Les modes de régulation des activités numériques : exploration des tensions entre l'approche par les risques (risk-based) et l'approche fondée sur la protection des droits

Winston Maxwell

LES MODES DE RÉGULATION DES ACTIVITÉS NUMÉRIQUES :

EXPLORATION DES TENSIONS ENTRE L'APPROCHE PAR LES RISQUES (*RISK-BASED*) ET L'APPROCHE FONDÉE SUR LA PROTECTION DES DROITS (*RIGHTS-BASED*)

Mémoire de synthèse pour présenter l'habilitation à diriger des recherches de l'Université Panthéon-Sorbonne, soutenue le 25 novembre 2022 par Winston Maxwell*

Jury:
Célia Zolynski, Professeure, Université Panthéon Sorbonne, Présidente du Jury
Brunessen Bertrand, Professeure, Université de Rennes, Rapporteure
Nicolas Curien, Professeur, Conservatoire National des Arts et Métiers, Rapporteur
Judith Rochfeld, Professeure, l'Université Panthéon-Sorbonne, Garante
Jean-Yves Ollier, Conseiller d'Etat
Céline Castets-Renard, Professeure University of Ottawa

*Directeur d'études, droit et numérique
Télécom Paris - Institut Polytechnique de Paris
Laboratoire i3 (UMR 9217)
winston.maxwell@telecom-paris.fr

Résumé
Pour soutenir mon habilitation à diriger des recherches, j'ai présenté le 25 novembre 2022 deux mémoires : un mémoire original sur le contrôle humain des systèmes d'IA, et le présent mémoire de synthèse sur les tensions entre l'approche de régulation par les risques et l'approche de régulation fondée sur la protection des droits.

Le présent mémoire de synthèse est divisé en deux parties. La première partie (Titre I) présente ce qu'est une approche par les risques, et une approche fondée sur le respect des droits. Ces deux approches puisent leurs origines dans les traditions philosophiques, l'utilitarisme pour l'approche par les risques, et la déontologie pour l'approche fondée sur le respect des droits. L'approche par les risques est influencée par l'analyse économique et la recherche du bien-être social par la mise en équilibre de différents droits et intérêts sociétaux. L'approche par les droits refuse une telle mise en équilibre car le centre de l'attention n'est pas la maximisation du bien-être collectif, mais les droits de l'individu en tant que tel. Néanmoins, les droits fondamentaux connaissent bien un mécanisme de pondération dans le cadre du contrôle de la proportionnalité. La deuxième partie du rapport (Titre II) va illustrer la tension entre l'approche par les risques et l'approche fondée sur le respect du droit à travers quatre exemples de régulation d'activités numériques. La première exemple concerne la régulation des communications électroniques ; le deuxième la régulation des

plates-formes numériques, notamment pour lutter contre des contenus illégaux ; le troisième exemple concerne la régulation des données à caractère personnel ; le quatrième exemple concerne la régulation de l'intelligence artificielle. Chacun de ces exemples montrera comment les deux approches, l'approche par les risques et l'approche fondée sur le respect des droits, coexistent. Enfin, une conclusion sera présentée dans laquelle je suggère une clé de lecture pour comprendre la coexistence, et la complémentarité, des deux approches dans la régulation des activités numériques.

TABLE DES MATIÈRES **PAGE**

TABLE DES MATIÈRES PAGE

TABLE DES MATIÈRES PAGE

TABLE DES MATIÈRES **PAGE**

PROPOS INTRODUCTIFS

Un parcours de recherche commencé en 2002

Mes activités de recherche scientifique ont débuté en 2002, en parallèle de mon activité d'avocat, avec la publication d'un ouvrage sur le nouveau cadre réglementaire européen pour les communications électroniques[1]. La même année, j'ai défendu un article sur la liberté d'expression sur internet à la conférence *European Communications Policy Research Conference -EuroCPR*[2]. Après 2002, mon intérêt pour la recherche s'est confirmé par la rédaction d'un livre sur la neutralité de l'internet avec Nicolas Curien[3] ainsi que la publication de nombreux articles traitant de la régulation de l'internet, la liberté d'expression et la régulation des données à caractère personnel[4]. En 2012 j'ai défendu à la *Telecommunications Policy Research Conference (TPRC)* un article sur l'utilisation de la méthodologie issue de la régulation des communications électroniques pour créer un cadre cohérent pour lutter contre la contrefaçon en ligne[5]. Cet article m'a donné envie de poursuivre la réflexion sur la régulation des activités numérique dans le cadre d'une thèse de doctorat, que j'ai poursuivie sous la direction du professeur Marc Bourreau à Télécom Paris, dans la discipline analyse économique du droit.

Une activité de recherche à plein temps à partir de 2019 avec des responsabilités d'encadrement

Après ma soutenance de thèse en 2016, j'ai entrepris des démarches pour me consacrer entièrement à la recherche et à l'enseignement. J'ai postulé pour plusieurs postes d'enseignant-chercheur, dont un poste d'enseignant-chercheur en droit et numérique au sein du département sciences économiques et sociales de Télécom Paris. Ma candidature a été retenue

Enseignant-chercheur à plein temps à partir de 2019, j'ai décidé d'orienter mes activités de recherche et d'enseignement vers la régulation de l'intelligence artificielle, un domaine où tout restait à faire. J'ai mis en place un programme interdisciplinaires au sein de Télécom Paris (Operational AI Ethics)

---

[1] W. Maxwell, Electronic Communications : The New European Framework, Oceana Publications (New York 2002)
[2] Créée en 1984, la conférence EuroCPR a cessé d'exister en 2015.
[3] *La neutralité d'Internet*, avec Nicolas Curien, Editions La Découverte, 2011.
[4] Pour une liste des principaux articles dans chaque domaine, voy. infra, sections II-1-c, II-2-e, II-3-i et II-4-e.
[5] *A Regulatory Framework for Dealing with Online Copyright Infringement (OCI), Research Paper presented at the 41st Telecommunications Policy Research Conference (TPRC), Virginia, September 2012.*

pour rassembler les enseignants chercheurs de différents disciplines – maths appliquées, statistiques, informatique, économie, sociologie, droit – autour des questions liées à l'éthique de l'intelligence artificielle. Sous l'impulsion du professeur David Bounie, j'ai rédigé en 2019 une proposition de recherche pour l'Agence National de la Recherche autour de l'intelligence artificielle explicable[6], ainsi qu'un article interdisciplinaire sur l'IA explicable[7]. Cet article, qui rassemble le point de vue de neuf enseignants chercheurs de différents domaines scientifiques à Télécom Paris, a été défendu dans une conférence internationale sur l'IA[8]. Ce travail d'équipe autour de l'explicabilité des algorithmes m'a initié à la richesse, et aux défis, de la réflexion interdisciplinaire. Chaque approche disciplinaire a son vocabulaire propre, ses références, et ses objectifs scientifiques, qu'il faut rendre interopérable, et insérer dans une réflexion scientifique commune. La proposition ANR (XAIforAML) a été retenue. J'ai alors mis en place une équipe et un calendrier d'actions de recherche autour du thème de l'IA explicable pour la détection d'activités de blanchiment de capitaux et de financement du terrorisme (LCB-FT)[9].

En 2020, deux professeurs en mathématiques appliquées, Florence d'Alché-Buc et Stéphan Clémençon, m'ont demandé de prendre en charge le volet régulation d'un deuxième programme de recherche ANR autour des systèmes de reconnaissance d'image dignes de confiance[10]. J'ai alors rédigé une partie de la proposition de recherche pour la demande ANR, et lorsque le projet a été accordé, j'ai recruté une doctorante, Mélanie Gornet, pour commencer une thèse sur les exigences de régulation autour de systèmes de reconnaissance d'images dignes de confiance[11].

