourd'hui, ces préoccupations ne sont plus d'actualité et le réseau 5G se déploie plus sereinement.

Enfin, dans un autre domaine, la normalisation pâtit d'un manque de formation et d'éducation des parties prenantes sur l'importance des normes et leur application. Il n'y a pas ou peu d'enseignement en école d'Ingénieurs ou dans des cursus appropriés. La formation des experts se fait sur le terrain, et se traduit par une expérience acquise au cours de la vie professionnelle. Orange avait poussé, avec les pouvoirs publics, à une intégration d'un

module de formation dédié à la standardisation, mais ce travail de longue haleine n'a pas abouti, malgré le soutien de l'Afnor et des pouvoirs publics.

Au-delà de la normalisation ?

De nombreuses voix se font entendre, stipulant que la normalisation a été utile pour le développement des réseaux dans le passé, mais qu'elle a fait son temps et qu'il faut se tourner désormais vers l'*open source*. Les organisations de ce domaine elles-mêmes exercent un *lobbying* important pour éclairer sur le rôle de l'*open source* et expliquer comment l'*open source* peut faire évoluer les contextes de standardisation.

Les arguments mettent en avant le caractère disruptif des solutions *open source* par rapport à celles de standardisation, la simplification des processus et la facilité d'adaptation au monde des technologies de l'information (IT), la rapidité d'implémentation des solutions au regard du temps long de développement des standards.

Dans ce contexte, les opérateurs de télécommunications ont entrepris de participer ou s'intéressent à plusieurs organisations dites *open source*, comme par exemple :

- Linux Foundation ;
- OASIS Open ;
- Eclipse Foundation ;
- Apache Foundation ;
- Linux Foundation Data and IA ;
- Node ;
- Kubernetes.

Cependant, les acteurs de l'*open source* ont eux aussi conscience des limites d'un système qui n'atteint pas l'efficacité des travaux élaborés dans les organisations de standardisation. Ils proposent ainsi de mettre en place des passerelles ou des processus afin que les travaux des communautés *open source* soient adoptés rapidement par les *forums* ou *consortiums*, voire d'établir des mécanismes de coopération formalisés entre les deux mondes. Ils proposent même de mettre en place de nouveaux processus au sein de la gouvernance des organisations européennes reconnues, afin que l'*open source* soit intégré à leurs travaux et, *in fine*, contribue à créer un environnement attractif et innovant pour la standardisation de l'IT en Europe. *A minima*, une collaboration devra être envisagée entre les deux mondes.

Conclusion : anticiper et préparer le futur

Le travail de normalisation n'est pas immédiatement payant. Certains choix, aussi, peuvent avec le recul ne pas avoir été pertinents. D'autres apports de normalisation sont contestés jusqu'au stade final : cela a, par exemple, été le cas de la norme sur le chargeur universel, qui a été contestée par un célèbre fabricant de téléphonie disposant d'une technologie propriétaire, pendant plus de dix ans, jusqu'à épuisement de tous les recours.

Cependant, la normalisation est une activité vivante et en constante évolution. Elle nécessite un investissement permanent que peu d'opérateurs ont encore les moyens de mobiliser ; ainsi, en France, seul Orange, parmi les quatre opérateurs mobiles, met encore des moyens en normalisation.

Les chantiers ne manquent pas. Pour les opérateurs de télécommunications, le futur proche se traduit par la préparation à l'évolution de la téléphonie mobile et de sa future norme, la 6G. Celle-ci intègre des aspects techniques plus complexes, comprenant par

exemple une dimension satellitaire. D'autres domaines nécessiteront aussi des travaux de standardisation, comme la définition des normes pour les *data centers*, et notamment leur consommation (énergie, eau, travaux sur les batteries), démultipliée suite à l'accroissement de l'usage de l'Intelligence artificielle.

L'acte de décès de la normalisation n'est donc pas prêt d'être publié !

La gouvernance d'Internet entre consolidation et fragmentation

Par Lucien CASTEX
Conseiller du Directeur général, Internet Gouvernance, Internet et Société,
Association française pour le nommage Internet en coopération (Afnic)

La gouvernance d'Internet s'est progressivement mise en place sur le modèle d'un internet ouvert et distribué aboutissant à une approche multi-parties prenantes consacrée par le sommet mondial sur la société de l'information.

Cette gouvernance d'Internet se trouve 20 ans après entre fragmentation et consolidation avec à la fois une multiplication et une complexification des processus, comme confrontée à une évolution technologique rapide et ubiquitaire. Internet et sa gouvernance se trouvent au centre d'enjeux politiques et géopolitiques, leur légitimité et leur efficience étant questionnées, ainsi que leur capacité – ou non – à gérer les problèmes de notre temps.

2025 sera-t-elle une année de fragmentation ? Internet et sa gouvernance semblent sur toutes les lèvres, tant dans les discussions politiques que techniques, avec la prise en compte des effets du quantique ou de l'intelligence artificielle, l'évolution des modalités d'accès à Internet, sa neutralité[1] ou encore sa sécurité, tout cela dans un contexte politique loin de l'équilibre.

Car Internet, réseau de réseaux, dont l'architecture distribuée a fait montre de résilience, a démontré sa capacité à évoluer et à s'adapter aux usages comme aux évolutions technologiques. Internet est toujours en construction, au niveau technique, par le développement de nouveaux protocoles et standards comme par l'évolution des usages et l'apparition de nouveaux services. La gouvernance d'Internet s'est développée sur ce même modèle *ad hoc*, distribué et inclusif.

Cette année 2025 marque le 20e anniversaire du Sommet mondial sur la société de l'information (SMSI) et avec lui un réexamen dont les enjeux dépassent le seul cadre de la gouvernance d'Internet. Internet est dans nos foyers, à nos poignets, dans des applications de la vie courante que nous ne soupçonnons parfois pas, au point d'en devenir quasi ubiquitaire. La complexité du monde numérique en 2025 réside dans cette intrication avec tous les aspects de nos existences, y compris avec les politiques publiques.

La gouvernance d'Internet se trouve ainsi au centre d'enjeux politiques et géopolitiques, sa légitimité et son efficience étant questionnées, ainsi que sa capacité – ou non – à gérer les problèmes de notre temps.

Progressivement mise en place sur le modèle d'un Internet ouvert et distribué, la gouvernance d'Internet issue du SMSI se trouve 20 ans plus tard questionnée face à la place croissante d'Internet dans la société.

[1] CASTEX L. (2020), « La neutralité de l'Internet face au besoin de régulation », in *Les enjeux contemporains des communications numériques* (dir. Hélène de Pooter, Marine They), Éds Pedone.

D'Internet à la gouvernance d'Internet : un développement en miroir

À l'heure du développement de l'ADSL en France, l'organisation pour la première fois d'un Sommet mondial sur la société de l'information marquait, de 2003 à Genève et 2005 à Tunis, la rencontre des parties prenantes dans un format plus ouvert et innovant, témoignant d'une volonté d'échanger sur un sujet qui traversait déjà la société et comportait de nombreux éléments d'extranéité. En France, le Programme d'action gouvernemental pour la société de l'information (PAGSI) lancé en 1997 pour préparer l'entrée dans la société de l'information venait d'être prolongé en novembre 2002 par le programme gouvernemental RE/SO 2007 – Pour une République numérique dans la société de l'information – avec notamment l'objectif de faire de l'État un acteur de la société de l'information ayant une vocation d'exemplarité.

Ainsi, le SMSI reconnaît la place des parties prenantes dans les discussions touchant à Internet et à son développement, et non pas une approche uniquement multilatérale. Est adopté un modèle dit multi-parties prenantes, à la fois distribué et ouvert, déjà expérimenté avec succès au sein de l'IETF, *Internet engineering task force*, qui développe des standards et protocoles Internet, ou de l'ICANN qui gère les ressources critiques d'Internet, telles que les noms de domaine de premier niveau, les adresses IP ou les numéros d'AS.

La gouvernance d'Internet s'inspire des modalités de fonctionnement et des propriétés d'Internet, distribuée, globale et en réseau. Personne n'a le pouvoir d'arrêter Internet, ce qui implique une forte et nécessaire collaboration entre les parties prenantes.

L'agenda de Tunis définit en 2005 la gouvernance d'Internet, développée au sein du groupe de travail sur la gouvernance d'Internet[2]. Ainsi, la gouvernance d'Internet consiste en « l'élaboration et l'application par les gouvernements, le secteur privé et la société civile, dans leurs rôles respectifs, de principes, normes, règles, procédures de prise de décision et programmes communs qui façonnent l'évolution et l'utilisation de l'Internet ». La reconnaissance du rôle des parties prenantes va de pair avec une spécialisation et la reconnaissance de la diversité des expertises et des points de vue : gouvernements, société civile, communauté technique ou secteur privé. Si les modalités de cette gouvernance sont globalement acceptées, elles n'en demeurent pas moins discutées et parfois contestées.

Le Forum sur la gouvernance de l'Internet voit le jour de la même manière. Si une discussion multipartite doit se tenir, il faut encore créer l'espace de discussion permettant de faire dialoguer ces expertises et faciliter une diversité des regards et perspectives. La tenue d'un forum annuel au niveau international est complétée par l'émergence de travaux organisés en forums de bonnes pratiques, en coalitions dynamiques librement formées et par la mise en place progressive de réseaux de politiques. À cet édifice, viennent s'ajouter des forums nationaux et régionaux qui se sont progressivement développés et permettent d'aborder ces enjeux localement. Il en résulte une hybridation croisée entre le Forum mondial et les forums locaux nationaux et régionaux.

La société de l'information, 20 ans après. Prévu par l'agenda de Tunis, l'examen du SMSI se déroule cette année, en 2025. Évaluer le SMSI à 20 ans pose la question plus large de l'adéquation du modèle de gouvernance distribuée, des modalités d'implication des parties prenantes, tout comme de la pertinence des sujets traités[3] : des lignes d'action

[2] Sommet mondial sur la société de l'information, Geneva Plan of Action, WSIS-03/GENEVA/DOC/0005, 12 December 2003.

[3] Voir le document final sur l'examen de la mise en œuvre des textes issus du SMSI, adopté le 16 décembre 2015 par l'Assemblée générale des Nations Unies (A/RES/70/125).

créées il y a 20 ans, aux mandats des agences des Nations Unies et jusqu'aux institutions créées.

L'importance et la centralité du numérique et des infrastructures sous-jacentes, en premier lieu Internet, accentuent les tensions politiques internes comme externes et laissent poindre un risque de fragmentation[4]. Non pas une fragmentation technique, mais bien une fragmentation des gouvernances.

Alors que la Commission de la science et de la technique au service du développement (CSTD) vient d'achever les travaux de sa 28e session[5], que le prochain Forum sur la gouvernance de l'Internet est prévu à Lillestrøm en Norvège en juin 2025, cet examen à 20 ans cristallise les tensions au niveau international, entre États comme entre les parties prenantes elles-mêmes, et une réémergence des questions de souveraineté technologique : des infrastructures elles-mêmes aux services numériques.

Les modalités de cet examen à 20 ans ont été adoptées en mars 2025. Elles reprennent celles d'il y a 10 ans tout en soulevant des inquiétudes quant à la capacité d'engagement réelle des parties prenantes dans le processus, vu le contexte géopolitique tendu et la transversalité des questions numériques. L'Agenda numérique global est contesté, du G20, sous présidence sud-africaine, au groupe des BRICS, sous présidence brésilienne en 2025, au G7 et à l'Assemblée générale des Nations Unies.

L'examen se déroule également dans des délais très contraints pour une adoption prévue en décembre 2025, laissant peu de temps à la discussion. Par comparaison, lors du dernier examen en 2015, un processus préparatoire avait été mis en place permettant en particulier une consultation approfondie des parties prenantes par le biais d'une plateforme mise en place par l'UIT avant même l'adoption des modalités d'examen.

La société de l'information, 20 ans après : vers une fragmentation des gouvernances ?

Le fonctionnement même d'Internet et ce modèle de gouvernance ont permis d'assurer le développement continu d'Internet, sa résilience et de favoriser un modèle d'innovation ouverte, sans permission, basé sur l'interopérabilité et la coopération[6].

Il y a 20 ans, la Déclaration du Millénaire[7] venait d'être adoptée en septembre 2000 – dont les 8 objectifs du Millénaire pour le développement sont intégrés aujourd'hui au sein des objectifs de développement durable – et l'Assemblée générale des Nations Unies (AGNU) relevait l'urgence « d'exploiter le potentiel que recèlent les connaissances et la technologie pour réaliser les objectifs de la Déclaration du Millénaire et de trouver des moyens efficaces et novateurs de mettre ce potentiel au service du développement pour tous »[8]. Ces mots sont d'une actualité renouvelée aujourd'hui alors que l'on aborde les enjeux du numérique et les développements de l'intelligence artificielle. Rappelons également l'actualité des

[4] PERARNAUD C., ROSSI J., CASTEX L. & MUSIANI F. (2022), "'Splinternets': Addressing the renewed debate on internet fragmentation", [Research Report], Panel for the Future of Science and Technology, Parlement européen, Scientific Foresight Unit (STOA).

[5] "Report on the progress made in the implementation of the outcomes of the WSIS during the past 20 years", United Nations Commission on Science and Technology for Development, 19 mars 2025.

[6] Lucien Castex (2024), « La gouvernance de l'Internet et la construction d'un nouveau multilatéralisme », in *Brunessen Bertrand, Guillaume Le Floch (dir.), La souveraineté numérique*, Bruylant.

[7] Déclaration du Millénaire, A/RES/55/2.

[8] Sommet mondial de la société de l'information, A/RES/56/183.

fractures numériques, avec une estimation de plus de 2,6 milliards de personnes encore non connectées à Internet[9] et le lien étroit entre niveau de développement et connectivité.

L'écosystème des Nations Unies a également largement évolué et s'est complexifié, faisant place à de nouveaux organes et devant composer avec les instances de normalisations comme avec de nouvelles initiatives portées par les parties prenantes.

Dans la suite de la publication du plan d'action de coopération numérique[10] qui répond au rapport du groupe de haut niveau éponyme, le Secrétaire général avance que l'ONU « est prête à servir de plateforme de dialogue sur les politiques à suivre entre les multiples parties prenantes concernant les technologies émergentes »[11] . Pour ce faire, et avec l'objectif de faciliter la coordination des activités menées par les Nations Unies, un envoyé pour les technologies est créé. L'année suivante, en 2021, le rapport du secrétaire général intitulé « Notre programme commun » propose l'adoption d'un pacte numérique mondial[12].

Un nouvel instrument est ainsi négocié pendant près de 2 ans jusqu'à son adoption en septembre 2024 : « Le pacte de l'avenir »[13] dont la première annexe consiste en un pacte numérique mondial.

Différentes phases de consultations, parfois tendues et diversement perçues par les parties prenantes, ont abouti à un document qui, s'il n'est pas contraignant, reconnaît la nécessité de renforcer la coopération numérique, le caractère mondial et multipartite de la gouvernance d'Internet[14] et rappelle le rôle du FGI comme « principale instance multipartite d'échanges » en matière de gouvernance d'Internet[15].

Ainsi, dans la lignée du SMSI, le pacte pose comme principe que « les États, le secteur privé, la société civile, les milieux technologiques et universitaires et les organisations internationales et régionales, chacun dans leur rôle et leurs missions, sont indispensables à l'avènement d'un avenir numérique inclusif, ouvert, sûr et sécurisé. La coopération que nous entendons mettre en place sera multipartite et mobilisera les contributions de toutes et de tous »[16].

Le pacte n'en crée pas moins plusieurs nouveaux organes. S'ajoutent également aux lignes d'action du SMSI, une série de nouveaux objectifs, de principes, d'engagements et d'actions rendant nécessaire une cartographie entre les livrables attendus, les lignes d'action mais aussi les objectifs de développement durable. La complexification s'accentue.

Est ainsi constitué un groupe scientifique international multidisciplinaire indépendant sur l'intelligence artificielle[17], ainsi qu'un bureau chargé de faciliter la coordination de l'ensemble du système des Nations Unies. Le bureau de l'envoyé spécial pour les technologies, créé en 2022, devient ainsi un bureau pour les technologies numériques et émergentes (ODET) rattaché directement au Secrétaire général. Ce nouveau bureau a pour mission de faciliter cette coordination et de travailler étroitement avec les mécanismes existants, dont le SMSI. Un *modus vivendi* reste à déterminer.

---

[9] UIT, Mesurer le développement numérique : Faits et chiffres 2024.

[10] Plan d'action de coopération numérique : application des recommandations du groupe de haut niveau sur la coopération numérique, Rapport du Secrétaire général, 29 mai 2020 (A/74/821).

[11] *Ibid* par. 73.

[12] La note d'orientation publiée le 17 janvier 2023 "Global Digital Compact: Background Note".

[13] Le Pacte pour l'avenir, 20 septembre 2024, A/79/L.2

[14] *Ibid*. Pacte numérique mondial 27.

[15] *Ibid*. Pacte numérique mondial 28 et 29 b).

[16] *Ibid*. Pacte numérique mondial 8.k.

[17] *Ibid*. Pacte numérique mondial 56 a).

La diversité des processus n'a d'égale que le nombre de consultations menées ces dernières années, en écho avec l'irruption d'Internet dans tous les champs humains. Le résultat est mitigé tant l'on perçoit un sentiment de méfiance des parties prenantes, voire de défiance. Différentes phases de consultations se sont déroulées dans le cadre des discussions du Sommet de l'Avenir. À cela s'ajoutent des consultations menées dans le cadre de l'évaluation des lignes d'action du SMSI, par la CSTD, par l'UIT – et notamment le groupe de travail du Conseil sur le SMSI et les objectifs de développement durable – au sein du FGI ou encore par des organisations régionales et nationales.

Identifier les lacunes et trouver les synergies avec ces nouveaux engagements passent par la mise à profit des succès du SMSI et sont les préalables à une coopération numérique renforcée, entre multipartisme et multilatéralisme. La diversité des perspectives répond à la nature même d'Internet, globale et distribuée.