En 2020, j'ai initié un programme de recherche avec le groupe Caisse des Dépôts autour de questions liées à l'intelligence artificielle dans l'intérêt public[12].

Sur le plan de l'enseignement, j'ai pris la direction de l'ensemble des enseignements au sein de Télécom Paris et des Masters IP Paris autour de l'IA Éthique. Sur le plan administratif, j'ai pris la

---

[6] https://anr.fr/Project-ANR-20-CHIA-0023

[7] Beaudouin, Valérie and Bloch, Isabelle and Bounie, David and Clémençon, Stéphan and d'Alché-Buc, Florence and Eagan, James and Maxwell, Winston and Mozharovskyi, Pavlo and Parekh, Jayneel, Flexible and Context-Specific AI Explainability: A Multidisciplinary Approach (March 23, 2020). Available at SSRN: https://ssrn.com/abstract=3559477 or http://dx.doi.org/10.2139/ssrn.3559477

[8] Identifying the 'Right' Level of Explanation in a Given Situation, avec Valérie Beaudouin, Isabelle Bloch, David Bounie, Stéphan Clémençon, Florence d'Alché-Buc, Florence, James Eagan, Pavlo Mozharovskyi, et Jayneel Parekh, Proceedings of the First International Workshop on New Foundations for Human-Centered AI (NeHuAI), Santiago de Compostella, Spain, September 4, 2020, CEUR Workshop Proceedings, Vol. 2659, p. 63

[9] infra, section II-4-b-(i)

[10] LIMPID, voy. infra section II-4-b-(ii).

[11] infra, section II-4-b-(ii).

[12] infra, section II-4-b-(iii).

codirection en 2022, avec le professeur David Massé, de l'équipe "Numérique, Organisation et Société[13]" à Télécom Paris.

L'objet du présent mémoire de synthèse

Le présent mémoire de synthèse pour l'habilitation à diriger des recherches a deux finalités. La première consiste à démontrer ma capacité à prendre de la hauteur par rapport à mes propres travaux de recherche, et les structurer autour d'une réflexion scientifique cohérente. Dans ce mémoire, j'essaie de présenter mes travaux de recherche de manière à mettre en évidence la tension entre deux visions de la régulation, l'une axée sur le respect des droits, l'autre axée sur l'analyse des risques. Mes travaux de recherche touchent sans cesse à la cohabitation de ces deux visions au sein de la régulation des activités numériques.

La deuxième finalité consiste à démontrer ma capacité à encadrer la recherche de jeunes chercheurs et animer des programmes de recherche. La présentation des programmes de recherche que je dirige, ou codirige, autour de la régulation de l'IA à Télécom Paris[14] mettront ces capacités en évidence.

Structure du mémoire

Le présent mémoire est divisé en deux parties. La première partie (Titre I) présente ce qu'est une approche par les risques, et une approche fondée sur le respect des droits. Ces deux approches puisent leurs origines dans les traditions philosophiques, l'utilitarisme pour l'approche par les risques, et la déontologie pour l'approche fondée sur le respect des droits. L'approche par les risques est influencée par l'analyse économique et la recherche du bien-être social par la mise en équilibre de différents droits et intérêts sociétaux. L'approche par les droits refuse une telle mise en équilibre car le centre de l'attention n'est pas la maximisation du bien-être collectif, mais les droits de l'individu en tant que tel. Néanmoins, les droits fondamentaux connaissent bien un mécanisme de pondération dans le cadre du contrôle de la proportionnalité.
La deuxième partie du rapport (Titre II) va illustrer la tension entre l'approche par les risques et l'approche fondée sur le respect du droit à travers quatre exemples de régulation d'activités

[13] L'équipe Numérique, Organisation et Société (NOS) fait partie du laboratoire CNRS i3 (Institut interdisciplinaire sur l'innovation UMR 9217). Elle regroupe 12 enseignants-chercheurs permanents en sociologie du numérique, management et droit, 8 doctorants, 5 post-doc, et 4 professeurs invités.
[14] infra section II-4-b

numériques. La première exemple concerne la régulation des communications électroniques ; le deuxième la régulation des plates-formes numériques, notamment pour lutter contre des contenus illégaux ; le troisième exemple concerne la régulation des données à caractère personnel ; le quatrième exemple concerne la régulation de l'intelligence artificielle. Chacun de ces exemples montrera comment les deux approches, l'approche par les risques et l'approche fondée sur le respect des droits, coexistent. La discussion sur la régulation de l'intelligence artificielle mettra en avant les programmes de recherche que j'encadre actuellement à Télécom Paris.

Enfin, une conclusion sera présentée dans laquelle je suggère une clé de lecture pour comprendre la coexistence, et la complémentarité, des deux approches dans la régulation des activités numériques.

TITRE I - PRÉSENTATION DES TENSIONS ENTRE L'APPROCHE PAR LES RISQUES (*RISK-BASED*) ET L'APPROCHE FONDÉE SUR LA PROTECTION DES DROITS (*RIGHTS-BASED*) DANS LE CADRE DE LA RÉGULATION DES ACTIVITÉS NUMÉRIQUES

1. Peut-on traiter les droits fondamentaux dans une analyse de risques ?

L'idée derrière ma thèse de doctorat, soutenue en 2016, était de transposer la méthodologie d'analyse utilisée pour la régulation des communications électroniques à la régulation des activités numériques pour la lutte contre les contenus illicites. La thèse essayait de démontrer qu'il était possible d'analyser les problèmes de contenus illicites de manière similaire à l'analyse des défaillances de marché sur le marché des communications électroniques. Il serait dès lors possible de d'analyser la nécessité et la proportionnalité des différentes options de régulation avec plus de rigueur et de cohérence. La thèse partait du constat que les interventions de l'État pour limiter l'accès à des contenus illégaux manquait de cohérence, les mesures adoptées en matière de lutte contre la contrefaçon étaient différentes des mesures adoptées pour lutter contre les contenus haineux ou pour lutter contre la pédopornographie. Une méthodologie plus explicite permettrait de développer des solutions techniques, et des approches de régulation, plus cohérentes entre ces différents "silos" de régulation de contenus en ligne. La thèse a démontré notamment que l'analyse de risques et le choix des méthodes de régulation les plus adaptés partageaient de nombreux points avec l'analyse de nécessité et de proportionnalité effectuée par la CJUE et la CEDH lorsqu'elles examinent des mesures de régulation, notamment pour lutter contre des contenus illégaux.

La démarche d'analyse de risques se retrouve aujourd'hui dans de nombreux textes de réglementation des activités numériques[15], confirmant ainsi la généralisation de cette technique de régulation. La question centrale est donc comment une approche par les risques - fondée à l'origine par une approche économique et utilisée largement pour la régulation de la sureté d'installations dangereuses[16] - peut intégrer les droits fondamentaux, et plus précisément si une approche par les risques peut cohabiter avec une approche fondée sur le respect des droits (*rights based*). Cette question centrale est explorée dans la plupart de mes recherches sur la liberté d'expression sur

[15] Notamment le RGPD, le règlement européen "Digital Services Act" (DSA), et le futur règlement sur l'intelligence artificielle (IA Act); De Gregorio, Giovanni and Dunn, Pietro, The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age (March 31, 2022). 59(2) Common Market Law Review 2022, 473-500, Available at SSRN: https://ssrn.com/abstract=4071437 or http://dx.doi.org/10.2139/ssrn.4071437

[16] Hopkins, safety case, op. cit.

internet, sur la protection des données à caractère personnel, et sur la régulation de l'intelligence artificielle.

Le mémoire original que je soumets dans mon dossier d'habilitation à diriger des recherches[17] met en évidence la tension entre une vision utilitariste du contrôle humain, une vision fondée sur les risques, et une vision qui considère le contrôle humain comme un droit en tant que tel, quel que soit son utilité, une approche fondée sur le respect des droits. Je démontre pourquoi et comment ces deux visions peuvent, et doivent, coexister. La vision fonctionnelle, utilitariste, du contrôle humain conduira à certaines modalités du contrôle humain, destinées à réduire les erreurs algorithmiques par exemple[18]. La vision fondée sur le respect des droits conduira à d'autres modalités qui ne visent pas nécessairement la correction d'erreurs. Une approche de régulation, notamment au sein du futur règlement IA Act, doit tenir compte de ces deux visions du contrôle humain, et tenir compte du fait que les modalités du contrôle humain ne seront pas forcément les mêmes selon ces deux visions.

Une approche par les risques s'apparente à une mise en équilibre de différents droits fondamentaux et objectifs d'intérêt public afin d'identifier des solutions techniques et de régulation proportionnées. La mise en équilibre de droits et d'objectifs d'intérêt général est au cœur du travail du législateur et des juges. La pratique est ancienne. En revanche, la formalisation et la systématisation de la méthode autour d'une analyse de risques sont plus récentes, ainsi que la délégation de cette démarche aux entreprises régulée. Avec la généralisation d'une méthode s'appuyant sur une analyse de risques, la mise en équilibre des droits et objectifs d'intérêt général suit dorénavant une méthodologie plus explicite et harmonisée. Cette consécration des analyses de risques, même sur les questions de droits fondamentaux, peus occulter la deuxième approche, toute aussi importante, fondée sur le respect des droits.

2. Définition des termes

a. "Réglementation" et "régulation"

[17] W. Maxwell, Le contrôle humain des systèmes algorithmiques - un regard critique sur l'exigence d'un humain dans la boucle, Mémoire original pour présenter l'habilitation à diriger des recherches de l'Université Panthéon-Sorbonne, 5 sept. 2022

[18] W. Maxwell, Un contrôle humain efficace pour détecter les erreurs algorithmiques, in "Un droit de l'intelligence artificielle : entre règles sectorielles et régime général. Perspectives de droit comparé", C. Castets-Renard (ed.), à paraître.

La “réglementation” désigne les mesures contraignantes adoptées par l’État : lois, décrets, arrêtés. Le terme “régulation” est plus large que le terme réglementation, la régulation désignant l’ensemble des systèmes de contraintes organisées autour d’une activité économique pour protéger et/ou promouvoir des objectifs d’intérêt général. Il peut s’agit de mécanismes d’autorégulation, de co-régulation, de soft-law, ou des mesures de réglementation[19].

b. “Activités numériques”, un terme générique, sans définition juridique

Les acteurs du numériques sont définis par de nombreux textes, dont la loi du 21 juin 2004 pour la confiance dans l’économie numérique, la loi du 30 septembre 1986 relative à la liberté de communication, le Code des Postes et des Communications électroniques, et le Code de la Consommation. D’autres définitions émergeront du futur règlement européen sur l’IA. Les questions de définitions dans le monde numérique sont complexes, mais n’ont pas d’impact sur les questions examinées dans ce mémoire. J’ai choisi donc d’utiliser le terme “activités numériques” - qui n’est pas un terme défini juridiquement - pour désigner l’ensemble des activités liées au traitement, à la transmission, et à l’hébergement de signaux numériques, englobant ainsi les activités de communications électroniques, d’hébergement, d’édition de contenus numériques, de traitement de données numériques, de gestion des plateformes, de conception et d’exploitation d’algorithmes.

3. Présentation d’une approche par les risques

a. Une approche de régulation par les risques décrit trois phénomènes

Une “approche de régulation fondée sur les risques” décrit trois phénomènes distinctes[20] :

1) Une analyse d’impact est effectuée avant l’adoption d’une réglementation pour vérifier sa nécessité, et l’absence d’effets secondaires excessifs. Cet aspect se retrouve dans l’approche “mieux légiférer” poursuivie aux États-Unis et en Europe fondée, comme nous le verrons[21], sur une analyse économique de la régulation ;

[19] Conseil d’État, Rapport public 2001, les autorités administratives indépendantes, p. 279.
[20] Black, Julia. "Risk-based regulation: choices, practices and lessons being learnt." (2010): 185-224; OCDE, “Risk and regulatory policy : improving the governance of risk”, 2010.
[21] infra, section I-3-c

2) L'analyse de risque permet de prioriser des mesures d'enquête et de contrôle par les autorités de régulation. L'administration utilise une approche par les risques pour optimiser l'utilisation des ressources publics[22] ;
3) L'analyse de risque est effectuée par un régulateur, ou par l'entreprise régulée, ou par les deux, pour définir les mesures de prévention devant être mise en place pour diminuer les risques identifiés.

Cette dernière approche est celle qui m'intéresse dans le cadre de la régulation d'activités numériques. Elle implique souvent une forme de co-régulation : un programme de gestion de risques est mis en place par un acteur privé à la suite d'une obligation légale. Le programme de risque est ensuite contrôlé, parfois corrigé, par un régulateur[23]. Une partie de la tâche de régulation est ainsi déléguée aux entreprises elles-mêmes, ces dernières étant mieux placées que l'État pour analyser les risques de leurs propres activités. Cette méthode de régulation soulève évidemment des risques de conflit d'intérêts[24], car l'entreprise aura naturellement tendance à sous-estimer certains risques, ou à proposer des méthodes de prévention moins coûteuses que celles qu'aurait choisi l'administration.

b. L'approche par les risques est une recherche d'efficacité économique fondée sur la tradition "*law & economics*", mais une recherche d'efficacité contestée

Dans les années 1980, l'analyse économique du droit (*law & economics*) s'insérait dans presque toutes des disciplines du droit : responsabilité civile délictuelle (*torts*), contrats, droit pénal, droit de la propriété[25], procédure civile, responsabilité pour les produits défectueux. Selon l'approche *law & economics*, les décisions de la *common law* tendent à encourager une organisation efficace de la société, en envoyant des signaux aux acteurs économiques pour encourager des comportements responsables, et décourager des comportements excessifs. La formule du juge Learned Hand[26] nous permet d'identifier le niveau optimal de mesures de prévention attendu d'une victime pour éviter ou minimiser les dommages, ainsi que le niveau de prudence attendu de l'auteur d'un dommage. Le principe de "*proximate cause*" nous conduit à allouer la responsabilité à l'acteur qui est en mesure d'éviter le dommage à moindre coût (*least cost avoider*), ou à celui qui est le mieux placé pour

---

[22] Conseil d'État, Les pouvoirs d'enquête de l'administration, Étude, avril 2021.
[23] Rothstein, Henry, et al. "The risks of risk-based regulation: Insights from the environmental policy domain." *Environment international* 32.8 (2006): 1056-1065.
[24] Gellert, Understanding the notion of risk in the General Data Protection Regulation, 34 Computer Law & Security Review (2018), p. 280.
[25] Barzel, Y. (1989), Economic Analysis of Property Rights, Cambridge U. Press.
[26] *U.S. v. Carroll Towing*, 159 F.2d 169 (2d Cir. 1947); Posner, R.A. (2011), Economic Analysis of Law, Aspen Casebook Series, 8 th Edition.

s'assurer contre le dommage. Dans les années 1980, les écrits de Richard Posner[27] façonnaient la perception du rôle du droit dans la société. Pour Posner, le droit est un outil pour maximiser le bien-être social (*social welfare*), et l'efficacité du droit se mesure par rapport à cet objectif. Cette tradition s'inspire des écrits de John Stuart Mill[28] et de Jeremy Bentham[29] et se retrouve actuellement dans la manière de réguler les risques[30].