Promouvoir la vision du SMSI d'une société de l'information axée sur les personnes et sur le développement ne peut faire l'économie d'une amélioration de l'approche multipartite et de la diversité des gouvernances qui en découlent. Rappelons les principes de NetMundial, réaffirmés et consolidés en 2024[18] par la déclaration multipartite NETmundial+10[19] qui vise justement un renforcement des processus de gouvernance de l'Internet et de politique numérique en favorisant l'implication des parties prenantes et une prise de décision ouverte.

En effet, cette approche multipartite est à nouveau mise à l'épreuve, interrogeant les modalités de participation des parties prenantes : image d'Épinal ou cheval de bataille ? L'examen à 20 ans du SMSI aura la valeur d'un test de cet héritage des débuts d'Internet.

Encourager la participation effective des parties prenantes n'est pas chose aisée. Cela peut consister en la mise en place de mécanismes spécifiques et transparents ainsi qu'en la prise en compte des acteurs les moins audibles.

[18] Voir le "Final Report NETmundial+10", publié en avril 2024, qui comprend une description détaillée du processus et de la méthodologie utilisée.

[19] NETmundial+10 Multistakeholder Statement, 30 avril 2024.

Entre ouverture et fragmentation : les deux visages de la « souveraineté numérique européenne »

Par Clément PERARNAUD
Brussels School of Governance (BSoG-VUB, Belgique)

La problématique de la « fragmentation d'internet » s'est récemment structurée comme problème public, aussi bien au sein de l'ONU que de l'UE, en parallèle de l'affirmation des discours et initiatives étatiques autour de la « souveraineté numérique ». Ces deux tendances sont régulièrement mises en relation, comme en témoigne le cas européen.

En tentant de s'extraire des dépendances et régimes de subordination qui caractérisent la situation européenne sur le plan numérique, les nouvelles politiques de l'UE en matière de souveraineté numérique interrogent la vision de l'exécutif européen concernant internet, et notamment sur le plan de son unité et de son ouverture.

Reprenant les conclusions d'un ouvrage récent, intitulé *L'avenir d'Internet : unité ou fragmentation ?*, et co-écrit avec Julien Rossi, Francesca Musiani et Lucien Castex[1], cet article interroge les tensions qui caractérisent les discours et initiatives appelant à un internet européen, à la fois ouvert et souverain.

L'accélération conjointe des débats autour de la souveraineté numérique et de la fragmentation d'internet

L'approche de l'Europe par rapport aux technologies numériques a pendant longtemps consisté à laisser une grande marge de manœuvre aux marchés, en s'inspirant de régulations d'outre-Atlantique.

Mais depuis le début des années 2010, l'Europe semble être sortie de sa « timidité numérique » suite aux scandales liés à la surveillance des citoyens européens révélés par le lanceur d'alerte Edward Snowden au début des années 2010. Ce moment fut l'un des principaux moteurs du processus d'adoption du RGPD, approuvé en 2016. Dans ce texte, deux innovations sont à souligner, à savoir un principe d'extra-territorialité de la régulation plus assumé, suivant lequel la loi s'applique aussi aux entreprises extra-européennes qui proposent des services à des citoyens de l'UE et l'introduction d'amendes

[1] Perarnaud Clément, Rossi Julien, Musiani Francesca & Castex Lucien (2024), *L'avenir d'Internet : unité ou fragmentation ?*, Le Bord de l'eau, 146 p.

d'une ampleur inédite. Ces évolutions préfigurent, dans une certaine mesure, l'agenda politique de souveraineté numérique européenne qui s'est accéléré dès 2019, notamment avec l'arrivée d'Ursula von der Leyen à la tête de la Commission européenne.

Cette quête plus affirmée de « souveraineté numérique » s'est en effet traduite par l'adoption de nombreuses autres règles contraignantes, comme la nouvelle directive sur le droit d'auteur en 2019, le règlement sur les services numériques qui encadre notamment la modération des contenus sur les plateformes (le *Digital Services Act*, ou DSA), le règlement sur les marchés numériques (le *Digital Markets Act*, ou DMA), tous deux en 2022, ou encore la loi sur l'intelligence artificielle de 2024, pour ne citer que quelques exemples d'une longue liste. Ces développements ont considérablement renforcé la réglementation applicable aux acteurs de l'économie numérique. C'est d'ailleurs au moment de l'adoption du DSA et du DMA que le groupe Meta, propriétaire entre autres de Facebook, Instagram et WhatsApp, avait menacé de quitter le marché européen. Cette menace n'a pas été suivie d'effets, mais elle souligne déjà comment de telles politiques, et les réactions qu'elles suscitent de la part d'entreprises privées, participent directement à entretenir des pressions pesant sur l'unité d'internet.

À cet égard, la question de la fragmentation d'internet doit d'abord être pensée comme un discours. La construction du sens passe tant par des normes langagières que par des stratégies d'influences et institutionnelles spécifiques. La problématique de la fragmentation d'internet s'invitant ainsi régulièrement dans le débat public, que cela soit en réponse à des interventions législatives récentes, comme lors de l'adoption du RGPD au niveau de l'Union européenne, ou pour le grand public, à travers la multiplication d'articles et de déclarations publiques.

La fragmentation comme arme rhétorique dans les débats politiques européens

Au sein de l'UE, le spectre de la fragmentation a été mobilisé régulièrement lors de l'émergence de nouvelles normes juridiques, susceptibles d'interférer avec la vision d'un internet perçu comme universel et unifié. C'est à ce titre que certains grands groupes technologiques étasuniens, à l'image de Google, se positionnent régulièrement comme des défenseurs de l'unité d'internet, face à ces logiques réputées « fragmentaires ». Comme nombre d'acteurs internationaux, ces entreprises souhaiteraient éviter un morcellement des règles nationales et régionales visant internet et les marchés numériques dans lesquels ils s'inscrivent. Dans ce cadre, la notion de fragmentation est ainsi un outil rhétorique pour dénoncer un horizon politique dans lequel la nature globale des plateformes ou la fluidité de l'accès à l'information et du partage de données serait en danger.

Ce débat a été justement au cœur des négociations européennes controversées du RGPD, notamment au sujet du droit à l'oubli. Ce droit à l'oubli est consacré par la Cour de Justice de l'Union européenne (CJUE) dans un arrêt Google Spain en 2014 sous la forme d'un droit au déréférencement. Il donna lieu à de vifs débats sur son application géographique et l'impact qui en découlait en termes de fragmentation de l'internet global. Lors des discussions sur le RGPD, qui a codifié le fonctionnement du mécanisme de droit à l'oubli, la législation européenne avait été accusée de contribuer à la fragmentation d'internet. Plusieurs voix s'étaient élevées pour avertir que ce règlement allait « inévitablement conduire à la fragmentation ». Depuis, plusieurs sites *web*, notamment aux États-Unis, ont rendu leurs pages indisponibles aux visiteurs se connectant avec une adresse IP européenne. Ces entreprises présentent ce choix comme un moyen d'éviter de tomber dans le champ d'application extraterritorial de la loi européenne sur la protection des données. Cependant, il faut rappeler ici que ni le déréférencement d'un site *web*, ni le blocage d'accès aux adresses IP de l'UE ne créent de fragmentation au niveau technique pour le

réseau. De plus, l'utilisation de moyens de contournement comme l'utilisation de réseaux privés virtuels (VPN) peut permettre de circonscrire les mesures de blocage géographique qui affecteraient les internautes européens.

Vers un internet européen ouvert et souverain ?

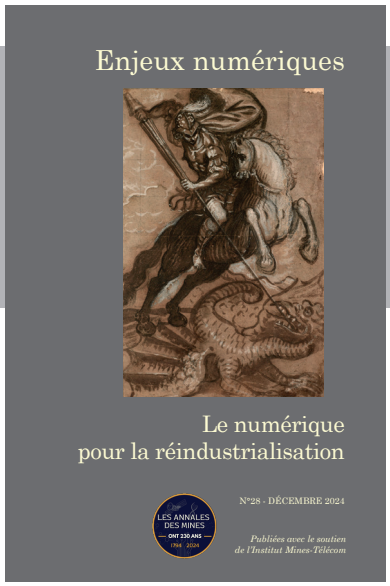
Du point de vue des discours actuels autour de la souveraineté numérique et de la fragmentation d'internet, le cas européen est particulièrement intéressant. L'Europe a bien compris qu'elle souffre de faiblesses structurelles : elle ne dispose ni des grands capitaux ou du dynamisme financier des États-Unis, ni des effets de la « planification technologique verticale » de la Chine. Mais elle semble avoir pris conscience d'une de ses forces : son approche fondée sur les principes et les droits fondamentaux, établie bien avant l'ère du numérique par les traités fondateurs européens. Cette approche est régulièrement présentée comme étant au centre de sa stratégie, et même s'il est trop tôt pour faire des prévisions à moyen et à long terme sur son succès, on peut d'ores et déjà dire que l'Europe tente par ce biais de s'extraire d'une situation de subordination géopolitique/numérique de plus en plus problématique.

Le modèle proposé par cet ensemble de régulations se veut basé sur les droits des individus (vie privée, liberté d'expression…), sur un certain nombre de valeurs sociotechniques (interopérabilité, portabilité…), et sur l'équilibre d'intérêts hétérogènes. On peut s'interroger pour savoir si l'action de l'Europe est, à certains égards, en train de promouvoir la fragmentation du réseau : en introduisant un certain nombre de lois et de règles qui ne s'appliquent qu'aux utilisateurs européens, l'Europe est en train de faire en sorte que l'internet européen se peuple de services et de contenus répondant précisément à ces nouvelles exigences.

Force est de constater que le principe d'un internet ouvert et global peut parfois entrer en contradiction avec d'autres principes fondamentaux, tels que le droit à la vie privée, le droit à la sécurité, ou les droits de propriété intellectuelle. Car lorsque l'UE – ou d'autres États démocratiques – impose de nouvelles règles aux acteurs de l'internet en vue de protéger ces droits, cela a pour effet d'affecter inévitablement la disponibilité de certaines informations à l'échelle régionale sur internet, et ce même si l'approche européenne semble de plus en plus extraterritoriale dans son champ d'application.

Au nom de la lutte contre les contenus illicites (de toute sorte : apologie du terrorisme, discours de haine, arnaques en ligne…), des États européens démocratiques mettent en place des mesures juridiques et techniques qui font souvent écho à celles d'autres États dont l'objectif assumé est de mieux contrôler, voire « policer », leurs infrastructures et les contenus numériques accessibles sur leur territoire, comme illustré par le cas chinois. Cela ne veut pas dire que l'objectif soit le même ; mais le moyen technique d'y arriver y ressemble.

Mais comme nous le savons, la Toile dépourvue de règles finit souvent, elle aussi, par se diviser et se fragmenter en plusieurs jardins clos, à l'avantage d'acteurs privés. L'action de l'Europe semble donc faire un pari : qu'une certaine fragmentation du réseau – concernant notamment la localisation des données, ou la protection de la vie privée – peut tourner à l'avantage des citoyens, si elle est gérée par une démocratie ou un ensemble de démocraties.



ENJEUX NUMÉRIQUES

Le numérique pour la réindustrialisation

N°28 - Décembre 2024

Ce numéro a été coordonné par
Léo QUENTIN et Anne-Lise THOUROUDE

Ce numéro peut être consulté et téléchargé gratuitement
sur notre site ***http://www.annales-des-mines.org***

Le Droit de la Compliance, voie royale pour réguler l'espace numérique

Par Marie-Anne FRISON-ROCHE
Professeure de Droit de la Régulation
et de Droit de la Compliance
Directrice du *Journal of Regulation & Compliance* (JoRC)
Directrice de l'École européenne de Droit
de la Régulation et de la Compliance

Pour décrire la place du Droit de la Compliance afin de réguler l'espace numérique et pour en conclure que cette nouvelle branche du Droit constitue la « voie royale » pour cela, l'étude procède en six étapes.

Premièrement, à première vue et conceptuellement il existe un fossé entre l'idée politique de Régulation et les idées (liberté et la technologie comme « loi ») sur lesquelles l'espace numérique s'est construit et se déploie.

Deuxièmement, en pratique, un fossé aussi immense existe entre les modes ordinaires du Droit de la Régulation, qui s'adosse à un État et l'organisation de l'espace numérique tenue par ces opérateurs économiques à la fois américains et globaux.

Troisièmement, la prétention, de nature politique, de civiliser l'espace numérique demeure pourtant et s'accroît, se concrétisant en s'appuyant sur la force même des entités en mesure de concrétiser cette ambition, ces entités étant les opérateurs numériques cruciaux eux-mêmes, saisis en *ex ante*.

Quatrièmement, cela correspond à la conception et pratique d'une nouvelle branche du Droit, le Droit de la compliance, qui ne doit pas se confondre avec la « conformité » et qui est normativement ancré dans ses « Buts Monumentaux ».

Cinquièmement, ce Droit opère une internalisation des buts monumentaux dans ces opérateurs numériques qui les diffusent en structures et en comportements dans l'espace numérique.

Sixièmement, s'articulent alors, par un intermaillage entre les législations, les décisions de justice et les comportements des entreprises, des concrétisations de gré ou de force des Buts Monumentaux qui peuvent civiliser l'espace numérique sans que la liberté y perde son primat.

Cet article a été aussi élaboré en anglais sous la forme d'un working paper, *doté de développements supplémentaires, de références techniques et de liens hypertextes, disponible à l'adresse suivante : https://mafr.fr/en/article/compliance-law-as-a-path-for-regulating-the-digita/*

Pour montrer que la régulation de l'espace numérique prend le chemin du Droit de la Compliance, cette étude pose six jalons. Le premier montre le fossé conceptuel entre l'idée de régulation et les deux idées sur lesquelles l'espace numérique s'est construit. Le deuxième aborde le fossé pratique entre les outils ordinaires de la régulation et le fonctionnement de l'espace numérique. Le troisième expose la prétention politique de civiliser l'espace numérique en s'appuyant sur la force des entreprises en position d'y contribuer. Le quatrième expose ce qu'est le Droit de la Compliance, nouvelle branche du Droit ancré dans ses « Buts Monumentaux ». Le cinquième explique l'internalisation dans les opérateurs économiques cruciaux de l'espace numérique des Buts Monumentaux de la Régulation de l'espace numérique. Enfin, le sixième démontre que Régulation et Compliance sont des techniques issues des activités, et desquelles se déduisent des Buts Monumentaux localisés à prétention globale. La conclusion en est que le Droit de la Compliance est la voie royale pour réguler l'espace numérique.

À PREMIÈRE VUE ET CONCEPTUELLEMENT : UN FOSSÉ ENTRE L'IDÉE DE RÉGULATION ET LES 2 IDÉES SUR LESQUELLES L'ESPACE NUMÉRIQUE S'EST CONSTRUIT ET SE DÉPLOIE

Au sens littéral, la « Régulation » consiste à poser des règles. Ces règles sont édictées avant que des comportements soient adoptés par des personnes. C'est pourquoi les personnes doivent respecter ces règles, posées en *ex ante*, soit que ces règles interdisent des comportements – un comportement contraire constituant alors une violation, qui sera sanctionnée –, soit que ces règles prescrivent un comportement – auquel cas la violation sera constituée par l'inaction et la personne alors contrainte à l'action. Ce schéma vaut que la règle soit juridique, technique, sociale, biologique, climatique, etc.

Celui qui fixe la règle a un immense pouvoir, puisque les comportements de toutes les autres personnes ne se déploient positivement (autorisation de comportement) ou négativement (interdiction de comportement) qu'au regard de ces règles. Le plus souvent, les humains ne disposent pas de la fixation des règles (physiques, climatiques, mathématiques, etc.).

Mais certains disposent du pouvoir d'édicter en *ex ante* des règles juridiques, soit générales par des lois et réglementations, soit particulières par des contrats et des jugements. Dans des systèmes juridiques construits sur le principe constitutionnel de la liberté des personnes, ce pouvoir d'interdire des comportements est une exception, afin que la liberté demeure le principe : le Droit pénal, qui interdit, a toujours statut constitutionnel d'exception, y compris dans l'appréhension des délits commis dans l'espace numérique[1].

Les tensions conceptuelles se sont accrues parce que l'espace numérique a été construit d'une part sur le principe de liberté et d'autre part sur la technologie. Au premier titre

[1] Cette conception de la Règle et des mœurs (que l'on peut retrouver par exemple chez Kant – *Métaphysique des mœurs*, 1797), continue de régir le Droit occidental sans qu'il faille exacerber la distinction que l'on fait souvent en exagérant la primauté entre les systèmes dits de *civil law* et les systèmes dits de *common law*, car tous les systèmes juridiques européens et américains sont construits sur l'idée de la personne, sujet de droit, qui agit librement en utilisant l'autonomie de sa volonté dans le cadre des lois et réglementations, tandis que cette conception n'est partagée ni en Asie ni en Afrique. Cela aura une grande importance, par exemple, dans le Droit des données à caractère personnel.

et comme on le sait, une conception libertaire a animé les premiers constructeurs de cet espace, conception qui resurgit aujourd'hui d'une façon amplifiée. Sur cette base conceptuelle, il est demandé une « dérégulation », la Régulation étant désignée comme illégitime par principe, voire contraire à la Constitution. Au second titre, il est soutenu que les règles qui régissent l'espace numérique ne seraient pas de nature juridique mais de nature technique. En effet, selon la formule désormais célèbre du Professeur de Droit Lawrence Lessig, "*Code is Law*"[2] : ce serait le codage informatique qui, dans ce nouvel espace enfin libéré des lois physiques du vieux monde, en constitue les lois constitutives, les lois nécessaires et suffisantes. Dès lors, toute règle, notamment juridique, serait une méconnaissance de cet espace, entravant son développement.

Il ne faut jamais sous-estimer l'importance de cette bataille conceptuelle, les idées menant le monde.

À première vue et en pratique : un fossé entre les modes ordinaires du Droit de la Régulation et l'organisation de l'espace numérique

Cet affrontement de représentations du monde, dans ce qu'il doit être à l'avenir, oppose deux ordres qui traditionnellement sont hiérarchisés : le monde des législateurs, régulateurs et juges d'une part et le monde des entreprises numériques et des internautes d'autre part. Classiquement, les premiers ordonnent et les seconds, assujettis, obéissent. Si les premiers pensent que la liberté, notamment la liberté d'expression, doit trouver ses limites, ils l'imposent par des lois et des jugements, et les assujettis (de mauvaise grâce) obtempèrent.