L'ensemble de mes professeurs ne partageaient pas ce point de vue. Robert Summers soulignait les valeurs non-quantifiables, liées au droit lui-même : des "*process values*" par opposition aux "*instrumental values*" de la loi[31]. Selon Summers, une loi peut avoir un double rôle : un rôle d'instrument pour atteindre un objectif, tel que la manifestation de la vérité dans un procès, et un rôle de préservation de valeurs humaines liée à l'existence de la loi elle-même. Le deuxième rôle est indépendant de l'efficacité de la loi dans son premier rôle. Dans le cadre de ce deuxième rôle, on considère la loi comme une valeur en soi. Pour Summers, les *"process values",* avec leurs inefficacités, sont nécessaires à une société démocratique[32]. Ce thème a été repris récemment par Paul Nemitz dans le cadre de la proposition de règlement européen sur l'IA[33]. Nemitz rappelle l'importance de compromis et d'ambiguïtés dans les textes de lois, incarnation de processus démocratiques profondément humains.

Les deux visions de la loi - la loi comme instrument, et la loi en tant que valeur autonome - se retrouvent dans les deux approches de régulation mentionnées ci-dessus : une régulation fondée sur les risques (*risk-based*), et une régulation fondée sur la protection des droits (*rights based*). Une approche par les risques obéit généralement à une logique de maximisation de bien-être social, alors qu'une approche fondée sur la protection des droits va se focaliser sur le droit en tant que valeur autonome, digne de protection sans considération des coûts.

---

[27] Landes, W. and R. Posner (1987), The Economic Structure of Tort Law, Harvard University Press; Posner, R.A. (2011), Economic Analysis of Law, op. cit.; Posner, R.A. (1978), An Economic Theory of Privacy, Regulation, May/June; Ehrlich, I. and R. Posner (1974), An Economic Analysis of Legal Rulemaking, 3 J. of Leg. Studies 257.

[28] Mill, John Stuart. *Utilitarianism* (1863). Second Edition. Edited by George Sher. Indianapolis: Hackett Publishing Company Inc., 2002.

[29] Bentham, Jeremy. *An Introduction to the Principles of Morals and Legislation* (1789). New York: Dover Publications, 2007.

[30] Coglianese, The Law and Economics of Risk Regulation, U. of Penn., Institute for Law & Economics Research Paper n° 20-18 (2020).

[31] RS Summers, Evaluating and Improving Legal Processes - A Plea for "Process Values", 60 Cornell L. Rev. 1, 12 (1974)

[32] Ce point est développé dans mon Mémoire HDR : W. Maxwell, Le contrôle humain des systèmes algorithmiques - un regard critique sur l'exigence d'un humain dans la boucle, Mémoire original pour présenter l'habilitation à diriger des recherches de l'Université Panthéon-Sorbonne, 5 sept. 2022.

[33] Nemitz, P. Democracy through law The Transatlantic Reflection Group and its manifesto in defence of democracy and the rule of law in the age of "artificial intelligence". *Eur Law J*. 2021; 1- 12. doi:10.1111/eulj.12407, p. 3

Certains auteurs de *law & economics* considèrent que les droits, y compris les *process values auxquelles* fait référence Summers, sont compatibles avec une approche par les risques[34]. Les droits font partie de l'équation bien-être social[35]. Holmes et Sunstein[36] démontrent même que les droits fondamentaux ont un prix, car ils dépendent pour leur existence de l'état de droit : policiers, magistrats, et d'un système de gouvernement et de taxation sans corruption. D'autres économistes démontrent qu'il est possible de quantifier certains droits, la protection de l'environnement par exemple, et intégrer ces chiffres dans une analyse coûts-bénéfices[37]. Sunstein souligne le rôle expressif et symbolique de la loi[38].

c. L'approche par les risques et la "science régulatoire"[39]

Selon une approche purement économique, la raison d'être de la régulation est de traiter des défaillances du marché qui ne peuvent être traitées par le droit de la concurrence seul. Cette approche économique de la régulation a inspiré le mouvement "mieux réguler" (*better regulation*)[40] défendu notamment par Stephen Breyer[41] et Cass Sunstein[42] aux États-Unis. Selon ce mouvement, une réglementation doit être précédée d'une analyse de marché, une définition précise du problème, et l'examen de plusieurs options de régulation, en comparant les coûts et les bénéfices de chaque option[43]. Ce mouvement a été repris par le gouvernement américain lorsqu'il a créé l'OIRA (Office of Information and Regulatory Affairs) en 1980[44], et par la Commission européenne en 2015 lorsqu'elle a créé le Regulatory Scrutiny Board et sa boîte à outil d'une meilleure régulation[45]. L'accord interinstitutionnel "mieux légiférer" de l'Union Européenne met en avant la nécessité de rendre la législation de l'UE le plus efficace et effective que possible dans l'atteinte des objectifs

---

[34] Mialon, H. and P. H. Rubin (2007), The Economics of the Bill of Rights, Emory Law and Economics Research Paper No. 07-15.
[35] Kaplow, L. and S. Shavell (2006), Fairness versus Welfare, Harvard University Press.
[36] Holmes, S. and C.R. Sunstein (2013), The Cost of Rights – Why Liberty Depends on Taxes, W.W. Norton & Company.
[37] Ackerman, F. and L Heinzerling (2002), Pricing the Priceless: Cost-Benefit Analysis of Environmental Protection, 150 U. of Penn. L. Rev. 1553.
[38] Sunstein, C.R. (1996), On the Expressive Function of Law, 144 U. of Penn. L. Rev. 2021.
[39] ENBOUZID Bilel, CARDON Dominique, « Contrôler les IA », *Réseaux*, 2022/2-3 (N° 232-233), p. 9-26.
[40] Baldwin, R. (2010), Better Regulation: the Search and the Struggle, in R. Baldwin, M. Cave and M. Lodge (ed.) Oxford Handbook of Regulation, p. 270; Graham, J.D. (2008), Saving Lives through Administrative Law and Economics, 157 U. Penn. L.Rev. 395.
[41] Breyer, S. (1982), Regulation and its Reform, Harvard University Press.
[42] Sunstein, C.R. (1996), Congress, Constitutional Moments, and the Cost-Benefit State, 48 Stanford L. Rev. 247.
[43] Cecot, C., R. Hahn, A. Renda, L. Schrefler (2007), "An Evaluation of the Quality of Impact Assessment in the European Union with Lessons for the U.S. and the EU", Working Paper, AEI-Brookings Joint Center for Regulatory Studies, December.
[44] White House Executive Order 12291.
[45] European Commission (2015), Better Regulation Guidelines, Commission Staff Working Paper, SWD(2015) 111 final, May 19.

stratégiques communs de l'Union[46]. Il s'agit d'une approche utilitariste[47], où chaque régulation est jugée selon son efficacité à réduire un risque bien identifié, tenant compte des coûts des mesures de régulation, de leurs effets bénéfiques, mais aussi de leurs effets collatéraux[48]. Une étude d'impact est au cœur de cette démarche, et l'efficacité est le principal critère de la démarche - un maximum d'effet bénéfique pour la société pour un minimum de coûts[49].

Cette recherche du bien-être social laisse naturellement la place à des compromis. On accepte de réduire un risque à un niveau "acceptable"[50], car réduire le risque à zéro serait excessif, conduisant parfois à l'arrêt total d'une activité qui génère par ailleurs des bénéfices importants pour la société[51]. Une approche fondée sur les risques accepte de s'attaquer en priorité aux risques les plus grands, en laissant de côté, au moins temporairement, les risques moins élevés dans un souci d'efficacité. On cherche à concentrer les efforts de prévention là où ils auront le plus d'impact. L'identification et la priorisation des risques "accroît l'efficacité de l'utilisation des ressources par les services étatiques et renforce l'efficacité globale des mesures[52]".

d. L'approche par les risques recherche l'efficacité, mais pour atteindre quel but ?

Appliquer une approche fondée sur les risques réduit les questions de conformité et de respect des droits à une question d'efficacité. Mais quelle efficacité, et pour quels objectifs ? Être efficace signifie produire l'effet qu'on attend[53], voire produire le maximum de résultats avec le minimum d'effort, de dépense[54]. Une loi efficace est une loi qui qui atteint les objectifs fixés par le législateur. Vue sous cet angle, une loi serait un simple outil permettant d'atteindre un objectif prédéfini, à l'instar d'un algorithme. Une loi efficace chercherait à atteindre l'objectif avec un minimum de coûts. Comme un ouvrage d'art bien conçu, une bonne loi résisterait au temps, serait suffisamment souple pour

---

[46] Accord Interinstitutionnel du 13 avril 2016, "Mieux légiférer", considérant 2.
[47] Byskov, Morten Fibieger. "Utilitarianism and risk." *Journal of Risk Research* 23, no. 2 (2020): 259-270. https://doi.org/10.1080/13669877.2018.1501600.
[48] Hutter, "A Risk regulation Perspective on Regulatory Excellence" in Coglianese (ed.), Achieving Regulatory Excellence (Brookings Institution Press, 2017), pp. 101-114
[49] Sur les cadres américains et européens de "better regulation", voy. W. Maxwell, *Smart(er) Internet Regulation Through Cost-Benefit Analysis - Measuring harms to privacy, freedom of expression, and the internet ecosystem*, Presses des Mines, 2017.
[50] *Les mesures appropriées et analyses de risques dans le RGPD*, La Revue du DPO, Rétrospective 2018, Université Paris 1, Mars 2019, pp 17-30, avec D. Ouandji.
[51] De Gregorio, Giovanni and Dunn, Pietro, The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age (March 31, 2022). 59(2) Common Market Law Review 2022, 473-500, Available at SSRN: https://ssrn.com/abstract=4071437 or http://dx.doi.org/10.2139/ssrn.4071437
[52] Conseil de l'Europe, Comité d'Experts sur l'évaluation de mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme, Approche fondée sur les risques, https://www.coe.int/fr/web/moneyval/implementation/risk-based-approach, consultée le 10 octobre 2022
[53] Dictionnaire en ligne de l'Académie française, consulté le 20 octobre 2022.
[54] Dictionnaire Le Robert en ligne, consulté le 20 octobre 2022.

s'adapter aux changements dans l'environnement, et serait élégante, à savoir accessible et compréhensible par le citoyen[55]. Lorsqu'une loi cesserait d'être utile, elle serait démantelée, comme un vieux pont.

A chaque loi correspond un ou plusieurs objectifs définis par le législateur : augmenter la concurrence et réduire les prix, promouvoir l'innovation, réduire les discriminations, traquer la fraude, lutter contre la pédopornographie, préserver le débat démocratique. L'efficacité d'une loi pourrait se mesurer par rapport à l'atteinte de chacun de ces objectifs pris séparément. Pour préserver l'efficacité de la loi dans le temps, le législateur pourrait prévoir la création d'une réglementation spécifique pour compléter la loi, et un régulateur spécialisé, aux manettes pour ajuster le trajectoire de la régulation en fonction des retours d'information. Une grande partie de la régulation des activités numériques est fondée sur ce modèle. La loi fixe les grands principes, et un régulateur spécialisé les applique de manière dynamique, en fonction des retours d'information[56].

e. L'approche par les risques s'appuie sur les traditions de l'utilitarisme

Une approche utilitariste conduira à la conclusion que l'on peut condamner une personne pour en sauver cinq. Ce choix utilitariste est souvent présenté dans le contexte du dilemme du tramway[57]. S'appuyant sur les théories de Mill[58] et de Bentham[59], les utilitaristes rechercheront la maximisation du bonheur collectif, parfois au détriment du bonheur individuel. Les analyses de risques sont parfaitement adaptées à cette vision du bien-être collectif[60].

4. Présentation de l'approche fondée sur le respect des droits : une vision plus absolue, pour défendre l'inquantifiable

a. Un respect des droits non-négociable

Une approche fondée sur la protection des droits se concentre sur le seul objectif de protection des droits et libertés individuels, sans prise en compte d'un bilan économique coûts/bénéfices[61].

---

[55] Conseil d'État, Simplification et qualité du droit, Étude 2016.
[56] Conseil d'État, Autorités administratives indépendantes, op cit.
[57] Philippa Foot, « The Problem of Abortion and the Doctrine of the Double Effect », *Virtues and Vices*, Oxford, Basil Blackwell, 1978première édition : *Oxford Review*, numéro 5, 1967.
[58] Mill, John Stuart. *Utilitarianism* (1863). Second Edition. Edited by George Sher. Indianapolis: Hackett Publishing Company Inc., 2002.
[59] Bentham, Jeremy. *An Introduction to the Principles of Morals and Legislation* (1789). New York: Dover Publications, 2007.
[60] Byskov, Morten Fibieger. "Utilitarianism and risk." *Journal of Risk Research* 23, no. 2 (2020): 259-270. https://doi.org/10.1080/13669877.2018.1501600; Parfit, Derek. *Reasons and Persons*. Oxford: Oxford University Press, 1984.
[61] Sander, Barrie. "Freedom of expression in the age of online platforms: The promise and pitfalls of a human rights-based approach to content moderation." *Fordham Int'l LJ* 43 (2019): 939.

L'approche fondée sur les droits considère le droit individuel comme méritant une protection forte, voire absolue, même aux dépens de l'intérêt collectif[62]. Une approche fondée sur la protection des droits n'admet pas une négociation en fonction de l'évaluation quantitative de risques[63].

En particulier, l'approche fondée sur le respect des droits (*rights-based*) refuse de considérer la violation d'un droit fondamental comme une unité quantifiable pouvant être mise en balance dans une analyse de risque. Il n'existerait pas de "petite" ou de "grande" violation d'un droit fondamental. Toute violation serait condamnable, et aucune violation ne pourrait être tolérée dans une recherche d'efficacité économique. Laisser de côté certains risques pour se concentrer sur d'autres plus importants, constituerait une discrimination intolérable envers les victimes des "petits" risques.

Ainsi, incorporer la violation de droits fondamentaux dans un système d'analyse de risques serait pour certains un non-sens[64]. Selon Smuha et al., "pour garantir le respect de droits fondamentaux pour toutes personnes en vertu de leur humanité, les droits fondamentaux ont un poids particulier dans l'architecture de protection des droits, un poids qui reconnaît que de tels droits ne se réduisent pas à des 'intérêts' d'individus à mettre en 'équilibre' avec les intérêts d'autres individus, voire les intérêts collectifs.[65]"

b. **Une approche ancrée dans les droits naturels d'Immanuel Kant**[66]

L'approche fondée sur le respect des droits s'appuie sur une vision déontologique des droits et devoirs. Aux États-Unis, cette tradition s'appelle le "rights tradition"[67], défendue notamment par John Rawls et Ronald Dworkin. Cette vision des droits refuse d'admettre qu'une personne puisse faire l'objet d'une exploitation sans son consentement, même si cela procure un bénéfice pour la collectivité[68]. Pour Schroeder, l'approche par les droits doit "reconnaître et préserver les

---

[62] Smuha, N.A. Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea. *Philos. Technol.* 34 (Suppl 1), 91–104 (2021). https://doi.org/10.1007/s13347-020-00403-w

[63] Johnson, S. Racing into the fourth industrial revolution: exploring the ethical dimensions of medical AI and rights-based regulatory framework. *AI Ethics* 2, 227–232 (2022). https://doi.org/10.1007/s43681-022-00153-9

[64] Yeung, Karen & Bygrave, Lee. (2021). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. Regulation & Governance. 16. 10.1111/rego.12401; Gellert, Raphaël, 'Introduction: The risk-based approach as the opposite of the rights-based approach, or as an opportunity to analyse the links between law, regulation, and risk?',The Risk-Based Approach to Data Protection (Oxford, 2020; online edn, Oxford Academic, 22 Oct. 2020), https://doi.org/10.1093/oso/9780198837718.003.0001,

[65] Smuha, Nathalie A. and Ahmed-Rengers, Emma and Harkens, Adam and Li, Wenlong and MacLaren, James and Piselli, Riccardo and Yeung, Karen, How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act (August 5, 2021), p. 10, traduit par moi.Available at SSRN: https://ssrn.com/abstract=3899991 or http://dx.doi.org/10.2139/ssrn.3899991

[66] Je remercie Joshua Brand, doctorant à Télécom Paris, pour son aide dans les sections touchant à la philosophie.