Mais nous savons qu'en pratique et dès le départ il n'en a pas été ainsi. Pour deux raisons. En premier lieu, l'espace numérique est global et les auteurs des normes juridiques sont cernés par des territoires. C'est surtout vrai pour les auteurs des règles juridiques générales, notamment le Législateur, les États se définissant par leur rapport au territoire national, la frontière qui signe leur faiblesse, incapables de régir un territoire global et immatériel.

En second lieu et en pratique, le Droit de la Régulation est une branche du Droit récente[3], qui se reconnaît le plus souvent par l'existence d'une « autorité de régulation » et qui se caractérise par un appareillage de réglementations, de décisions, de principes et de raisonnements, permettant de bâtir pour un secteur qui le requiert un équilibre entre le principe de concurrence et un autre principe, et de maintenir cet équilibre dans la durée. Il faut supposer que ce secteur n'a pas les forces suffisantes pour produire lui-même cet équilibre entre la concurrence et un autre principe (a-concurrentiel, voire anticoncurrentiel). La Régulation vient donc pallier cette « défaillance de marché ».

Mais l'espace numérique n'est pas un secteur. Convergent en son sein de multiples régulations, depuis toujours[4]. Il en ressort des contentieux d'une grande complexité car chacun

[2] L. Lessig (2000), "Code Is Law. On liberty in cyberspace", *Harvard Magazine*, 1er janvier 2000.

[3] M.-A. Frison-Roche (2001), « Le droit de la régulation », *Recueil Dalloz, Chronique*, pp. 610-616.

[4] M-A. Frison-Roche (2005), « L'hypothèse de l'interrégulation », *in* M.-A. Frison-Roche (dir.), *Les risques de régulation*, Dalloz et Presses de Sciences-Po, coll. « Droit et Économie de la Régulation », t. 3, 2005, pp. 69-80. Voir aussi M-A. Frison-Roche (dir.) (2016), *Internet, espace d'interrégulation*, Dalloz, coll. « Thèmes & Commentaires », série « Régulations », 2016, 208 p.

est légitime à s'y prononcer, comme le montre notamment la difficulté juridique à imposer le contrôle de l'âge des internautes accédant à des sites dont le contenu est interdit aux mineurs[5].

Face à ces difficultés conceptuelles et pratiques, que faire ?

La prétention politique de civiliser l'espace numérique en s'appuyant sur la force des entreprises en position d'y contribuer

Le Droit est un art pratique dont toute société a besoin pour que les rapports humains ne soient pas livrés à la seule force[6]. Face à des difficultés nouvelles, les systèmes juridiques génèrent des solutions nouvelles. Le Droit est en train de concevoir une nouvelle branche du Droit : le Droit de la Compliance[7].

Plutôt que de penser en termes d'assujettissement de l'un par l'autre (les entreprises par le Politique ; les réglementateurs par les entreprises innovantes), il faut penser en termes de « prétentions ».

Le Politique est légitime à exprimer une volonté pour élaborer ce qui lui paraît juste pour l'avenir du groupe social qu'il représente. En cela, il construit une « politique ». L'Europe, notamment pour des raisons historiques en ce qu'elle porte la marque de ce que produisit dans l'Allemagne nazie la constitution de fichiers, souvenirs que ne portent pas les États-Unis[8] et qui expliquent en grande partie l'opposition juridique sur la question des transferts de données personnelles entre les deux continents, a posé par sa jurisprudence et ses régulations successives que les systèmes numériques et algorithmiques ne doivent pas broyer les êtres humains qui y sont ou y seront de gré ou de force impliqués.

Pour cela, le Politique ne pouvant pas réguler directement l'espace car l'espace sur lequel il a emprise est trop étroit, il n'a pas les moyens informationnels, financiers et humains pour cela, va s'appuyer directement sur les entreprises qui ont construit et qui font fonctionner l'espace numérique. L'internalisation de ces buts fait naître cette nouvelle branche du Droit qu'est le Droit de la Compliance[9].

---

[5] M.-A. Frison-Roche (dir.) (2025), *Contentieux Systémique Émergent*, LGDJ, coll. « Droit & Économie », à paraître, 2025.

[6] *Ubi societas, ubi jus.*

[7] M.-A. Frison-Roche (2016), « Le Droit de la compliance », *Recueil Dalloz, Chronique*, 2016, pp. 1871-1874 ; *L'apport du Droit de la Compliance à la Gouvernance d'Internet*, rapport demandé par le Gouvernement, remis en avril 2019, publié le 15 juillet 2019, 139 p. ; « Naissances d'une branche du droit : le Droit de la Compliance », *in Mélanges offerts à Louis Vogel. La vie du droit*, LexisNexis - Dalloz - LawLex - LGDJ, 2024, pp. 177-188.

[8] M.-A. Frison-Roche (2018), « Compliance : avant, maintenant, après », *in* N. Borga, J. -Cl. Marin et J.-Ch. Roda (dir.), *Compliance : l'entreprise, le régulateur et le juge*, Dalloz, coll. « Thèmes & Commentaires », série « Régulations & Compliance », 2018, pp. 23-36.

[9] M.-A. Frison-Roche (2017), « Du Droit de la régulation au Droit de la compliance », *in* M.-A. Frison-Roche (dir.), *Régulation, Supervision, Compliance*, Dalloz, coll. « Thèmes & Commentaires », série « Régulations », 2017, pp. 1-14.

Parce que nouveau, le Droit de la Compliance est encore très mal connu et ses immenses capacités pratiques assez peu explorées, sans doute parce qu'il est enseveli sous la « masse réglementaire » avec laquelle il est confondu.

Le Droit de la Compliance, nouvelle branche du Droit ancrée dans ses « Buts monumentaux »

Cette nouvelle branche du Droit est souvent difficilement perçue, car on la confond avec la « conformité »[10] à la masse réglementaire à laquelle les entreprises sont assujetties. Il est en effet parfois affirmé que la « Compliance » ne serait que le terme anglais pour désigner la « conformité » qui serait, à travers le « Droit de la Conformité », l'obligation pour l'entreprise de se conformer à toutes les réglementations qui lui sont applicables et de donner à voir cette « conformité ». Dès lors et par exemple, les entreprises assujetties devraient non plus agir en toute liberté puis répondre en *ex post* de violations prouvées par ceux qui leur demandent des comptes devant une Autorité ou un juge[11], mais devraient donner à voir à tout moment, en tous lieux et à travers chaque personne dont elles devraient répondre, le respect de l'ensemble de la réglementation qui leur est applicable[12].

Les entreprises, notamment celles qui ont des activités dans l'espace numérique, rejettent conceptuellement cette définition, car le principe de liberté n'est plus premier, et pratiquement il est impossible qu'un sujet de Droit soit en conformité avec toutes les réglementations qui lui sont applicables[13], ne serait-ce que parce qu'il ne les connaît pas et que le sens de celles-ci évolue.

Mais le Droit de la Compliance ne s'est jamais réduit à la conformité, et c'est aussi cette confusion menant à une définition de la Compliance obligeant à une obligation injustifiée et impossible à satisfaire qui, par un mouvement de balancier, a entraîné l'outrance inverse, à savoir le désir de jeter par-dessus bord toute règle, à travers le mouvement dit de « dérégulation », hostile à toute « réglementation » : un excès produit l'excès inverse. Mais le Droit de la Compliance n'est pas le « droit de la conformité ».

Le Droit de la Compliance, terminologie qu'il faut conserver dans la langue française, s'ancre normativement dans des « Buts Monumentaux »[14] à la concrétisation desquels les

[10] M.-A. Frison-Roche (2024), « Compliance et conformité : les distinguer pour les articuler », *Recueil Dalloz, Chronique*, 2024, pp. 497-499.

[11] Ce qui est le socle des États de Droit occidentaux, comme il a été expliqué plus haut.

[12] Par exemple à travers chaque personne appartenant à leur chaîne de valeur, ou à travers chaque internaute qui s'exprime sur une plateforme, alors même que le Droit de l'Union a repris le principe dit « d'irresponsabilité ». Pour l'analyse de cette situation particulière au regard de la responsabilité civile, voir M.-A. Frison-Roche, « Compliance, Vigilance et Responsabilité civile : mettre en ordre et raison garder », *in* M.-A. Frison-Roche (dir.) (2025), *L'Obligation de Compliance*, Journal of Regulation & Compliance (JoRC) et Dalloz, coll. « Régulations & Compliance », 2025.

[13] Ce que promettent pourtant les prestataires technologiques à travers la *compliance by design*… (dont la responsabilité a vocation à être engagée à ce titre). Voir sur cette question, M.-A. Frison-Roche, « Le juge requis pour une obligation de compliance effective », *in* M.-A. Frison-Roche (dir.) (2025), *L'Obligation de Compliance, ibid.*

[14] M.-A. Frison-Roche (dir.) (2022), *Les Buts Monumentaux de la Compliance*, Journal of Regulation & Compliance (JoRC) et Dalloz, coll. « Régulations & Compliance », 2022, 520 p.

entreprises en position d'y contribuer sont sollicitées. Ces Buts Monumentaux systémiques sont tout d'abord de « nature négative », car il s'agit que les systèmes ne s'effondrent pas, qu'il s'agisse du système bancaire, financier, énergétique, climatique, etc. ou numérique. Ces Buts Monumentaux peuvent être aussi de « nature positive », c'est-à-dire qu'il s'agit non seulement d'assurer la durabilité des systèmes[15] mais encore de les améliorer pour qu'ils soient des espaces plus solides et qui profitent davantage aux personnes présentes et futures qui y vivent.

Les entreprises ne sont pas légitimes à fixer les Buts Monumentaux à la place des Autorités politiques et publiques, et l'espace numérique ne relève pas de l'autorégulation quand bien même une entreprise ou un groupe d'entreprises ou toutes seraient animées de la volonté de se soucier d'autrui. L'éthique des affaires, la prise en charge spontanée d'un autrui lointain, dans l'espace ou dans le temps, démarche qui correspond à la « responsabilité sociétale » ne peut pas remplacer des choix politiques opérés par des gouvernants politiquement désignés. Mais d'une part les entreprises sont libres d'organiser les moyens par lesquels elles participent à concrétiser ces buts[16]. D'autre part, elles peuvent adhérer à ces buts, par exemple les reproduire dans leurs « Outils de Compliance »[17], voire aller au-delà de ceux-ci si elles ne les contredisent pas, mais pas davantage car elles ne peuvent pas devenir les nouveaux « constituants » du monde et le régenter.

L'internalisation dans les opérateurs économiques cruciaux de l'espace numérique des Buts Monumentaux de la Régulation de l'espace numérique

Les Autorités publiques vont alors par des législations, réglementations ou diverses lignes directrices qui constituent un « intermaillage » de Droit dur et de Droit souple que les opérateurs économiques reçoivent avec attention et suivent[18], internaliser cette régulation directement dans les opérateurs cruciaux, c'est-à-dire ceux qui tiennent l'espace numérique, opérateurs dont la liste est dressée et dont les critères sont élaborés. Une fois ce cercle de sujets de Droit ainsi chargés de mettre en œuvre des structures de Compliance, par exemple la surveillance des contenus, en raison même de leur position de puissance dans l'espace (*gatekeepers*), les obligations de Compliance sont édictées.

[15] La durabilité est une notion clé du Droit de la Compliance, notion qui n'est pas limitée aux enjeux climatiques mais prend plutôt naissance dans le secteur bancaire.

[16] Pour une description complète et détaillée de toutes les obligations de compliance, notamment celles qui concernent les acteurs du numérique, voir M.-A. Frison-Roche, « Obligation de Compliance : construire une structure de compliance produisant des effets crédibles au regard des Buts Monumentaux visés par le Législateur », *in* M.-A. Frison-Roche (dir.) (2025), *L'Obligation de Compliance*, *op. cit.*

[17] M.-A. Frison-Roche (dir.) (2021), *Les outils de la Compliance*, Journal of Regulation & Compliance (JoRC) et Dalloz, coll. « Régulations & Compliance », 2021, 323 p.

[18] Sur la puissance de cet intermaillage mondial et les raisons de cette puissance, voir M.-A. Frison-Roche, *L'apport du Droit de la compliance à la gouvernance d'Internet*, rapport au Gouvernement, préc.

Les obligations de Compliance sont de deux types et peuvent avoir de ce fait deux portées différentes[19]. Il peut s'agir de la mise en place de « structures de Compliance » par lesquelles les opérateurs puissants sont requis d'accroître leur puissance pour permettre au système d'être en mesure d'atteindre les buts. Par exemple, des structures de réception d'alerte, des structures de détection de messages anormaux, etc. doivent être mises en place. Il s'agit alors d'obligations de résultat, c'est-à-dire que celui qui agit en manquement ou en responsabilité contre l'opérateur pourra obtenir sa condamnation en montrant simplement la non-obtention du résultat comme fait constitutif du manquement ou générateur de la responsabilité. Mais il peut s'agir aussi de l'obtention de « comportements de Compliance », par exemple d'obtenir que l'espace numérique soit un espace civilisé où le respect d'autrui soit la norme de comportement, que les personnes qui s'y expriment ne se dissimulent pas, etc. Il s'agit alors d'une obligation de moyens, c'est-à-dire que celui qui agit contre l'opérateur en manquement ou en responsabilité devra démontrer l'existence d'un fait générateur distinct, à savoir une faute ou une négligence.

Le prolongement du Droit de la Régulation en Droit de la Compliance résout en grande partie ce qui a semblé l'aporie du territoire[20], puis le scandale de « l'extraterritorialité ». En effet, en internalisant dans un opérateur numérique, qui, lui n'est pas dans son activité limité à un territoire, l'obligation de prendre en considération des buts à la réalisation desquels il doit contribuer, par exemple lorsque l'Arcom requiert de Meta ou de Google un meilleur contrôle des contenus, la régulation bénéficie de la puissance même de son assujetti et la Compliance dépasse ainsi la Régulation, qu'elle transforme au-delà d'un simple prolongement[21]. Notamment dans cet espace global et a-territorial qu'est le numérique.

Les Autorités de Régulation deviennent ainsi des Autorités de Supervision[22]. Le modèle de référence en est le secteur bancaire, qui, comme le numérique, a été construit par les banques elles-mêmes qui continuent en grande partie à le gouverner et à en inventer les produits, leurs fonds propres et quasi-propres assurant la solidité du système lui-même, adossé à des normes prudentielles communes aux opérateurs bancaires qui fonctionnent ensemble (ce que le Droit de la concurrence désignerait comme une « entente »). Comme le font les Banques Centrales, les Autorités de Régulation sont aussi des Autorités de Supervision : pour assurer la durabilité du secteur ou de l'espace, l'Autorité publique a le pouvoir permanent de contrôler l'opérateur crucial. C'est l'inverse du modèle du marché concurrentiel qui repose sur l'atomicité des opérateurs en lutte les uns contre les autres, la disparition d'un acteur, voire d'un marché, donnant lieu à l'apparition d'un nouvel acteur ou d'un nouveau marché. Comme pour un secteur régulé, l'on s'accordera pour dire que la disparition de l'espace digital étant exclue (But Monumental Négatif du Droit de la Compliance numérique[23]), la concurrence n'y joue pas le même rôle (*cf*. le *Digital Services Act* européen) et la Régulation devient Supervision par le mécanisme de Compliance.

[19] Pour une description plus précise et les références de droit positif, voir M.-A. Frison-Roche, « Obligation de Compliance : construire une structure de compliance produisant des effets crédibles au regard des Buts Monumentaux visés par le Législateur », préc.

[20] L'aporie du territoire qui à première vue est pourtant difficile à dépasser ; voir sur ce point les développements précédents.

[21] M.-A. Frison-Roche (2018), « Le Droit de la Compliance au-delà du Droit de la Régulation », *Recueil Dalloz, Chronique*, 2018, pp. 1561-1563.

[22] M.-A. Frison-Roche (dir.), Régulation, Supervision, Compliance, *op. cit*.

[23] Sur la notion de « But Monumental négatif », voir les développements précédents.

Ce prolongement de la Régulation en Compliance transforme aussi profondément l'office du juge[24]. L'on a pu croire que les Outils de Compliance, notamment les algorithmes organisant des conformités automatiques par *compliance by design* allaient éliminer le juge, puisque celui-ci est un personnage de l'*ex post*. L'on assiste au contraire à une « Juridictionnalisation de la Compliance »[25]. La puissance de la Compliance démultipliant celle de la Régulation, même si la Compliance conduit aussi à contractualiser les rapports avec les Autorités, les grands cas litigieux vont apparaître. Ils relèvent du « Contentieux systémique »[26]. En effet, comme on peut le voir par exemple dans le cas *Epic Games v. Apple*, c'est le système lui-même qui est devant le juge et dont les intérêts propres doivent aussi être pris en considération par celui-ci. Cela est logique, puisque le système étant internalisé à travers les textes de Régulation devenant des textes de Compliance, les contentieux entre les parties deviennent eux-aussi systémiques. Les procédures vont devenir globales.

Articulation entre d'une part Régulation et Compliance techniques et globales issues des activités et d'autre part Régulation et Compliance déduites de Buts Monumentaux localisés à prétention globale

L'espace numérique requiert ainsi des systèmes juridiques qu'ils s'adaptent sans cesse, dans une transformation en profondeur, puisque le Droit doit ici être pensé sans un rapport direct au territoire. Cela n'était pas opéré par le Droit de la Régulation, mais c'est ce que parvient à atteindre le Droit de la Compliance, faisant de celui-ci le Droit de demain.

Cette mise à distance des territoires pose la question d'un possible « Droit global », dont le Droit du numérique pourrait être l'épigone, succédant ainsi au Droit financier, auquel il ressemble sur beaucoup d'aspects, notamment la domination des entreprises américaines.

Cela dépend de la place des Buts Monumentaux qui sera laissée dans la pratique et la conception des obligations de Compliance que les « masses réglementaires » accumulent, et dans les décisions de justice qui vont venir, notamment les décisions de la Cour de justice de l'Union européenne d'une part et de la Cour suprême des États-Unis d'autre part.

Cela est à croiser avec la montée en puissance des « souverainetés numériques », qui ne sont plus nécessairement liées à un État, mais plutôt à un projet, y compris à un projet industriel. C'est vrai aussi bien pour l'Europe, pour la Chine (qui a un plan souverain numérique) que pour la Californie (projet souverain étatique qui affaiblit une volonté fédérale portée par un chef dont le projet est incertain).

[24] Conseil d'État et Cour de cassation, *De la régulation à la compliance : quel rôle pour le juge ?* Regards croisés du Conseil d'État et de la Cour de cassation, La Documentation française, coll. « Droits et Débats », 2024, 241 p.

[25] Sur ce mouvement, voir d'une façon générale, M.-A. Frison-Roche (dir.), La juridictionnalisation de la Compliance, Journal of Regulation & Compliance (JoRC) et Dalloz, coll. « Régulations & Compliance », 2023, 490 p.

[26] M.-A. Frison-Roche (dir.) (2025), *Contentieux Systémique Émergent, op. cit*.

Comme dans toutes Régulations, les obligations de Compliance des entreprises peuvent venir des contraintes et ambitions techniques elles-mêmes, par exemple en matière de cybersécurité. Elles sont alors d'une part naturellement mondiales et peuvent être laissées en très grande partie à des entreprises, supervisées par des Autorités publiques. Les Régulations peuvent aussi venir d'ambitions politiques propres, comme la promotion des femmes dans la *tech* ou la protection des enfants, ce qui n'implique pas le même partage, et donc ne justifie pas les mêmes contraintes. Le juge de la Compliance dressera cette cartographie en n'oubliant pas, s'il est occidental, que dans l'État de Droit le premier principe est celui de la liberté.

Régulation économique et « magistère d'influence »

Par Xavier MERLIN
Membre du collège de l'Autorité de régulation des Communications électroniques, des Postes et de la Distribution de la presse (Arcep)

Depuis la création de l'Arcep lors de l'ouverture à la concurrence du secteur des télécoms il y a 30 ans, le champ d'intervention du régulateur sectoriel s'est progressivement étendu au numérique. Au-delà de la régulation technico-économique, au cœur de son action, d'autres compétences en matière de couverture numérique du territoire, ou plus récemment d'évaluation de la soutenabilité du numérique, lui ont également été attribuées, notamment en tant qu'expert neutre du secteur.

À côté des outils traditionnels dont il dispose (pouvoir d'édiction de règles, pouvoir de sanction), le régulateur a été amené à recourir à d'autres formes d'action comme la régulation par la donnée, visant à réduire l'asymétrie d'information, ou la définition de bonnes pratiques, dont le but est d'orienter le comportement. La mesure de l'impact environnemental du numérique et le référentiel général d'écoconception des services numériques constituent deux exemples de ce « magistère d'influence » de l'Arcep.

À l'image d'autres secteurs, la régulation des « télécom » a vu le jour lors de l'ouverture de ce marché à la concurrence. Dans le contexte de la libéralisation décidée au niveau européen en 1996, il a été jugé pertinent de prévoir une intervention publique consistant à l'origine à corriger les défaillances de ce marché pour en accompagner la mue concurrentielle. Confiée à l'ART[1] nouvellement créée, cette régulation est venue compléter en amont le contrôle dit *ex post* assuré par le Conseil (puis l'Autorité) de la concurrence des éventuelles infractions à ce droit. Elle a notamment consisté à stimuler l'émergence d'acteurs alternatifs à l'opérateur historique France Telecom, en leur facilitant un accès non discriminatoire au réseau cuivre de ce dernier.

Près de 30 ans après, les objectifs assignés à l'Arcep[2] (qui a succédé à l'ART en 2005) se sont étoffés au fil des évolutions du cadre juridique[3]. La régulation des communications électroniques vise maintenant à assurer le dynamisme du secteur, en apportant la prévisibilité nécessaire aux acteurs économiques pour qu'ils innovent et investissent dans des infrastructures résilientes et durables, au bénéfice des consommateurs qui doivent pouvoir accéder à des services de qualité à des prix raisonnables, en tout point du territoire.

[1] Autorité de régulation des télécom.

[2] Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

[3] *Cf.* article L.32-1 du code des postes et communications électroniques.

Parallèlement, le champ de compétences de l'Arcep s'est significativement élargi dans le numérique, au-delà des « télécom », mais son intervention repose toujours sur les mêmes principes pro-concurrentiels (accès, interopérabilité, transparence, en particulier). Dès 2015, le régulateur a été chargé de faire respecter le règlement européen sur l'Internet ouvert, qui garantit au consommateur l'accès au contenu de son choix. Depuis la mise en œuvre du *Digital Market Act* en 2024, l'Arcep contribue[4] à assurer l'interopérabilité des grandes messageries instantanées. Dans le cadre du *Data Act*[5], elle œuvre depuis un an au dynamisme concurrentiel du marché du *cloud*. Enfin, le régulateur participe également à l'émergence d'un marché de la donnée numérique au travers des dispositions du *Data Governance Act* européen relatives aux intermédiaires de données.

Au sein de ce périmètre élargi, le régulateur dispose d'une « boîte à outils » diversifiée pour atteindre les objectifs qui lui sont assignés par le législateur européen ou national. Il a la capacité de définir de manière autonome des règles d'application du cadre réglementaire, par exemple pour fixer des conditions d'accès (principes d'accès transparent et non discriminatoire aux réseaux, règles d'interopérabilité ou de portabilité du *cloud*), ou pour déterminer un encadrement tarifaire (fixation des tarifs du dégroupage de la boucle locale cuivre de l'opérateur historique, définition de plafonds tarifaires pour les frais de « sortie » du *cloud*). En cas de non-respect de ces règles, le régulateur possède *in fine* des pouvoirs de sanction propres.

À côté de cette régulation, que l'on peut qualifier de « traditionnelle » car en vigueur depuis la création du régulateur, d'autres modalités d'intervention se sont développées plus récemment, pour répondre à des besoins spécifiques. Relevant du *soft power*, elles n'en sont pas moins efficaces pour autant.

Fort justement décrites par un rapport sénatorial[6] portant sur les autorités administratives indépendantes comme un « magistère d'influence », elles reposent selon ce document d'une part sur « un pouvoir juridique de savoir », qui permet au régulateur d'obtenir des informations, et d'autre part sur un « pouvoir de faire savoir », qui s'appuie sur ses outils de communication.

Régulation par la donnée et évaluation de l'impact environnemental du numérique

En raison de son positionnement central dans l'écosystème numérique et de ses compétences techniques, l'Arcep dispose de données chiffrées, fournies par les acteurs économiques au terme d'obligations réglementaires, et qu'elle est en mesure d'analyser et de restituer selon un format qu'elle détermine. Le choix de les rendre publiques, appelé « régulation par la donnée », constitue un moyen de réduire les asymétries d'information, et donc d'influer sur les comportements de différents acteurs ainsi « encapacités ». Les consommateurs peuvent s'en saisir pour s'informer (en termes de prix, de qualité de service) en amont de leurs choix. Au vu des données publiées, les acteurs économiques peuvent anticiper les réactions des consommateurs et adapter leur offre. Enfin, les pouvoirs publics ou le parlement peuvent s'appuyer sur ces données pour apprécier l'opportunité d'élaborer des politiques publiques ou des réglementations.

[4] Au sein du BEREC, organe regroupant l'ensemble des régulateurs européens des communications électroniques.

[5] Ainsi que de celle de la loi visant à renforcer l'ordre public dans l'espace numérique (dite SREN), qui introduit des mesures du *Data Act* par anticipation.

[6] Rapport 2005-2006 (Sénat n°404) « Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié ».

Ainsi, en matière de téléphonie mobile, l'Arcep publie depuis 2017 des cartes interactives détaillées de couverture mobile du territoire par les différents opérateurs sur son site monreseaumobile.fr, à partir des simulations de mesure réalisées par les opérateurs et vérifiées par le régulateur. Le site propose aussi depuis 2020 des données complémentaires issues du *crowdfunding*, fournies par des tiers à l'Arcep, particuliers ou acteurs de la mesure, pour enrichir l'information mise à disposition et éclairer les choix des utilisateurs. Au cas d'espèce, cette modalité d'action du régulateur vient compléter les obligations de couverture dont il assure le respect.

La régulation par la donnée peut également s'avérer un moyen d'action approprié lorsqu'elle concerne un domaine qui n'entre pas pleinement dans le champ de compétences du régulateur, ou lorsque celui-ci implique des acteurs multiples qui ne sont pas tous visés par sa régulation traditionnelle. La neutralité du régulateur d'une part, et son expertise du secteur d'autre part, peuvent justifier qu'il recoure à cet outil. Le législateur[7] a ainsi confié à l'Arcep en 2021 une mission nouvelle de mesure de l'impact environnemental du numérique. Cette disposition est apparue dans le contexte de contestations relatives à l'attribution par l'Arcep des fréquences 5G, motivées par des craintes concernant l'impact de cette nouvelle technologie sur l'environnement[8]. Le législateur a souhaité que le régulateur, en tant qu'expert neutre, soit en mesure de produire une analyse factuelle des enjeux environnementaux, à l'époque méconnus, et qui donnent depuis lors lieu à des publications annuelles[9].

Pour être pertinente et donc susceptible d'être effective, la régulation par la donnée suppose deux conditions. D'une part, la fiabilité et l'exhaustivité des données doivent être assurées, ce qui requiert que le régulateur dispose juridiquement d'un pouvoir de collecte auprès des acteurs qui les détiennent. Pour reprendre l'exemple de l'impact environnemental du numérique, le législateur a permis à l'Arcep d'assurer une collecte auprès de tous les acteurs (opérateurs télécoms bien sûr, mais aussi équipementiers de réseaux fixes et mobiles, ou gestionnaires de centres de données, qui ne relevaient initialement pas du périmètre de compétences de l'Arcep). D'autre part, elle doit s'appuyer sur une méthode rigoureuse et cohérente. Celle utilisée par l'Arcep pour évaluer l'impact environnemental a été élaborée en lien étroit avec l'Ademe et traite toutes les étapes du cycle de vie des produits et services numériques (fabrication, utilisation, recyclage), et l'ensemble des impacts (empreinte carbone, électricité, métaux rares, eau).

Sous ces conditions, la régulation par la donnée peut constituer un outil efficace pour lutter contre les informations incomplètes voire fausses, telles que le *greenwashing* en matière environnementale, qui conduit souvent à mettre en avant des données tronquées ou une vision simpliste pouvant orienter vers des choix inappropriés. Dans le cadre des interrogations sur le volet énergétique de l'intelligence artificielle, le régulateur peut ainsi utilement contribuer à alimenter le débat public par ses données objectivées.

[7] Loi du 15 novembre 2021 pour la réduction de l'empreinte environnementale du numérique (loi dite REEN).

[8] En particulier par l'impact de la multiplication des objets connectés.

[9] Le numérique représente ainsi 4,4 % de l'empreinte carbone nationale (étude Ademe et Arcep 2025).

Bonnes pratiques : l'exemple du Référentiel général de l'Écoconception des services numériques (RGESN)

Sans pour autant contraindre les acteurs, le régulateur peut aussi souhaiter dépasser la simple publication de données, en incitant ceux-ci à faire évoluer leur comportement, en suivant une « bonne pratique » particulière, qui découle de ses travaux sur la donnée.

Les mesures publiées par l'Arcep révèlent que les terminaux (téléphones, PC, etc.) concentrent l'essentiel de l'empreinte environnementale du numérique[10], et qu'au cours du cycle de vie, l'étape de fabrication est celle qui y contribue le plus. La pratique d'écoconception[11] des terminaux est donc un moyen efficace pour réduire cet impact, et l'écoconception des services numériques est un puissant levier pour lutter contre l'obsolescence des terminaux résultant de leur utilisation pour ces usages. Seuls les produits (ordinateurs, téléviseurs, téléphones, etc.) font l'objet d'une réglementation au plan européen : est proscrite la mise sur le marché de produits qui n'ont pas été écoconçus conformément au règlement européen. En revanche, aucune disposition contraignante ne concerne à ce jour les services numériques. Dans ce contexte, l'Arcep s'est vu confier par la loi REEN, en lien avec l'Ademe, la mise en place d'un guide de référence pour accompagner les développeurs de services numériques (application, site internet, service vidéo, etc.) dans une démarche visant à intégrer l'enjeu environnemental dès l'origine de la conception de ceux-ci. Publié en 2024, le Référentiel général de l'écoconception des services numériques (RGESN) se décline en une série de fiches détaillées interrogeant chaque étape du processus d'élaboration.

L'intelligence artificielle étant un service numérique, ce référentiel donne en particulier des clefs pour réduire son impact environnemental, en encourageant les concepteurs à prévoir dès l'origine des modalités d'entraînement des algorithmes proportionnées aux besoins essentiels du service, en privilégiant les modèles pré-entraînés, et s'appuyant quand c'est possible sur des bases de données préexistantes, ce qui limite la fréquence de mise à jour des données et donc l'impact énergétique. Il fournit donc un outil concret pour travailler à l'élaboration de systèmes d'IA frugaux et durables.

La mise en œuvre de ces bonnes pratiques est également de nature à améliorer l'expérience utilisateur. En réduisant la complexité des interfaces et en optimisant les parcours utilisateurs, elle favorise des interactions plus intuitives et plus rapides. Par exemple, un site *web* éco-conçu, avec un design épuré, se charge plus vite, même avec une connexion au réseau limitée ou sur un appareil plus ancien. Le référentiel recommande par ailleurs de limiter le défilement infini ou le déclenchement automatique des vidéos. Il préconise de redonner à l'utilisateur le contrôle de ses usages grâce à un bouton « stop » ou à un mode « économie de données » et promeut également la limitation de la captation de données à des fins de profilage publicitaire. Ainsi, au-delà des enjeux environnementaux qui l'ont motivé, le référentiel peut aussi contribuer à traiter la question – non moins prégnante – de l'économie de l'attention, dont l'addiction aux écrans constitue une forme exacerbée.

Par définition, une bonne pratique, comme le référentiel, n'a rien d'obligatoire. Elle repose donc sur le volontariat des opérateurs économiques intéressés et peut s'inscrire dans une démarche de transformation voulue par l'entreprise elle-même, qui peut même en faire

[10] Plus que les réseaux et les centres de données. *Cf.* Enquête annuelle pour un numérique soutenable (Arcep).

[11] Prise en compte de l'impact environnemental dès l'étape d'idéation et de conception.

un critère de différenciation vis-à-vis de ses concurrents. Plus largement, dans le contexte de mise en œuvre par toutes les entreprises des obligations issues de la directive CSRD, le référentiel constitue un outil pour aider les acteurs économiques à mieux comprendre, si ce n'est à repenser, les outils numériques qu'ils utilisent.

Enfin, dans un contexte où l'atteinte de l'Accord de Paris sur le climat constitue un enjeu mondial, l'un des intérêts de cette démarche est qu'elle pourrait permettre de rallier plus facilement aux enjeux environnementaux du numérique d'autres pays, notamment en développement, qui cherchent par ailleurs à atteindre les objectifs de développement définis par les Nations Unies[12]. Ils pourraient en effet trouver dans cette approche non réglementaire une orientation pour utiliser les bienfaits du numérique comme moyen d'assurer leur développement, sans impacter négativement l'environnement. Le référentiel esquisse en quelque sorte la voie d'un compromis possible entre les enjeux de développement économique, numérique et durable.

Conclusion

L'Arcep a défini son ambition pour 2030 comme étant de contribuer à doter le pays d'infrastructures numériques « accessibles à tous, partout et pour longtemps ». Dans cette perspective, la régulation par la donnée et les guides de bonne pratique resteront des outils indispensables à l'Arcep, comme à d'autres régulateurs sectoriels qui y recourent également, pour tracer un chemin souhaitable vers un numérique durable. Complémentaires à la régulation « traditionnelle », ils ont montré leur intérêt pour appréhender, entre autres, des sujets en émergence, notamment ceux à caractère plus sociétal, ou ceux dont les acteurs ne relèvent pas tous de la compétence de l'Arcep. En matière d'évaluation de l'impact environnemental du numérique, la Banque mondiale et l'UIT ont reconnu le travail pionnier du régulateur français, encourageant dans le même temps son appropriation par d'autres régulateurs étrangers.

Pour autant, ces approches ne sont pas exclusives de la régulation classique, qui pourra, le cas échéant, trouver à s'appliquer dans un second temps, par exemple si les résultats atteints sans contrainte ne sont pas jugés suffisants par les pouvoirs publics, et une fois que des cadres juridiques appropriés auront été élaborés, sur la base notamment des données fournies par le régulateur.

[12] https://www.undp.org/fr/sustainable-development-goals

L'Arcom à l'heure du règlement sur les services numériques

Par Martin AJDARI
Président de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom)

Le règlement sur les servies numériques vise à protéger la liberté d'expression, tout en corrigeant les défauts structurels résultant du fonctionnement et des usages des très grandes plateformes en ligne (TGPL) ou des très grands moteurs de recherche (TGMR). Il institue ainsi une régulation dite « systémique » proportionnée, attentive aux libertés, qui se fonde sur une approche par les risques que les plateformes ont l'obligation de déterminer puis d'atténuer.

Désignée coordinateur des services numériques en France, l'Arcom contribue à la mise en œuvre de cette nouvelle forme de régulation. En plus de son rôle historique de régulateur des médias traditionnels, elle assume ainsi pleinement sa nouvelle mission de chef de file de la régulation numérique en France aux côtés de la Commission européenne et en lien étroit avec les autres autorités nationales compétentes en matière de RSN.

Le règlement sur les services numériques (RSN), souvent connu sous son appellation anglaise de *Digital Services Act* (DSA), répond au constat suivant : eu égard aux évolutions technologiques et à la puissance des entreprises opérant les grands services numériques présents dans la vie de tous nos concitoyens (les Facebook, Instagram, Google, YouTube, X, TikTok, Snapchat, mais aussi Booking.com et tant d'autres) une approche nationale ou communautaire isolée pour réguler leur activité ne fonctionne pas. Pour être efficace, les deux échelons doivent être associés, en étendant au niveau communautaire des outils juridiques existants en matière de régulation numérique tout en associant les autorités nationales à leur mise en œuvre.