[67] C.H. Schroeder, Rights against Risks, 86 Columbia L. Rev. 495 (1986).

[68] G. Calabresi et P. Bobbitt, Tragic Choices 39 (1978).

caractéristiques d'individus en tant qu'agents moraux libres et autonomes. Selon cette approche, l'individu est défini avant de définir les conditions selon lesquelles l'individu pourra faire l'objet d'interventions… ces conditions [seront] définies de manière à protéger et préserver ce qui est essentiel à l'individu.[69]"

c. Les droits pourtant mis en équilibre dans le contexte du contrôle de la proportionnalité

Cette vision absolutiste du respect des droits cache cependant une nuance qui tend à rapprocher la vision *rights-based* et la vision *risk-based*. Certains droits fondamentaux ne sont pas absolus, et peuvent, dans certaines conditions définies à l'article 52(1) de la Charte, être mis en équilibre avec d'autres droits et objectifs d'intérêt publique. Cette mise en équilibre vérifie notamment le caractère nécessaire et proportionné d'une ingérence. En m'appuyant sur les travaux de Portuese[70], j'ai essayé d'identifier les points communs entre les tests de nécessité et de proportionnalité appliqués par la CJUE et les étude coûts-bénéfices[71]. Certes, les droits et les ingérences ne sont pas quantifiés dans une démarche de proportionnalité, mais leur gravité est caractérisée, et une pondération équitable est recherchée. La recherche de proportionnalité serait ainsi un autre moyen de rechercher l'équilibre, exprimé en termes économique par la maximisation du bien-être social.

Cette tentative d'insérer les droits fondamentaux dans une recherche de bien-être économique se heurte au problème de la quantification, quasi impossible, des droits fondamentaux. Elle ignore également l'aspect déontologique des droits en tant qu'expressions de valeurs non-négociable.

5. La nécessaire cohabitation des deux approches

Percevoir la loi seulement à travers le prisme de l'efficacité masquerait une autre dimension de la loi toute aussi importante, à savoir le rôle de la loi dans préservation de certaines valeurs, parfois génératrices d'inefficacité. Au lieu de voir le droit comme une série d'ouvrages d'ingénierie, chaque loi obéissant à ses propres règles d'ingénierie avec ses propres objectifs et critères d'efficacité, on pourrait considérer les lois comme faisant partie d'un écosystème qui tient ensemble grâce, en partie, à ses multiples contradictions et inefficacités. Pour Paul Nemitz, une loi parfaite, et

[69] Schroeder, op cit., p. 509.
[70] Portuese, A. (2013), Principle of Proportionality as Principle of Economic Efficiency, 19 European L.J. 612; De Vries, S. (2013), Balancing of Fundamental Rights with Economic Freedoms According to the European Court of Justice, 9 Utrecht L. Rev. 169.
[71] A Method to Assess Regulatory Measures Designed to Limit Access to Harmful Content on the Internet (October 4, 2016). Available at SSRN: https://ssrn.com/abstract=3558490

parfaitement efficace dans son application, serait un signe de fascisme[72]. Une recherche excessive de l'efficacité au sein d'une seule loi, dans la lutte contre le terrorisme par exemple, nuirait à écosystème dans son ensemble, un écosystème que Karen Yeung appelle les "*democratic commons*"[73]. Cet écosystème échappe en grande partie à la vision et à l'action d'un seul régulateur spécialisé. Pour certains, il peut même échapper à une analyse fondée uniquement sur la protection des droits individuels. Pour Benbouzid et al., "il n'y a pas toujours une relation univoque entre un droit individuel et un préjudice sociétal[74]". La protection de l'écosystème relève plutôt du travail des généralistes du droit, tels que les tribunaux et le législateur[75].

L'approche *risk-based* tend vers une efficacité économique ; l'approche *rights-based* tend vers une proportionnalité dans le respect des droits et dans les ingérences nécessaires pour protéger d'autres droits. La régulation des activités numériques doit tenir compte de ces deux approches, en recherchant une efficacité adéquate, mais non-excessive, et respectueuse des droits. De Gregorio et Dunn décrivent les deux approches, celle par les risques et celle fondée sur le respect des droits, ainsi :

> "...l'approche fondée sur le respect des droits et l'approche par les risques peuvent se rattacher respectivement à un modèle de régulation traditionnel du haut vers le bas ("command and control"), et un modèle de régulation appelé "meta-regulation", une sous-catégorie du modèle de régulation fondé sur les principes ("principles based"), selon lequel l'objectif est d'encourager l'industrie à mettre en place ses propres systèmes de gestion qui sont ensuite contrôlés par le régulateur.[76]"

Les auteurs proposent une approche hybride, fondée sur les risques mais qui tient également compte de droits constitutionnels.

---

[72] Nemitz, P. Democracy through law The Transatlantic Reflection Group and its manifesto in defence of democracy and the rule of law in the age of "artificial intelligence". *Eur Law J*. 2021; 1- 12. doi:10.1111/eulj.12407, p. 3

[73] Yeung, Karen & Bygrave, Lee. (2021). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. Regulation & Governance. 16. 10.1111/rego.12401 ; Gellert R (2015) Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative. International Data Privacy Law 5, 3–19.

[74] Benbouzid, Bilel, Yannick Meneceur, et Nathalie Alisa Smuha. « Quatre nuances de régulation de l'intelligence artificielle. Une cartographie des conflits de définition », *Réseaux*, vol. 232-233, no. 2-3, 2022, pp. 29-64, p. 50.

[75] Yeung, Karen, Constitutional Principles in a Networked Digital Society (March 3, 2022). Available at SSRN: https://ssrn.com/abstract=4049141 or http://dx.doi.org/10.2139/ssrn.4049141

[76] De Gregorio, Giovanni and Dunn, Pietro, The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age (March 31, 2022). 59(2) Common Market Law Review 2022, 473-500, Available at SSRN: https://ssrn.com/abstract=4071437 or http://dx.doi.org/10.2139/ssrn.4071437, traduction par moi.

Nemitz, pourtant un fervent défendeur de l'approche rights-based, propose néanmoins d'imposer aux acteurs économiques l'obligation d'effectuer une analyse d'impacts sur les droits fondamentaux, une démarche qui contribuera à une nouvelle culture de responsabilisation dans la préservation de la démocratie, l'état de droit et des droits fondamentaux[77].

Dans les exemples qui suivent, nous essaierons d'identifier les zones de cohabitation entre l'approche par les risques et l'approche fondée sur le respect des droits dans le domaine de la régulation des activités numériques. Dans la conclusion émergera une suggestion pour rendre compatibles entre-elles les deux approches.

[77] Nemitz, Paul, Constitutional democracy and technology in the age of artificial intelligence, Phil. Trans. R. Soc. A. 376, 2018, p. 12.