Le RSN se présente ainsi sous la forme d'un règlement de droit commun dit « horizontal », applicable à tous les types de contenus en ligne, et qui a pour objet de prévenir et répondre aux risques, pour les individus comme pour la société, résultant du fonctionnement et des usages des services les plus populaires, tout en protégeant les libertés fondamentales, la liberté d'expression comme la liberté d'entreprendre.

Pour garantir cet équilibre, le RSN instaure une régulation dite « systémique », dont l'objet, plutôt que de désigner *a priori* ce qu'il convient de réguler, consiste à demander aux plateformes d'évaluer, en transparence et en lien avec la société civile, les risques liés à leurs services et d'y apporter des réponses appropriées et proportionnées. Ces risques sont de nature très diverse et concernent aussi bien les individus (lutte contre la haine en ligne ou les discriminations, l'exposition à des contenus nocifs mais aussi les escroqueries et fraudes), les entreprises (propriété intellectuelle) ou la société dans son ensemble (santé publique, désinformation et intégrité des scrutins électoraux).

Le RSN obéit à deux grands principes issus du droit communautaire. Le premier est celui de l'harmonisation maximale : contrairement aux dispositions de la directive « services de médias audiovisuels » (SMA), les règles du RSN s'appliquent de manière identique à tous les États membres. Le second principe est celui dit du « pays d'origine » qui confie

la compétence de droit commun à l'autorité de l'État membre du siège de la plateforme. Le pays de destination, celui dans lequel le service est utilisé, dispose d'une capacité d'intervention plus limitée qui consiste, pour l'essentiel, à saisir de plaintes l'autorité compétente du pays d'origine ou la Commission européenne et à leur fournir toutes informations ou études pour étayer d'éventuelles procédures.

Le RSN reprend également l'économie générale de la directive « commerce électronique » qui institue un régime de responsabilité limitée pour les intermédiaires techniques, lesquels ne sont pas considérés comme éditeurs des contenus. Il crée cependant une sous-catégorie d'hébergeurs, celle des fournisseurs de plateformes en ligne qui mettent à la disposition du public des contenus produits par des utilisateurs, spécificité qui justifie un renforcement de leurs obligations. Ces plateformes ne sont pas, en principe, responsables des contenus qu'elles hébergent. Mais leur responsabilité peut être engagée si ces derniers présentent un caractère manifestement illicite et s'il est établi que, bien qu'en ayant eu connaissance, elles n'ont pas fait preuve de diligence pour le retirer.

Un des objectifs du RSN consiste précisément à faciliter cette information en instituant, à son article 16, un mécanisme de notification au profit des utilisateurs ou en créant, à son article 22, un statut de « signaleur de confiance ». Ce statut est accordé par le coordinateur national, compétent pour les services numériques, à des personnes morales qui disposent d'une expertise reconnue en matière de détection. Les plateformes sont alors tenues de traiter en priorité leurs signalements de contenus manifestement illicites, étant précisé qu'est illicite au sens du RSN tout contenu contraire au droit d'un État membre ou de l'Union européenne.

Ainsi que le prévoit la directive sur le commerce électronique, les fournisseurs d'accès à internet (FAI) relèvent quant à eux du régime des « services de simple transport » et ne sont pas responsables des contenus qu'ils transmettent. Ils doivent toutefois agir de manière neutre, c'est-à-dire ne pas être à l'origine de la transmission, ne pas sélectionner le destinataire de la transmission, ni les informations qui en font l'objet. Cela ne signifie pas qu'ils échappent à toute responsabilité. Une autorité judiciaire ou administrative peut exiger d'un FAI qu'il mette un terme à une infraction ou qu'il la prévienne en bloquant l'accès à un site internet au contenu illicite.

Le RSN institue, pour les services désignés comme « très grande plateforme en ligne » (TGPL) et « très grand moteur de recherche » (TGMR) une approche par les risques. Pour permettre de les identifier et ensuite les atténuer, le RSN prévoit d'abord des obligations qui s'imposent à toutes les plateformes, quelle que soit leur taille, comme l'obligation de mettre en place des mécanismes permettant de signaler la présence d'un contenu illicite ; de garantir la transparence des paramètres utilisés pour la recommandation de contenus (2° de l'article 27), tout en prévoyant une fonctionnalité pour les modifier (3° de l'article 27) ; d'assurer la transparence de leurs politiques et de leurs décisions de modération (articles 14, 15, 17 et 24) ; ou encore l'obligation d'identifier les publicités politiques (article 26).

S'y ajoutent, et c'est le « cœur du réacteur » du RSN, des obligations spécifiques renforcées pour les TGPL et les TGMR, ceux qui comptent plus de 45 millions d'utilisateurs mensuels (10 % de la population totale de l'Union) sur le territoire de l'Union européenne. Parmi ces obligations, on peut citer celle d'évaluer leurs risques systémiques et de les atténuer (articles 34 et 35) ; de tenir des registres des publicités ayant été diffusées au cours de l'année, précisant leur auteur, leur financeur et le groupe de personnes qu'elles visent (article 39) ; ou enfin, l'obligation de garantir aux autorités compétentes et à des chercheurs agréés, un large accès à leurs données, notamment de consommation (article 40), et donc à la connaissance de leurs interactions avec leurs utilisateurs.

Ces obligations font l'objet d'un suivi grâce à la publication de rapports de transparence. Ceux-ci précisent par exemple le nombre de notifications adressées par les utilisateurs

ou par les signaleurs de confiance, les suites qui leur sont réservées, le nombre de litiges en résultant transmis aux organes de règlement extrajudiciaires (prévus à l'article 21), les ressources humaines affectées à la modération des contenus. Si ce travail de *reporting* peut sembler fastidieux, c'est lui qui permet d'identifier les risques de manière précise et de vérifier la réalité et l'effectivité des mesures prises pour les atténuer. En cas de manquement, ce travail permet également de fonder l'engagement de procédures formelles susceptibles de se traduire par le prononcé de sanctions très lourdes, jusqu'à 6 % du chiffre d'affaires mondial.

Un pilotage partagé entre Commission européenne et autorités nationales

Dans un double souci d'efficacité et de pragmatisme, le RSN confie à la Commission européenne et à l'équipe de 150 collaborateurs constituée à cette fin à la « DG Connect » la supervision des TGPL et des TGMR, dont l'activité se déploie de fait à l'échelle de tout le territoire de l'Union. La DG Connect peut compter, depuis le mois d'avril 2023, sur l'appui du Centre européen pour la transparence algorithmique (ECAT).

Les articles 65 à 69 et l'article 72 du RSN confèrent ainsi d'importants pouvoirs d'enquête à la Commission européenne qui les exerce soit de sa propre initiative, soit à la suite d'une demande motivée d'un coordinateur pour les services numériques (article 65). Ces pouvoirs peuvent prendre la forme de l'envoi de demandes d'informations aux TGPL ou TGMR ; de la réalisation d'entretiens formels dans le pays concerné ; de l'envoi de demandes d'accès aux bases de données et aux algorithmes. En cas d'absence de diligences, la Commission européenne peut assortir ces demandes d'informations ou d'entretiens d'astreintes voire prononcer des amendes sans préjudice de celles prévues en cas de manquements.

Au quotidien, la régulation du RSN s'exerce en réseau. Chaque État membre désigne un « coordinateur des services numériques », membre d'un réseau animé au niveau européen par le « comité pour les services numériques » ou « DSA Board ». Outre des représentants des 27 régulateurs européens, ce comité compte des membres de la Commission européenne, qui le préside. Il se réunit en principe une fois par mois, mais peut se réunir de manière *ad hoc* en cas de nécessité. Aux termes de l'article 35 du RSN, il publie chaque année, sur le fondement des rapports d'évaluation et d'atténuation des risques systémiques publiés par les TGPL ou TGMR, un bilan des risques les plus importants répertoriés par État membre ainsi qu'une liste de bonnes pratiques. Un premier rapport devrait être publié avant la fin du premier semestre 2025.

La loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (loi « SREN ») a désigné l'Arcom « coordinateur des services numériques » pour la France. À ce titre, l'Autorité est compétente pour appliquer les dispositions du RSN aux plateformes établies en France (telles que Doctolib, Meetic ou Blablacar). Elle veille également à la bonne coordination de l'action des autres autorités nationales compétentes au titre du RSN, à savoir la CNIL et la DGCCRF, ainsi que d'autres partenaires, tels que Viginum, service à compétence nationale placé auprès du secrétaire général de la sécurité et de la défense nationale (SGDSN), spécialisé dans la détection d'ingérences étrangères. L'Arcom est enfin chargée de désigner des « signaleurs de confiance » pour le compte de la France.

Déploiement du RSN : premiers résultats et perspectives

Ce cadre et ces principes étant désormais posés et en vigueur, l'enjeu consiste aujourd'hui à réussir le déploiement opérationnel du RSN aux niveaux européen et national, un déploiement qui a commencé et donne de premiers résultats.

La Commission européenne a ainsi désigné 25 TGPL et TGMR. Au mois de novembre 2024, 19 de ces services avaient publié leur premier rapport d'évaluation et d'atténuation des risques systémiques. Vingt, dont trois plateformes proposant des contenus pornographiques, ont fait l'objet ou font l'objet d'enquêtes ou de demandes d'informations. S'y ajoutent des exercices plus « pratiques » destinés à mieux anticiper certains risques. À la suite de l'annulation du premier tour de l'élection présidentielle de Roumanie en raison de soupçons d'ingérences étrangères, la Commission européenne a invité le 27 mars 2025 les très grandes plateformes à participer à un « stress test » en matière de lutte contre la manipulation de l'information, en prévision de la tenue de nouvelles élections le 4 mai 2025. Enfin, certaines plateformes vont parfois au-delà de ce que prévoient leurs obligations : LinkedIn vient par exemple d'annoncer la suppression, de sa propre initiative, de près d'1,7 million de faux comptes.

Au niveau national, dès 2024, les équipes de l'Arcom ont constitué un dossier national d'information pour nourrir l'enquête de la Commission européenne sur les risques de dépendance liés au service TikTokLite. Rappelons que l'ouverture de cette procédure a suffi, dès le mois d'août 2024, à convaincre la plateforme d'abandonner ce service nocif en Europe[1]. Plus récemment, au mois de janvier 2025, l'Arcom a été destinataire de deux plaintes de parlementaires françaises – Aurore Lalucq, députée européenne, et Marie-Claire Carrège-Gée, sénatrice de Paris – déposées en application de l'article 53 du RSN et portant sur le système de recommandation de X, semblant mettre en avant les publications de son propriétaire. L'Arcom a instruit puis transmis ces plaintes à son homologue irlandais et à la Commission qui, le 17 janvier 2025, a adressé au réseau social X des demandes d'informations relatives au fonctionnement de son système de recommandation. L'Arcom mène de son côté une étude pour identifier l'existence de biais et en communiquera les résultats à la Commission européenne.

Depuis le mois de janvier 2025, l'Arcom a reconnu la qualité de « signaleurs de confiance » à cinq associations disposant d'une expertise dans des domaines différents : l'ALPA (prévention et lutte contre le piratage d'œuvres audiovisuelles) ; l'IFAW (sauvetage et préservation des espaces sauvages) ; Indecosa-CGT (information et défense des consommateurs salariés) ; Point de Contact (lutte contre les cyberviolences) et Addictions France (prévention et lutte contre les addictions). Avec l'association *e*-Enfance désignée en 2024, cela porte à six le nombre d'associations agréées, ce qui place la France au premier rang au niveau européen. Ces désignations vont se poursuivre car elles sont décisives pour obtenir le retrait rapide de contenus illicites.

En matière électorale, l'Arcom a adopté au mois de mars 2024 des préconisations pour aider les plateformes à lutter contre les manipulations lors des élections européennes et législatives. Ces préconisations sont très concrètes : prévoir des équipes internes dédiées aux élections et formées au droit électoral ; désigner des interlocuteurs pour les autorités nationales afin de faciliter les échanges en cas de soupçons d'ingérences étrangères ; afficher clairement les annonces publicitaires présentant un caractère politique. Des échanges ont été organisés entre les équipes de l'Arcom et les représentants français des plateformes pendant les élections pour s'assurer de leur bonne mise en œuvre. Ce dialogue, encore inexistant il y a quelques années, permet aujourd'hui de diffuser une « culture de la régulation » auprès d'acteurs qui y étaient étrangers. Forte de cette expérience réussie, l'Arcom va désormais travailler à la mise en place d'un « dispositif de réponse rapide » plus structuré, comme le prévoit le code de conduite approuvé par la Commission européenne en février 2025, autour de trois objectifs : faciliter les échanges entre autorités publiques pendant les élections ; mobiliser les médias, en particulier les vérificateurs de faits ; renforcer la coordination avec les plateformes.

[1] Il s'agissait d'un système qui récompensait le temps d'écran, au risque d'augmenter dangereusement l'addiction de ses utilisateurs à la plateforme.

Ce déploiement opérationnel du RSN a vocation à s'amplifier, dans une mesure qui dépendra de la capacité de mobilisation de la société civile. Le RSN offre en effet des outils précieux, en particulier les rapports d'évaluation des risques et les registres de données publicitaires, mais qui représentent une masse d'informations considérable que les seules autorités administratives nationales ne peuvent matériellement analyser. L'Arcom entend donc faire appel au monde de la recherche et aux acteurs de la société civile pour que dans chaque domaine concerné (santé publique, qualité du débat démocratique, protection des minorités et des enfants, propriété intellectuelle), ceux-ci s'emparent de ces données et aident les pouvoirs publics à les exploiter.

Conclusion

Le RSN, au-delà de ses objectifs propres, participe à une démarche plus large visant à favoriser la production et la circulation d'une information professionnelle. Cette approche s'appuie sur d'autres dispositions comme celles du règlement européen sur la liberté des médias (EMFA), en vigueur depuis le 7 mai 2024 ou, en France, les conclusions des États généraux de l'information. Des initiatives qui répondent à des objectifs communs : renforcer l'indépendance des médias, consolider leur modèle économique, garantir une meilleure visibilité aux informations produites par des journalistes professionnels, prévenir les ingérences et lutter contre la désinformation. Elles se fondent sur une conviction : l'information constitue un bien public inestimable pour nos démocraties. Sans information professionnelle, objective et sûre, il n'y a pas de débat public ni de scrutin éclairé. Régulateur de la communication audiovisuelle et numérique, l'Arcom s'attachera, conformément aux missions qui lui sont confiées par la loi, à en préserver l'intégrité.

Le baromètre du numérique - publication 2025

Par Michel SCHMITT,
Matthias de JOUVENEL
et Thierry SERIN
Conseil général de l'Économie

Le baromètre du numérique est un sondage récurrent qui porte sur les équipements et usages numériques de la population française. Nous présentons ici quelques-uns des résultats de la publication 2025 de ce baromètre. Ainsi, la population française se rend compte qu'elle passe beaucoup de temps devant les écrans et sent qu'elle passe à côté du réel qu'elle aime bien, finalement.

L'intelligence artificielle est une révolution qu'un tiers des Français a déjà testée. Pour que l'IA se développe harmonieusement, il va cependant falloir lever les nombreuses craintes et inquiétudes qu'elle suscite, et qui sont beaucoup plus importantes que lors de l'introduction du numérique.

Enfin, en ce qui concerne l'empreinte carbone, le comportement des Français va dans le bon sens. Il semble cependant que celui-ci ne soit que peu dicté par des considérations écologiques, mais avant tout par des considérations de coût.

Qu'est-ce que le baromètre du numérique ?

Il s'agit d'une enquête par sondage, menée chaque année, portant sur les équipements et les usages numériques des individus en France. Elle a été lancée par le Conseil général de l'Économie (CGE) en 2000, rejoint successivement par l'Autorité de régulation des Communications électroniques, des Postes et de la Distribution de la presse (Arcep) en 2003, par l'Agence nationale de la Cohésion des territoires (ANCT) en 2016 et enfin par l'Autorité de régulation de la Communication audiovisuelle et numérique (Arcom) en 2022. Chaque partenaire oriente le baromètre sur les thèmes spécifiques liés à son champ de compétences. Ainsi, le CGE se concentre sur les usages.

Pour la publication 2025, l'enquête a été réalisée par le Credoc, du 5 juillet au 6 août 2024, selon un mode mixte, en ligne et par téléphone. Une enquête flash par téléphone auprès de 1 000 personnes a permis de déterminer la proportion de la population ne disposant pas d'une connexion internet à domicile, donc moins susceptible de répondre à un sondage en ligne. L'échantillon complet compte 4 066 personnes résidant en France métropolitaine, dont 208 personnes de 12 à 17 ans (interrogées par internet), 601 personnes de plus de 18 ans ne disposant pas de connexion internet à leur domicile (interrogées par téléphone) et 3 257 personnes de plus de 18 ans (interrogées par internet). Les résultats ont été redressés selon l'âge, le sexe, la catégorie socioprofessionnelle, le niveau de diplôme, la taille de l'agglomération et la région.

Le questionnaire, constitué cette année de 102 questions, est composé d'un squelette stable dans le temps (taux d'équipement en téléphone fixe, *smartphone*, ordinateur à domicile, achats en ligne, administration en ligne, recherche d'offres d'emploi en ligne, freins à

l'utilisation d'internet…), de focus particuliers à chaque année ainsi que de questions à fréquence variable, selon l'actualité (sociabilité, télétravail, déconnexion, intelligence artificielle, règles pour les enfants…).

Le rapport d'analyse complet comprend 330 pages en raison de la richesse du questionnaire. L'ensemble des documents, le rapport d'analyse, la présentation utilisée lors de la conférence de presse[1] et une infographie de deux pages sont disponibles sur le site du CGE[2]. Toutes les données de l'enquête depuis 2007 sont accessibles sur la plateforme ouverte des données publiques françaises[3].

Les Français sont de plus en plus connectés. Ils sont 94 % à avoir accédé à internet au cours des 12 derniers mois, 84 % se connectant tous les jours (contre 68 % en 2015). Les 6 % non internautes sont essentiellement des personnes de plus de 70 ans, souvent dans l'incapacité de se débrouiller par elles-mêmes, faisant appel aux services d'un tiers. On peut donc considérer que la très grande majorité, voire l'ensemble de la société française est maintenant connectée.

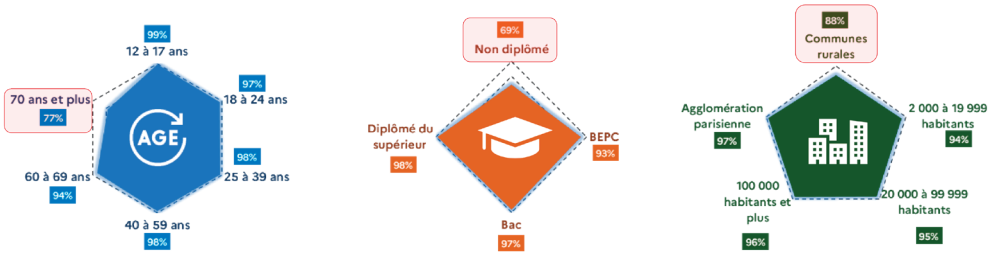


Figure 1 : Fréquence de connexion à internet, quel que soit le mode et le lieu de connexion - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

Comment les Français se connectent-ils à internet ?

Les trois-quarts de la population disposent désormais d'un accès internet à leur domicile (fibre ou câble) en nette progression (+ 8 points en un an), notamment pour les habitants des communes de 2 000 à 19 999 habitants (71 % en 2024 contre 54 % en 2023).

[1] Conférence de presse du 19 mars 2025 en présence de Clara Chappaz, ministre délégué chargé de la Transition numérique et des Télécommunications.

[2] https://www.economie.gouv.fr/cge/barometre-du-numerique-0

[3] https://www.data.gouv.fr/fr/datasets/barometre-du-numerique/

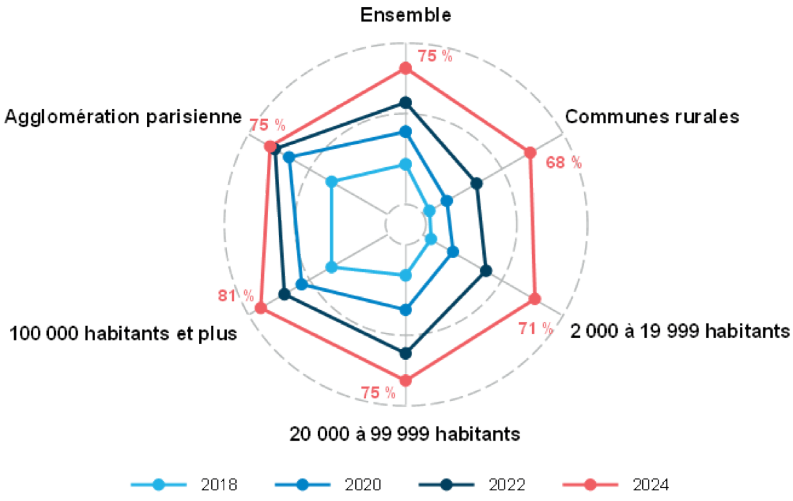


Figure 2 : Taux d'équipement en connexion internet à domicile - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

Les Français accèdent aussi à internet grâce à leur mobile en plus de leur connexion à domicile (79 %), une petite partie uniquement grâce à son mobile (9 % mais 19 % des 18-24 ans en hausse de + 7 points). Les connexions uniquement à domicile sont minoritaires (4 %).

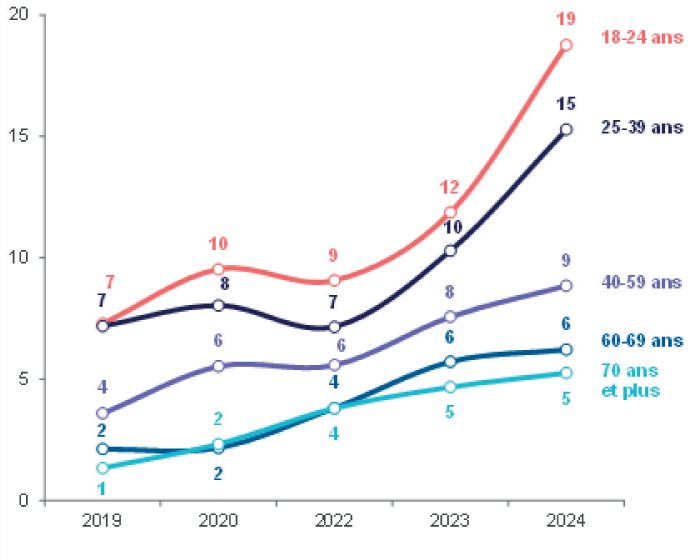


Figure 3 : Part de la population se connectant exclusivement par mobile - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

Si l'on examine la quantité de données utilisée :

- 50 % des personnes utilisant internet disposent d'un espace de stockage sur le *cloud*, le plus souvent gratuit. Lorsque l'hébergeur est gratuit, il est choisi par défaut dans la plupart des cas (41 %). Lorsqu'il est payant, le tarif est le premier critère de choix (33 %), devant la protection des données personnelles (28 %) et le recours à un hébergeur proposé par défaut (25 %).
- En 4 ans, la part des détenteurs de forfaits mobiles de plus de 100 Go a doublé, passant de 15 à 32 %. Cependant, les deux tiers des détenteurs de forfaits déclarent qu'ils ne consomment jamais ou de temps en temps l'intégralité de ce volume.

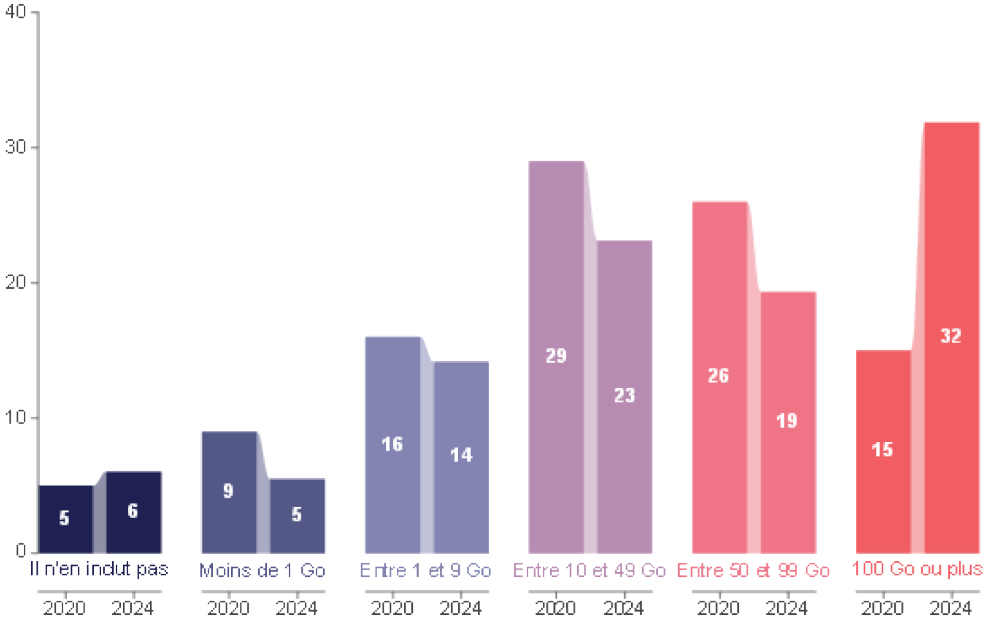


Figure 4 : Volume de données disponible dans les forfaits mobiles souscrits - Champ : population disposant d'un forfait mobile, en % (Source : baromètre du numérique 2025).

Quelques usages d'internet

La vie quotidienne des Français est largement connectée. À titre d'exemples, au cours des 12 derniers mois :

- 73 % des internautes ont réalisé au moins une démarche administrative[4] ;
- 67 % ont pris au moins un rendez-vous médical ;

[4] Il ne faut pas oublier que le baromètre du numérique est une enquête individuelle. Ainsi, si dans un foyer de deux personnes, l'une se charge de l'ensemble des démarches administratives (et il y en a toujours plus d'une par an), cela se traduira par « 50 % ont réalisé au moins une démarche administrative » dans les résultats du baromètre.

- 75 % ont recherché un itinéraire ;
- 31 % ont consulté des offres d'emploi.

Examinons à présent les comportements des Français en ce qui concerne les achats sur internet.

Achat sur internet, achat en magasin

Les achats en ligne sont revenus à leur niveau de 2020, plafonnant à 77 % de la population.

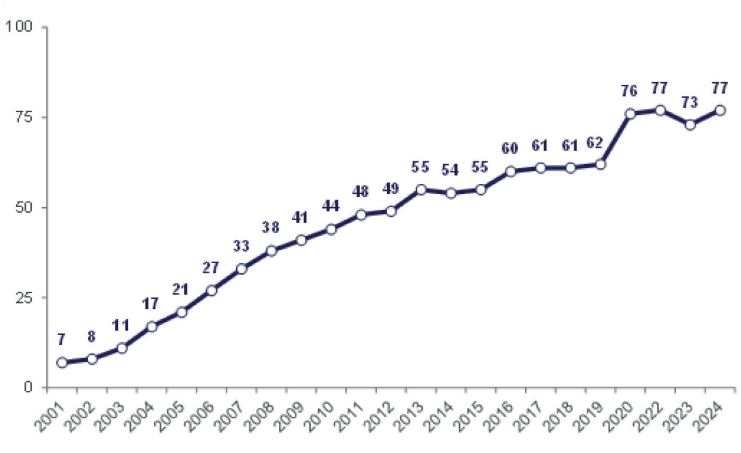


Figure 5 : Part de la population ayant réalisé des achats en ligne au cours des 12 derniers mois - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

Cependant, pour les achats de vêtements ou d'alimentation, les Français préfèrent réaliser leurs achats physiquement dans des magasins. Ils sont 64 % à préférer se déplacer pour leur habillement, et même 82 % pour leur alimentation.

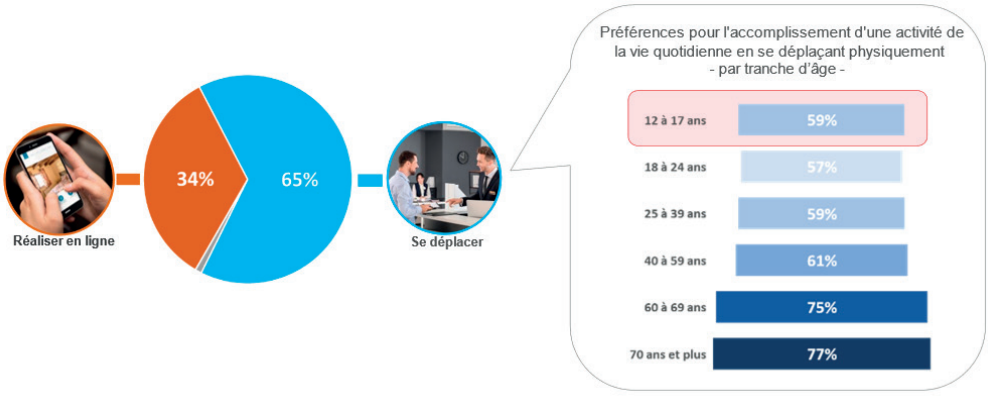


Figure 6 : Préférence pour l'accomplissement d'une activité de la vie quotidienne - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

Cet attrait pour le réel est également présent pour les livres papier, où 78 % des lecteurs restent attachés au livre papier.

Ceci montre l'usage raisonné du numérique par les Français pour les actions de la vie quotidienne, où se déplacer reste la norme (65 %) et, contrairement aux idées reçues, cela concerne également les jeunes.

Achat-vente d'objets de seconde main

L'achat-vente d'objets sur un site de seconde main n'est plus du tout marginal. En effet, 53 % des personnes disent avoir effectué une vente ou un achat d'objets de seconde main. Ceci concerne toutes les tranches d'âge de 20 à 60 ans.

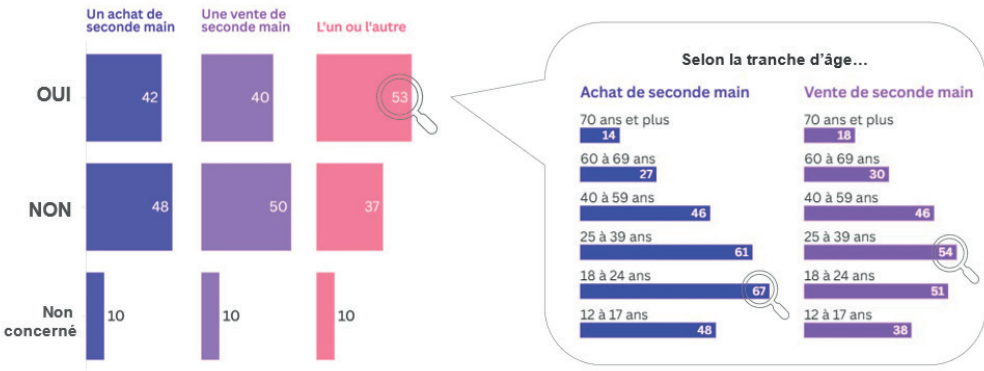


Figure 7 : Proportion d'individus un achat et/ou une vente sur des sites de seconde main - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

Les outils d'intelligence artificielle

La diffusion de l'intelligence artificielle (IA) dans la société française soulève des questions fondamentales quant à son adoption, à la confiance qu'elle inspire et à la perception de ses bénéfices et risques potentiels. Les résultats offrent un éclairage sur ces aspects. Ils révèlent une progression significative de l'adoption de l'IA en France, avec, paradoxalement, une population encore majoritairement méfiante et plutôt inquiète envers cette technologie.

En 2024, un tiers des Français déclare avoir déjà utilisé l'IA, marquant une augmentation significative de 13 points par rapport à 2023. Mais des disparités sont constatées selon le genre et l'âge, les hommes et les jeunes étant plus enclins à utiliser l'IA.

Concernant la confiance dans l'IA, la population française est encore majoritairement méfiante (56 %). Toutefois, cette méfiance est beaucoup moins marquée chez les utilisateurs d'IA (74 %) que chez les non-utilisateurs (26 %) et elle tend à augmenter avec l'âge. Dans un contexte mondial marqué par une quête croissante de sécurité, de transparence et de responsabilité, le concept d'IA de confiance émerge aujourd'hui comme une priorité. C'est le choix qu'a fait l'Union européenne en se dotant d'une réglementation renforcée dans ce domaine avec l'IA Act entré en vigueur le 12 juillet 2024.

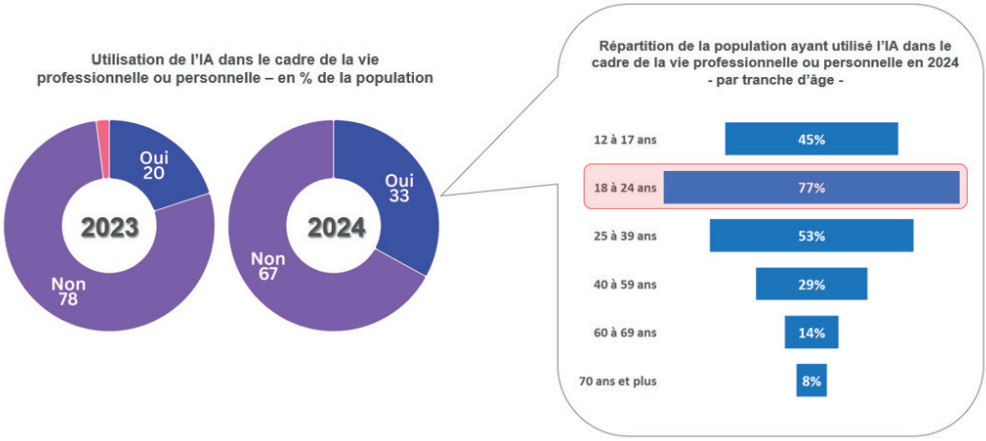


Figure 8 : Utilisation des outils d'IA et répartition par âge -
Champ : ensemble de la population de 12 ans et plus
(Source : baromètre du numérique 2025).

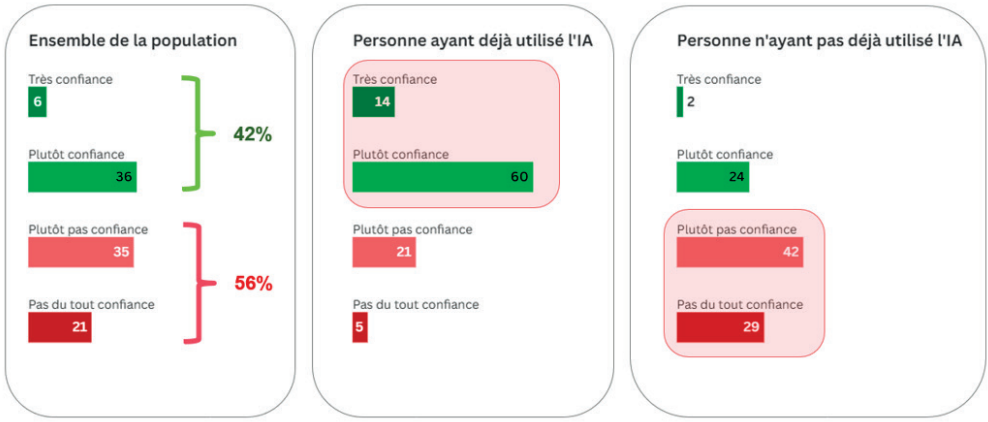


Figure 9 : Confiance dans les outils d'IA -
Champ : ensemble de la population de 12 ans et plus
(Source : baromètre du numérique 2025).

La perception de l'IA comme une opportunité ou une menace est, quant à elle, un peu plus nuancée. Si l'intelligence artificielle est majoritairement perçue comme une menace pour l'emploi (62 %) et la création artistique (53 %), les opinions sont partagées concernant son impact sur l'environnement (opportunité pour 48 % des répondants). À titre de comparaison, internet suscitait en 2008 un vrai enthousiasme dans le domaine de l'emploi (84 %), voire de la création artistique (63 %).