TITRE II - ILLUSTRATIONS, À TRAVERS QUATRE THÉMATIQUES, DE LA COEXISTENCE D'UNE APPROCHE PAR LES RISQUES ET D'UNE APPROCHE FONDÉE SUR LE RESPECT DES DROITS

Mes activités de recherche depuis 2002 se sont organisées autour de quatre thématiques :

1. Les modes de régulation des communications électroniques, et notamment de la neutralité de l'internet (§ II-1 infra) ;
2. Les approches de mise en équilibre de la liberté d'expression sur les plateformes et la protection d'autres droits, tels que le respect du droit d'auteur et la protection des enfants (§ II-2 infra) ;
3. La régulation des données à caractère personnel dans le cadre d'activités numériques (§ II-3 infra) ;
4. La régulation de l'intelligence artificielle, et en particulier la recherche d'équilibre entre la performance algorithmique, la transparence, et la présence de discriminations (§ II-4 infra).

Ces quatre thématiques mettent en évidence une question commune, liée au mode de régulation des activités numériques, et en particulier l'utilisation croissante d'une approche par les risques. Le cadre réglementaire pour les communications électroniques (thématique 1) s'appuie sur une analyse de marché pour définir les problèmes devant faire l'objet d'une intervention de l'État. Après cette analyse, le régulateur doit examiner plusieurs options de régulation pour traiter ces problèmes, et choisir l'option qui crée le moins de distorsions possibles sur le marché, tout en restant efficace. Cette méthodologie s'inspire du droit de la concurrence, et des tendances émergentes aux États-Unis et en Europe pendant les années 1990 de s'appuyer sur les analyses d'impacts pour justifier de la nécessité d'une mesure de régulation. Les analyses d'impacts, appelé aussi analyses de risques, viennent à l'origine de la régulation des installations dangereuses[78]. Petit à petit, une approche de régulation fondée sur une analyse des risques s'est généralisée au sein de la régulation des activités numériques. On retrouve les analyses d'impact, et une approche par les risques, dans la régulation des plateformes dans la lutte contre les contenus illégaux (thématique 2), la régulation des données à caractère personnel (thématique 3), et la régulation de l'intelligence artificielle (thématique 4).

[78] A Hopkins (2012). 'Explaining the "safety case"', *Regulatory Institutions Network*, Working Paper 87. Available athttp://www.csb.gov/assets/1/7/WorkingPaper_87.pdf, cité dans Yeung, Karen and Howes, Andrew and Pogrebna, Ganna, AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing (June 21, 2019). in M Dubber and F Pasquale (eds.) The Oxford Handbook of AI Ethics, Oxford University Press (2019) , Available at SSRN: https://ssrn.com/abstract=3435011 or http://dx.doi.org/10.2139/ssrn.3435011

1. Première thématique : la régulation des communications électroniques

a. La régulation asymétrique : une approche par les risques fondée sur une analyse du marché

A la fin des années 1990, les États-Unis et l'Europe ont entamé un processus de libéralisation des réseaux et services de télécommunications, et cette libéralisation s'est accompagnée d'une nouvelle réglementation technique pour accompagner l'introduction de nouveaux opérateurs. Cette réglementation était appliquée par des autorités de régulation spécialisées, la Federal Communications Commission aux États-Unis, l'Autorité de régulation des télécommunications, le prédécesseur de l'ARCEP, en France. La loi confiait à ces régulateurs la mission de concilier plusieurs objectifs : encourager la concurrence, encourager l'investissement dans les réseaux, et préserver le service universel. En majorité ingénieurs, les régulateurs des télécommunications appliquaient les textes afin de maintenir l'équilibre entre différents objectifs, à l'instar de pilotes d'avion recherchant un trajectoire optimal. Pour maintenir le cap, les régulateurs se nourrissent en permanence d'informations sur l'efficacité de leurs actions. Ils reçoivent des déclarations d'opérateurs et créent des observatoires sur l'état du marché : niveaux de prix, nombre de concurrents, parts de marché, nombre d'abonnements, état des réseaux.

La libéralisation des réseaux et services s'est accompagnée de mesures de régulation de deux types : une régulation asymétrique visant uniquement les opérateurs historiques, et une régulation symétrique visant l'ensemble des opérateurs, qu'ils soient petits ou grands. La dichotomie entre régulation symétrique et asymétrique a été reprise dans la régulation des plateformes. Les règlements DMA et DSA imposent des obligations renforcées aux plateformes structurantes.

La régulation asymétrique a été mise en place pour permettre aux nouveaux entrants d'accéder à certains services et infrastructures contrôlés par les opérateurs historiques. Ces mesures créaient des ingérences importantes dans le droit de propriété de l'opérateur historique, et potentiellement un frein à l'investissement par celui-ci. Pour respecter l'équilibre entre l'encouragement de la concurrence, le respect du droit de la propriété, et des incitations à l'investissement de part et d'autre, la directive "cadre" a organisé une méthode de régulation qui s'appuie sur une analyse du marché, et sur la sélection de mesures de régulation qui permettent de concilier plusieurs objectifs contradictoires. Il s'agit du premier exemple à ma connaissance d'une approche de régulation des activités numériques qui se fonde sur une analyse de marché et sur le choix de mesures de régulation qui tentent de répondre, de manière proportionnée, aux défaillances révélées lors de l'analyse du marché. Cette méthode découle de ce que Benbouzid et Cardon appellent la "science

régulatoire[79]", une approche fortement ancrée dans des analyses d'impact, et la comparaison systématique de plusieurs options de régulation, y compris l'option de ne rien faire, pour choisir l'option de régulation qui est efficace sans créer trop d'effets indésirables. Les analyses d'impact en matière de régulation des communications électroniques m'ont impressionné par leur rigueur. Chaque analyse était revue par un service spécialisé de la Commission européenne, et les choix proposés par les autorités nationales de régulation contestée. Les services de la Commission s'efforcer d'assurer que les outils de régulation asymétriques à la disposition des autorités nationales seraient déployés avec réserve, de préférence au niveau des services de gros afin de ne pas perturber le bon fonctionnement du marché de détail.

Dans ce domaine de régulation asymétrique du marché des communications électronique, l'approche fondée sur le respect des droits est inexistante. Tout est susceptible de rentrer dans une analyse coûts/bénéfices et faire l'objet de pondérations. Seule compte le résultat : la recherche d'une intervention optimale de l'État pour favoriser l'émergence d'une concurrence durable sur le marché des communications électroniques. Cette méthodologie de régulation s'inspire des principes de "*better regulation*" qui reconnaissent qu'une mesure de régulation doit cibler un problème (généralement une défaillance de marché) spécifique, qu'elle ne doit pas créer des effets indésirables excessifs, et qu'elle doit être retirée dès qu'elle n'est plus nécessaire. Cette méthode est dynamique, devant s'adapter en permanence en fonction des évolutions du marché.

La régulation symétrique, elle, n'est pas dynamique. Elle s'applique, de manière stable, à tous les acteurs du secteur. Cette régulation vise à protéger les consommateurs, la sécurité des réseaux, le financement du service universel, et l'accès aux ressources de l'État (droits de passage, spectre radioélectrique). Elle vise également à garantir la neutralité de l'internet[80].

b. La régulation de l'internet ouvert : une approche fondée sur le respect des droits

La technologie internet a permis aux services et aux applications d'échapper complètement au contrôle de l'opérateur de réseau. Celui-ci a vu son rôle réduit à celui d'un simple transporteur de signaux. La valeur des services, que ce soit pour la téléphonie, la vidéo, les services *cloud*, s'est concentrée aux extrémités des réseaux, échappant ainsi au contrôle de l'opérateur, et ceci au moment où celui-ci devait investir massivement dans la fibre et dans les nouvelles technologies

---

[79] ENBOUZID Bilel, CARDON Dominique, « Contrôler les IA », *Réseaux*, 2022/2-3 (N° 232-233), p. 9-26. DOI : 10.3917/res.232.0009. URL : https://www.cairn.info/revue-reseaux-2022-2-page-9.htm

[80] N. Curien et W. Maxwell, *La neutralité d'Internet*, Editions La Découverte, 2011.

mobiles (3G, 4G, 5G). Il était tentant pour les opérateurs d'ériger des barrières de péage, pour percevoir une commission, même petite, pour chaque transaction conclue par les internautes utilisant le réseau, à l'instar du modèle des câblo-opérateurs qui distribuent des services audiovisuels[81]. L'incitation économique était donc forte pour les fournisseurs d'accès de chercher à monétiser leurs services auprès des prestataires aux extrémités des réseaux, notamment les GAFAM, qui profitent grassement de l'ensemble des services fournis aux internautes. Mais pour négocier avec ces prestataires, il faut avoir la possibilité de bloquer ou ralentir leurs services si les négociations échouent. Cela signifierait la fin de ce que constitue la magie de l'internet[82], à savoir la possibilité pour chacun de proposer n'importe quels services ou contenus aux internautes du monde entier, sans négocier un droit de passage avec chaque opérateur en bout de chaîne.