L'AI index publié en 2025 par l'Université de Stanford montre que d'importantes différences régionales persistent en matière d'optimisme à l'égard de l'IA. En 2024, la France était l'un des pays les plus sceptiques, avec seulement 41 % des répondants estimant que l'IA apporte plus de bénéfices que d'inconvénients. Malgré une augmentation de 10 points

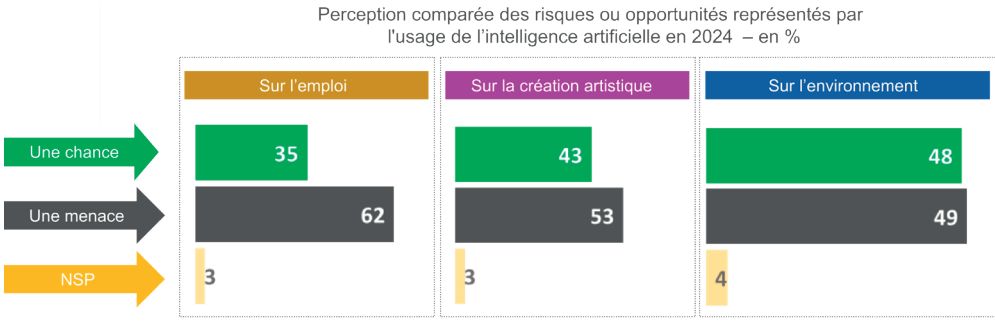


Figure 10 : Perception comparée des risques ou opportunités représentés par les outils d'IA - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

entre 2022 et 2024, la France reste donc parmi les pays les moins optimistes concernant l'IA, aux côtés des Pays-Bas (36 %), des États-Unis (39 %) et du Canada (40 %). La France s'inscrit dans une tendance observée dans plusieurs pays occidentaux : un scepticisme initial important vis-à-vis de l'IA, qui s'atténue progressivement, mais qui reste nettement plus marqué que dans les pays asiatiques ou d'Amérique latine.

Le temps passé devant les écrans est-il perçu comme raisonnable ?

Nous avons vu que les Français ont une large préférence pour se déplacer pour les actions de la vie quotidienne. Cependant, une large majorité estime que le temps passé devant les écrans pour leur usage personnel est excessif. En effet, 72 % déclarent passer plus de 2 heures par jour devant un écran et 25 % plus de 5 heures. Ce phénomène concerne surtout les 18-24 ans (39 %). Les autres tranches d'âge ont des comportements similaires entre elles.

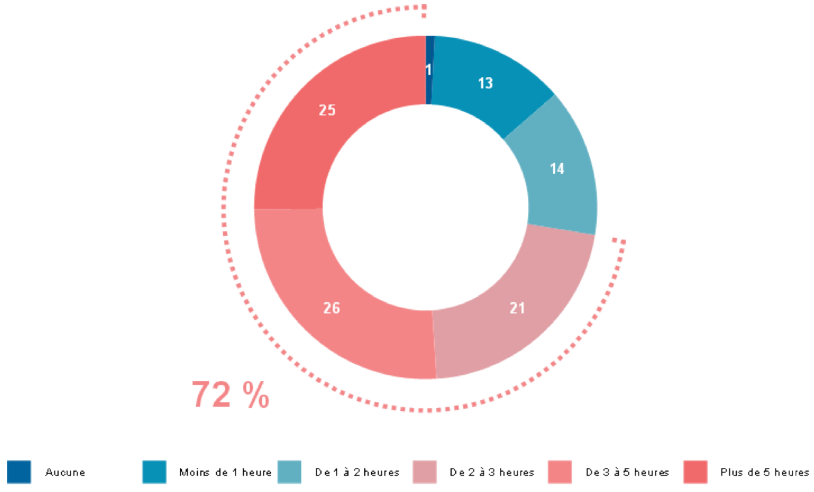


Figure 11 : Temps passé quotidiennement devant un écran pour un usage personnel - Champ : ensemble de la population ayant donnée une réponse chiffrée, en % (Source : baromètre du numérique 2025).

Ce temps passé devant les écrans est jugé « trop important » par 42 % des utilisateurs et « beaucoup trop important » par 19 % d'entre eux. Cette proportion augmente avec l'augmentation du temps passé devant les écrans. Si les plus jeunes passent plus de temps sur les écrans (60 % des 18-24 ans y passent plus de 3 heures par jour), ils sont toutefois plus prompts à estimer leur temps d'écran excessif que le reste de la population, à usage égal. 62 % des 18-24 ans qui déclarent passer plus de 3 heures par jour sur les écrans estiment ce temps excessif. Ce taux n'est que de 31 % chez les plus de 70 ans.

Ce sentiment d'addiction est fortement lié à l'utilisation des réseaux sociaux. 59 % des personnes qui utilisent plusieurs fois par jour les réseaux sociaux estiment leur temps d'écran excessif. À temps d'écran égal, les utilisateurs fréquents des réseaux sociaux sont 2 à 3 fois plus à estimer leurs temps d'écran excessif.

Parmi les personnes passant plus de 5 heures par jour devant un écran et utilisant plusieurs fois par jour les réseaux sociaux, 67 % estiment que leur temps d'écran est excessif. Ce taux est de 36 % chez celles qui n'utilisent pas les réseaux sociaux.

Cependant, même si les Français ont une certaine conscience de l'excès de temps passé devant les écrans, 65 % ne peuvent se passer de leur *smartphone* une journée.

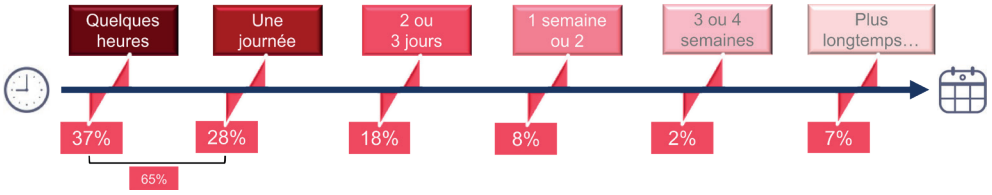


Figure 12 : Temps maximum pouvant être passé sans *smartphone* - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

Empreinte carbone des équipements numériques

L'empreinte carbone du numérique est essentiellement liée aux équipements, et dans une moindre mesure aux usages.

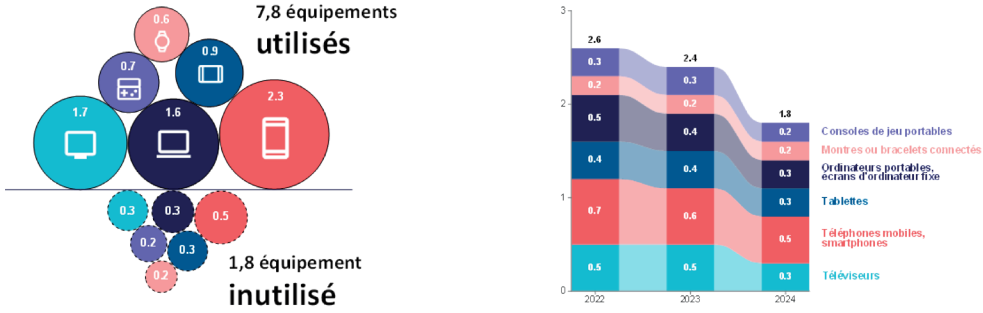


Figure 13 : Nombre d'écrans par foyer - Champ : ensemble de la population de 12 ans et plus (Source : baromètre du numérique 2025).

Le nombre d'équipements numériques par foyer reste élevé (9,6 équipements numériques avec écran en moyenne par foyer, dont 7,8 équipements utilisés et 1,8 inutilisés). Cependant, on observe une baisse du nombre d'écrans inutilisés (2,4 en moyenne en 2023, 1,8 en 2024, soit une baisse d'environ 25 % en un an).

Parallèlement, la durée de détention des *smartphones* s'allonge. 27 % des individus conservent le même *smartphone* pendant trois ans ou plus (+ 11 points depuis 2020). La part de *smartphones* renouvelés bien qu'encore fonctionnels diminue de 4 points par rapport à 2020. La proportion d'acquisitions de *smartphones* d'occasion ou reconditionnés reste stable (22 % contre 78 % de neuf).

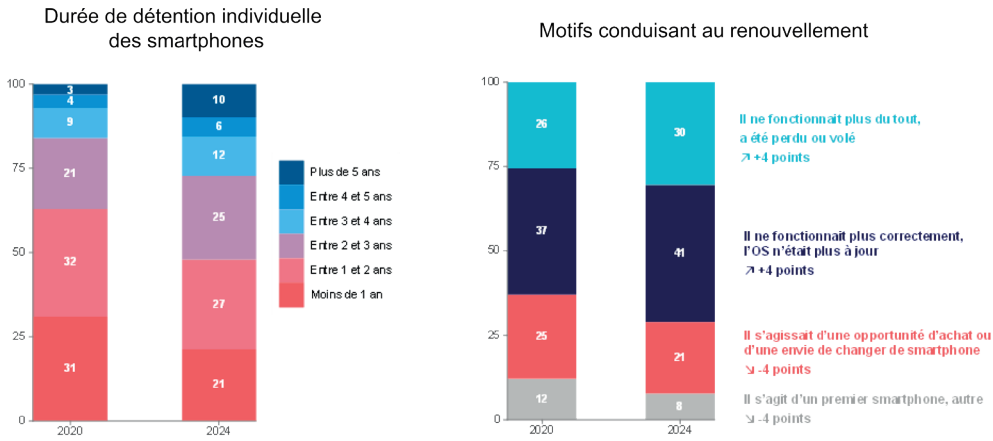


Figure 14 : Durée de détention et motif de changement d'un smartphone - Champ : ensemble de la population disposant d'un *smartphone* (Source : baromètre du numérique 2025).

Depuis le 1er janvier 2022, les opérateurs internet et mobile doivent informer leurs clients sur l'empreinte carbone de leurs consommations de données (loi Agec[5]), mais 60 % des clients ignorent cette exigence et seulement 14 % se disent incités à limiter leur consommation de données mobiles. Ils représentent un tiers des personnes ayant connaissance de cette information. Interrogés en 2023 sur les actions jugées utiles pour limiter leur empreinte environnementale numérique, 20 % des répondants considéraient la limitation de leur consommation de données mobiles comme une action efficace.

Ainsi, bien que l'empreinte du numérique diminue grâce à la réduction du nombre d'écrans possédés individuellement et l'allongement de la durée de détention des *smartphones*, ce comportement est plus lié à des considérations financières qu'à des considérations écologiques.

[5] https://www.ecologie.gouv.fr/loi-anti-gaspillage-economie-circulaire

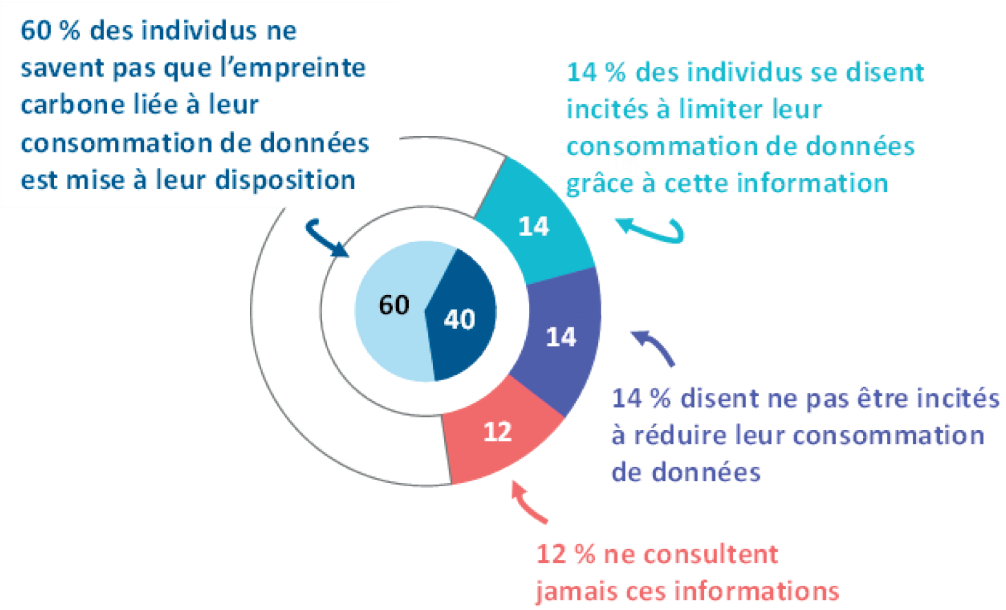


Figure 15 : Consultation des informations relatives à l'empreinte carbone liée à la consommation des données mobiles - Champ : population de plus de 18 ans disposant d'un téléphone mobile (Source : baromètre du numérique 2025).

Conclusion

De nombreux autres aspects sont abordés dans le baromètre du numérique 2025, en particulier sur les questions d'inclusion, de freins et de compétences liés au numérique.

Ce qui nous semble devoir être noté dans la présente publication du baromètre est le fait que la population française se rend compte qu'elle passe beaucoup de temps devant les écrans et sent qu'elle passe à côté du réel qu'elle affectionne, finalement. L'intelligence artificielle est une révolution qu'un tiers des Français a déjà testée. Pour que l'IA se développe harmonieusement, il va falloir lever les nombreuses craintes et inquiétudes qu'elle suscite. Ces craintes et inquiétudes étaient bien moindres lors de la diffusion du numérique. Enfin, en ce qui concerne l'empreinte carbone, le comportement des Français va dans le bon sens. Il semble cependant que celui-ci ne soit que peu dicté par des considérations écologiques, mais avant tout par des considérations de coût. En effet, garder son téléphone plus longtemps permet de réaliser des économies.

Ceci doit être pris en compte dans le développement de tout nouveau service numérique ainsi que dans la définition des politiques publiques, si l'on veut que la population française se les approprie.

Compliance and new regulations

Introduction

Overview of different regulations

Online platforms institute power dynamics, especially between the different categories of publics that they bring together. This mediation often relies on algorithms that are opaque both to the individuals that are involved and to society at-large. The right of access to one's personal data, currently provided under article 15 of the GDPR, has in part been created to provide remedies to such informational asymmetries.

In this article, we will examine recent case law that pave the way towards the development of both individual and collective uses of this right of access, thereby contributing to a higher degree of individual transparency and collective comprehension of platform power.

It is impossible to draw up an exhaustive list, or even a simple typology, of the actors targeted by the eleven texts on cybersecurity that mark the first half of the Digital Decade. There are so many of them that the architects of this monumental piece of legislation are far from having anticipated everything. Unforeseen issues are emerging, both in terms of the classification of the actors concerned and the corresponding legal regime.

In response to the risks inherent in the digital space in general and artificial intelligence in particular, a body of rules aimed at detecting and preventing these risks has gradually been built up, brick by brick. This construction, which originated mainly in the European Union, is part of a broader framework: Compliance Law. The rules that make up this body share common methods and tools, and above all a common goal: preserve and/or improve systems so that the human beings involved are protected.

Europe has thus established a model based on a balance between freedom and the protection of individuals, *i.e.* a model of Regulation. This regulation is directly integrated into the operators controlling the systems in question, requiring them

to detect, prevent and, where necessary, repair and remedy the risks generated, making this Regulation not only an element but also an example of Compliance Law.

31 Digital law: towards the disappearance of the judge?
Olivier ITEANU

The member states of the European Union have relinquished the privilege of regulating the digital sector to the Union's institutions. This has resulted, over the past thirty years, in the establishment of a regulatory structure that renders the judicial system invisible, populating the regulatory system with independent administrative authorities and organizations of various kinds. This article examines this through two popular EU texts: the GDPR of 2016, which came into force in 2018, and the AI Act of 2024. However, the judicial judge remains accessible, within a different sphere of intervention. This article argues that this invisibility of judges should not become an erasure.

European regulation : protection or hindrance?

38 The role of standardisation in European digital policy
Louis MORILHAT

At a time when technical norms and standards in the telecommunications and digital sectors are gradually moving away from the purely technical sphere to encompass issues of governance, ethics and sovereignty, standardisation bodies are emerging as forums for shaping the technological balance of power between players.

By reaffirming standardisation as an instrument of technological competitiveness and integrating it as a tool of open strategic autonomy, the European Union is making strong use of this lever to shape its regulatory framework through a novel governance architecture based on a hybrid between legislation and technical specifications.

The aim of this article is to analyse the issues specific to the digital domain in standardisation, the integration of this field into European digital policy and the gradual transformation of norms and standards into tools of technological influence.

45 Action by operators
Dominique WURGES

After recalling some general considerations on the interest of standardisation for telecommunications operators, the author details in this article the specific elements of this sector and describes the main principles guiding the action of operators in their standardisation activities and the resources they allocate to it.

In particular, this article presents the increasingly broad field of activities of ICT sector bodies dedicated to standardisation, their specific features, and sets out the main issues involved in participating in these activities for a major operator. It is completed by an analysis of two concrete examples. Finally, the article extends the discussion to considerations related to standardisation and raises the question of its future in the face of the rise of open source.

Fourthly, it corresponds to the conception and practice of a new branch of Law, Compliance Law, which should not be confused with "conformity" and which is normatively anchored in its "Monumental Goals".

Fifthly, Compliance Law internalises Monumental Goals in the digital operators which disseminate them through structures and behaviours in the digital space.

Sixthly, through the interweaving of legislation, court rulings and corporate behaviour, the Monumental Goals are given concrete expression, willingly or by force, in ways that can civilise the digital space without undermining the primacy of freedom.

Since Arcep's creation when the telecoms sector was opened to competition 30 years ago, the sector regulator's scope of intervention has gradually expanded to include digital technology. Beyond technical and economic regulation, which is at the heart of its work, it has also been granted other responsibilities in terms of digital coverage of the territory, or more recently, in assessing the sustainability of digital technology, notably as a neutral expert in the sector.

Alongside the traditional tools at its disposal (rule-making power, sanctioning power), the regulator has been led to resort to other forms of action, such as data-driven regulation, aimed at reducing information asymmetry, or the definition of best practices, the aim of which is to guide behavior. Measuring the environmental impact of digital technology and the general eco-design framework for digital services are two examples of Arcep's "magisterium of influence".

The Digital Services Act is designed to protect freedom of speech while correcting structural flaws resulting from the operation and uses of very large online platforms (VLOP) or very large search engines (VLSE). It thus establishes so-called "systemic" regulation that is proportionate, attentive to freedoms, and based on a risk-based approach that platforms are obliged to identify and then mitigate.

Designated coordinator of digital services in France, Arcom contributes to the implementation of this new form of regulation. In addition to its historical role as regulator of traditional media, it thus fully assumes its new mission as leader of digital regulation in France alongside the European Commission and in close collaboration with the other national authorities competent in matters of DSA.

Miscellany

The Digital Barometer is a recurring survey that looks at the digital equipment and uses of the French population. Here we present some of the results of the 2025 publication of this barometer. The French population is realising that it spends a lot of time in front of screens and feels that it is missing out on the real thing that it actually likes.

Artificial intelligence is a revolution that a third of French people have already tried out. If AI is to develop harmoniously, however, we will have to overcome the many fears and concerns it arouses, which are much greater than when digital technology was first introduced.

Finally, as far as the carbon footprint is concerned, the behaviour of the French is moving in the right direction. However, it seems that this behaviour is dictated not so much by ecological considerations, but above all by cost considerations.

Issue editors

Pierre Bonis and Lucien Castex

Ont contribué à ce numéro

Martin AJDARI est diplômé de l'École supérieure de commerce de Paris et de Sciences Po Paris, ancien élève de l'École nationale d'administration (Promotion René Char). Il commence sa carrière en tant qu'administrateur civil au ministère de l'Économie et des Finances. En 1999, il est nommé directeur administratif et financier de Radio France Internationale (RFI). Entre 2000 et 2002, il est conseiller technique au sein des cabinets de Laurent Fabius, ministre de l'Économie, des Finances et de l'Industrie, et de Florence Parly, secrétaire d'État au Budget, avant d'être nommé, en 2002, chef du bureau du financement du logement à la direction du Trésor.
En 2004, Martin Ajdari est nommé directeur général délégué de Radio France puis il rejoint l'Opéra de Paris en 2009 en qualité de directeur adjoint. En 2010, il intègre le groupe France Télévisions, comme directeur général délégué aux ressources, fonctions qu'il cumule ensuite avec celles de secrétaire général. Il rejoint en 2014 le ministère de la Culture et de la Communication, en tant que directeur du cabinet, successivement d'Aurélie Filippetti et de Fleur Pellerin. Il est nommé à la tête de la direction générale des Médias et des Industries culturelles (DGMIC) de ce même ministère en 2015. Il retrouve l'Opéra national de Paris en 2020, en tant que directeur général adjoint.
Par décret du président de la République, il est nommé président de l'Autorité de régulation de la communication audiovisuelle et numérique à compter du 2 février 2025.
→ ***L'Arcom à l'heure du règlement sur les services numériques***

Pierre BONIS, diplômé de la Sorbonne en philosophie et littérature, débute sa carrière au ministère des Affaires étrangères. Conseiller sur les questions de fracture numérique de 2002 à 2004, il devient en 2005 chef du bureau des NTIC au ministère des Affaires étrangères. Il rejoint une première fois l'Afnic en janvier 2008 en qualité de responsable Produits et Partenariats, au sein de la direction de la Communication. En janvier 2009, il est nommé conseiller au cabinet de la Secrétaire d'État au Développement de l'économie numérique. Il y est chargé des sujets d'innovation, de contenus et des affaires internationales. De novembre 2010 à février 2012, il poursuit sa mission de conseiller auprès de la ministre de l'Écologie, du Développement durable, des Transports et du Logement.
Il rejoint l'Afnic une seconde fois en octobre 2012. Il y occupe le poste de directeur général adjoint. Spécialiste des questions de coopération internationale, il est également membre du conseil d'administration du CENTR, association européenne des registres nationaux de noms de domaine, de 2016 à 2020, réélu pour un nouveau mandat en 2025. Sur recommandation du conseil d'administration de l'Afnic, il est nommé directeur général de l'association au 1er septembre 2017. En 2018, il est co-président du comité d'organisation du Forum mondial sur la Gouvernance d'internet de Paris, organisé dans le cadre des Nations unies. En 2019, il est élu président du groupe de liaison sur la Gouvernance de l'Internet du CCNSO (ICANN).
Ses principales publications récentes sont « Les fractures numériques » dans l'ouvrage collectif *Les défis du numérique*, coordonné par Dalila Rahmouni-Syed Gaffar, éditions Bruyland, février 2019 ; avec Godefroy Beauvallet, « Les infrastructures du numérique », dans l'ouvrage collectif *Numérique, action publique et démocratie* aux Presses Universitaires de Rouen et du Havre (PUHR), novembre 2020.
→ ***Réguler le numérique, ou Sisyphe heureux***

Lucien CASTEX est conseiller du directeur général de l'Afnic en charge des sujets Gouvernance, Internet et société. Il a pour principales missions les questions de prospective touchant à l'évolution d'internet et aux interactions entre internet et société, et de représenter l'Afnic en France et à l'international, notamment dans le champ des politiques publiques liées au développement de l'internet et du numérique.

À ce titre, il coordonne le Forum français sur la gouvernance de l'Internet (FGI France) et participe à l'organisation du Forum mondial organisé sous l'égide des Nations unies (UN IGF). Depuis 2020, il est co-responsable du groupe de recherche Gouvernance et régulation d'Internet, GDR, CIS, CNRS et depuis 2022, le point focal de l'Afnic au sein de l'Union internationale des Télécommunications (UIT) et au sein des groupes de travail interministériels dédiés.
Il est par ailleurs chercheur associé au sein de l'Université Sorbonne Nouvelle – Paris 3 et a été nommé au sein de la Commission nationale consultative des droits de l'Homme (CNCDH).
Ses dernières publications sont : PERARNAUD C., ROSSI J., MUSIANI F. & CASTEX L. (2024), *L'avenir d'internet : unité ou fragmentation ?*, Bordeaux, Le Bord de l'Eau, 146 pages et CASTEX L. (2024), « La gouvernance de l'internet et la construction d'un nouveau multilatéralisme », *in La souveraineté numérique* (dir. Bertrand B.), Bruylant.
→ ***La gouvernance d'Internet entre consolidation et fragmentation***

Matthias de JOUVENEL, ancien élève de l'École Normale Supérieure de Cachan (département d'économie et de gestion 1997-2000) et ancien élève de l'École nationale supérieure des Postes et Télécommunications (2001-2002), est administrateur de l'État en poste au Conseil général de l'Économie (CGE), où il pilote le baromètre du numérique depuis plusieurs années. Il est l'auteur de rapports publics dans des domaines variés (tourisme, devoir de vigilance, économie circulaire, contrefaçon, filières REP…) et il a appuyé plusieurs missions parlementaires dont celle confiée au député Éric Bothorel « Pour une politique publique de la donnée ».
→ ***Le baromètre du numérique - publication 2025***

Marie-Anne FRISON-ROCHE, agrégée des Facultés de droit, est spécialisée en Droit de la Régulation et de la Compliance. En 2001 à Sciences Po, elle a créé le Master de Droit Économique, le Forum de la Régulation et la Chaire Régulation. Depuis 2009 elle a fondé et dirige le *Journal of Regulation & Compliance* (JoRC), qui organise des manifestations scientifiques et publie des ouvrages. Elle dirige les collections : chez Dalloz Cours Dalloz-Droit privé et Régulations & Compliance, chez Bruylant Compliance & Regulation, chez Lextenso Droit & Économie. Elle a notamment en 2019 remis au Gouvernement français un rapport sur L'apport du Droit de la Compliance à la gouvernance d'Internet.
→ ***Réguler le numérique, ou Sisyphe heureux***
→ ***Le Droit de la Compliance, voie royale pour réguler l'espace numérique***

Olivier ITEANU est avocat à la cour d'appel de Paris depuis 1989. Il est chargé d'enseignement dans le Master 2 « Droit du numérique, administrations et entreprises » de l'Université Paris I Sorbonne depuis 15 ans, dirigé par les Professeurs William Gilles et Irène Bouhadana et, de 2001 jusqu'en 2022, dans le Master 2 « Droit des activités spatiales et des télécoms » de l'Université Paris-Saclay dirigé par le Professeur Philippe Achilleas.
Olivier Iteanu est l'auteur du premier ouvrage jamais publié sur le droit français et Internet paru aux Éditions Eyrolles en Avril 1996 Internet et le droit et de 4 autres ouvrages dont le dernier, *Quand le digital défie le droit* (Éditions Eyrolles, novembre 2016) a reçu le prix spécial du jury au Forum International de la Cybersécurité en 2017 (FIC 2017).
Il est le fondateur et co-dirige Iteanu Avocats, une société d'avocats composée de 12 professionnels basée à Paris 8e qui dédie son activité au droit du numérique et de la donnée depuis 30 ans. Il est médiateur, notamment agréé par le Centre de Médiation et d'Arbitrage de Paris (CMAP) et régulièrement désigné par les tribunaux, et arbitre.
Il est président d'honneur du Chapitre français de l'Internet Society (ISOC France) après avoir été son président de juin 2000 à juin 2003 et président de la coordination européenne des Chapitres de l'Internet Society de juin 2003 à juin 2004. Il a été par

ailleurs vice-président de l'association Hexatrust & Cloud Confidence, cybersécurité et cloud de confiance, en charge du Groupe de travail juridique et *lobbying* jusqu'en janvier 2021, l'un des fondateurs de Cloud Confidence et d'Eurocloud France,
Il a été également désigné par le conseil d'administration de l'Internet Corporation for Assigned Names and Numbers (ICANN), l'autorité mondiale de gestion des adresses et noms de domaine Internet basée aux États-Unis en Californie, comme un des 9 membres du Comité d'Etude At Large Membership et l'un des deux représentants européens auprès de ce comité. Il a également été membre pour deux années du comité de sélection de l'Internet Review Panel, chambre des recours de l'ICANN. Il est président d'honneur du Chapitre français de l'Internet Society (ISOC France) dont il a été le président de 2000 à 2003 puis président de la coordination européenne jusqu'en 2005.
→ ***Droit du numérique : vers l'effacement du juge ?***

Xavier MERLIN, Ingénieur général des Mines, diplômé de l'École polytechnique et de Telecom Paris et ancien élève de l'Institut d'Études politiques de Paris, a été nommé membre du collège de l'Arcep par la présidente de l'Assemblée nationale le 12 janvier 2024.
Il débute sa carrière en 1996 à la direction de la Prévision du ministère de l'Économie, des Finances et de l'Industrie en tant que chargé des études économiques sur internet, l'audiovisuel, les télécommunications et la concurrence. Il intègre en 1998 la direction des Relations économiques extérieures (DREE) de ce même ministère comme chargé des négociations multilatérales sur le commerce électronique, l'audiovisuel, les télécommunications et la poste.
Nommé en 2000 conseiller technique en charge des affaires européennes et multilatérales auprès de Catherine Tasca, alors ministre de la Culture et de la Communication, il devient en 2002 directeur des affaires européennes et internationales du Centre national de la cinématographie (CNC). En 2008, il rejoint la direction générale des Entreprises (DGE) en tant que sous-directeur de la réglementation et des affaires européennes et multilatérales en matière de communications électroniques. Il y est nommé chef du service de l'action territoriale, européenne et internationale en 2014. En 2019, il prend la direction de la mission interministérielle relative à la simplification des formalités administratives des entreprises et de publicité légale, en charge de la mise en œuvre du guichet unique pour les formalités d'entreprise, prévu par la loi Pacte.
Il est par ailleurs auteur et directeur de collection d'ouvrages parascolaires aux éditions Ellipses.
→ ***Régulation économique et « magistère d'influence »***

Louis MORILHAT est en charge des sujets de normalisation du numérique au sein du service de l'Économie numérique de la direction générale des Entreprises. À ce titre, il représente la France à l'Union internationale des télécommunications (UIT), à l'Institut européen des normes de télécommunications (ETSI) et contribue à assurer la prise en compte des stratégies industrielles de l'État au sein du CEN-CENELEC et de l'ISO-IEC à travers les commissions de normalisation Afnor. Auparavant, il travaillait au sein d'Afnor Normalisation sur les sujets d'intelligence artificielle et de souveraineté numérique.
→ ***La place de la normalisation dans la politique européenne du numérique***

Alex NICOLLET est doctorant en droit à l'Université Jean Moulin Lyon 3. Il réalise une thèse sur le sujet « Droit de la concurrence et Droit de la Compliance », sous la direction du Professeur Jean-Christophe Roda.
Il est par ailleurs *Junior Editor* du *Journal of Regulation & Compliance* (JoRC).
→ ***Le Droit de la Compliance, clé de voute de la Régulation de l'intelligence artificielle***

Clément PERARNAUD est docteur en science politique, chercheur à la Vrije Universiteit de Bruxelles (VUB). Ses travaux récents portent sur la fabrique des politiques numériques européennes et sur les rapports de pouvoir dans la gouvernance d'Internet.

→ ***Entre ouverture et fragmentation : les deux visages de la « souveraineté numérique européenne »***

Julien ROSSI est maître de conférences à l'Université Paris-VIII Vincennes-Saint-Denis, et chercheur au Centre d'études sur les médias, les technologies et l'internationalisation (CÉMTI). Co-coordinateur du groupe de travail sur la gouvernance et la régulation d'Internet du GDR Internet, IA et Société du CNRS, ses travaux se situent à l'intersection des études sur la gouvernance d'Internet et de celles sur le rapport entre droit et technologie. Il est l'auteur d'une thèse et de plusieurs papiers sur l'histoire du droit des données à caractère personnel et sur les rapports entre Droit et standardisation technique.
Il a récemment publié, avec Clément Perarnaud, Francesca Musiani et Lucien Castex, un livre intitulé *L'avenir d'Internet : unité ou fragmentation ?*, tiré d'un projet de recherche mené pour le compte du Parlement européen sur les craintes d'une possible fragmentation d'Internet. Depuis janvier 2025, il est responsable scientifique du projet ANR DATARights, qui étude les usages et non-usages du droit d'accès aux données à caractère personnel.

→ ***Droit des données personnelles, plateformes et transparence algorithmique***

Michel SCHMITT est membre du Conseil général de l'Économie, président de la section Innovation, Compétitivité, Modernisation. Titulaire d'un doctorat et d'une habilitation à diriger les recherches en Morphologie Mathématique, il a successivement occupé des postes dans l'industrie (Laboratoire Central de Recherche de Thalès) et dans l'enseignement supérieur (directeur de la recherche de Mines ParisTech, vice-président numérique de Paris Sciences et Lettres).
Ses centres d'intérêt scientifiques concernent le numérique et le traitement des données au sens large – probabilités, analyse d'image, intelligence artificielle, bio-informatique. Il est à l'origine de la création de l'unité mixte Inserm U900 « Cancer et génome : bioinformatique, biostatistiques et épidémiologie des systèmes complexes » ainsi que du « Centre de recherche sur les risques et les crises » de Mines Paris.

→ ***Le baromètre du numérique - publication 2025***

Michel SÉJEAN est Professeur agrégé de droit privé et sciences criminelles à l'Université Sorbonne Paris Nord (Villetaneuse). Il codirige le Code de la cybersécurité aux éditions Dalloz, et est chercheur à l'Institut de Recherche pour un Droit Attractif (IRDA), et chercheur associé de la Chaire Souveraineté numérique et Cybersécurité de l'IHEDN. Il codirige le Master 2 de Droit des Activités Numériques de l'Université Sorbonne Paris Nord.

→ ***Les acteurs visés par la législation européenne sur la cybersécurité***

Thierry SERIN est secrétaire général adjoint du Conseil général de l'Économie. Attaché d'administration de l'État hors classe, titulaire d'une maîtrise d'administration économique et sociale et d'un DEA de droit public, il a rejoint le ministère de l'Économie et des Finances en 2001 où il a d'abord occupé différents postes dans les fonctions support (RH, informatique, immobilier et logistique). En 2013 il devient secrétaire général de la Mission interministérielle d'inspection du logement social (Miilos) puis de l'Agence nationale de contrôle du logement social (ANCOLS).
En 2015, il réintègre le ministère de l'Économie et des Finances où il occupe la fonction de chef du bureau « mobilités-distribution » avant de rejoindre le CGE en 2022. Ayant

développé une appétence pour le numérique tout au long de son parcours, il s'intéresse plus particulièrement au domaine de l'intelligence artificielle depuis 2023.
→ ***Le baromètre du numérique - publication 2025***

Dominique WURGES est actuellement directeur des relations institutionnelles pour la normalisation au sein d'Orange. Il est responsable des relations avec les organisations internationales impliquées dans les activités de normalisation aux niveaux national, européen et international (UIT, ETSI, Afnor, etc.) et participe aux réunions de gouvernance de ces organisations. Il a été vice-président de l'assemblée générale de l'ETSI de 2018 à 2022. Il est actif sur de nombreux sujets traités par les organismes de normalisation et les forums, tels que l'impact des TIC sur le changement climatique, les relations entre opérateurs ou l'évolution du système de normalisation de la radiodiffusion.
Au sein de la Commission européenne, il est membre du Forum de haut niveau sur la normalisation européenne (HLFS), représentant l'ETNO (opérateurs de réseaux de télécommunications européens), et membre de la plateforme multipartite européenne de normalisation des TIC.
Au niveau international, il a été élu président de la Commission d'études 5 de l'UIT-T, la commission technique de l'Union internationale des télécommunications (UIT) en charge de l'environnement, de l'action climatique, de l'économie circulaire et des champs magnétiques électroniques. Il est le seul président européen de cette agence spécialisée du système des Nations unies.
En France, Dominique Wurges est membre du Comité de coordination et de pilotage de la normalisation (CCPN) d'Afnor et vice-président du Comité stratégique Numérique d'Afnor. Il est également membre du conseil d'administration du Forum audiovisuel numérique français (FAVN).
Il est diplômé de l'ENSPTT (École nationale supérieure des PTT) après un passage à l'Ena et de Paris-Dauphine (DESS de gestion des Télécommunications et de l'audiovisuel).
→ ***L'action des opérateurs***