En 2010 le régulateur américain a tenté pour la première fois d'imposer le principe de neutralité de l'internet, un principe qui interdirait toute discrimination ou blocage de services ou de contenus par les opérateurs en bout de chaîne, à savoir ceux qui proposent l'accès internet à leurs abonnés. Seules seraient permises des mesures nécessaires pour la bonne gestion du réseau. Le régulateur américain a retiré son règlement après les élections présidentielles de 2016[83], mais le principe de l'internet ouvert a été repris par le législateur dans plusieurs états, dont la Californie[84]. En Europe, le règlement 2015/2120 du 25 novembre 2015 sur l'internet ouvert reprend les mêmes principes.

La neutralité de l'internet pourrait être vue simplement comme un outil pour prévenir des pratiques anticoncurrentielles. A l'origine, la régulation avait un objectif économique : empêcher le fournisseur d'accès de favoriser ses propres services[85]. Mais l'intérêt de la régulation comme un outil de la liberté d'expression a rapidement pris le dessus. Plus qu'un règlement économique, le règlement sur l'internet ouvert est une garantie de protection de la liberté d'expression à l'égard de l'un des acteurs les plus puissants dans la chaine de transmission, le fournisseur d'accès qui contrôle les derniers

---

[81] CSA Lab, Le distributeur de services audiovisueLs à L'ère numérique : statut juridique et activité économique, juin 2017.
https://www.csa.fr/Informer/Collections-du-CSA/Perspectives-numerique/Le-distributeur-de-services-audiovisuels-a-l-ere-numerique-statut-juridique-et-activite-economique

[82] Yochai Benkler décrit cette spécificité de l'internet comme le principe de "l'innovation sans permission". Y. Benkler, The Wealth of Networks - How Social Production Transforms Markets and Freedom, Yale Univ. Press, 2006.

[83] W. Maxwell, *Pourquoi la FCC prépare l'abrogation de son règlement sur la neutralité de l'Internet,* 18 septembre 2017, Editions Multimedi@ n°174

[84] W. Maxwell, Quel futur pour la neutralité du net aux Etats-Unis ? ARCEP, L'état de l'internet en France 2021, p. 76-77

[85] W. Maxwell, *La neutralité de l'internet aux USA: le régulateur américain privilégie le droit de la concurrence*, janvier 2018, Légipresse

tuyaux menant jusqu'au domicile de l'internaute. Un filtrage à ce niveau serait incontournable et très dommageable pour la liberté d'expression. Le législateur a donc choisi tout simplement d'interdire toute discrimination ou blocage à ce niveau du réseau.

Le règlement européen sur l'Internet ouvert est un exemple d'une approche fondée sur la protection des droits, car la règle imposée aux fournisseurs d'accès ne dépend pas d'une appréciation des risques. Elle est absolue, les seules exceptions concernant les discriminations nécessaires pour la bonne gestion du réseau. Il n'existe pas de "petites" ou des "grandes" violations de la règle, chaque cas de blocage ou de discrimination étant condamnable. Le règlement sur l'Internet ouvert fournit ainsi une protection absolue de la liberté d'expression sur Internet. Certes, cette protection s'applique sur un tronçon très limité, le réseau d'accès, mais elle est absolue, à l'instar de ce qu'on imagine être une approche fondée entièrement sur la protection des droits.

c. Thématique 1 - articles et ouvrages représentatifs

W. Maxwell, *La neutralité de l'internet aux USA: le régulateur américain privilégie le droit de la concurrence*, janvier 2018, Légipresse

W. Maxwell et D. Brenner, Confronting the FCC Net Neutrality Order with European Regulatory Principles, The Journal of Regulation, 2012

W. Maxwell et N. Curien, *La neutralité d'Internet*, Éditions La Découverte, 2011.

W. Maxwell et N. Curien, Net Neutrality in Europe: An Economic and Legal Analysis, Concurrences, Review of competition laws, 2010 N°4.

W. Maxwell, La neutralité du net et la liberté d'expression, Légipresse n° 273, juin 2010

W Maxwell et D. Sieradzki, The FCC's Network Neutrality Ruling in the Comcast case ; Towards a Consensus in Europe ?), Communications & Strategies, 4ème trimestre 2008

W. Maxwell, *Europe's New Regulatory Toolbox, CommLaw Conspectus, Journal of Communications Law and Policy, 2004*

W. Maxwell, *Electronic Communications: The New EU Framework*, Oceana Publications (NY) 2002.

2. Deuxième thématique : La régulation des plateformes numériques

a. La liberté d'expression favorisée par une absence d'obligation générale de surveillance

La manière d'équilibrer la liberté d'expression et la protection d'autres droits sur internet a donné lieu rapidement à des litiges, notamment l'affaire *LICRA c. Yahoo* en France, et l'affaire *Reno c. ACLU* aux États-Unis[86]. L'obligation pour un prestataire technique d'exercer un contrôle préalable des contenus partagés par les utilisateurs sur un forum de discussion était jugé attentatoire à la liberté d'expression aux États-Unis. La législation américaine (*Communications Decency Act, Digital Millenium Copyright Act*), et la législation européenne (directive commerce électronique) ont convergé vers un système fondé sur une notification *ex post*. L'opérateur de l'espace d'hébergement devait agir s'il avait une connaissance du caractère illicite du contenus, notamment grâce à une notification par un utilisateur. L'absence d'obligation de contrôle préalable, et l'absence d'obligation de surveillance continue, étaient considérées nécessaires pour préserver la liberté d'expression et l'émergence de nouveaux moyens de communication par internet.

b. Les moyens techniques pour lutter contre la contrefaçon ne doivent pas être excessifs

Cet équilibre a été rapidement mis sous tension par la prolifération de contenus échangés en violation du droit d'auteur. Les moyens techniques existaient pour mettre fin à la plupart des échanges en violation du droit d'auteur, mais ces techniques créaient des ingérences dans d'autres droits, dont la protection des données à caractère personnel. Dans un premier arrêt, *Scarlet Extended*, la CJUE a estimé que l'ordonnance d'un juge obligeant un fournisseur d'accès à analyser les fichiers échangés pour détecter la présence d'œuvres protégés par le droit d'auteur était excessive, créant notamment une ingérence excessive dans le droit à la protection des données à caractère personnel[87]. Le choix des moyens techniques pour la lutte contre les contenus illicites n'a pas cessé de générer des controverses. Un outil technique trop efficace dans la détection de contenus illicite serait excessif au regard de la protection d'autres droits tels que la protection des données à caractère personnel, et au regard de l'équilibre fixé par le législateur dans la directive commerce électronique. Une multitude de méthodes techniques et institutionnelles a été essayée pour limiter

---

[86] W. Maxwell, "La jurisprudence américaine en matière de liberté d'expression sur Internet" *Conseil d'Etat, Etude annuelle 2014 sur le numérique et les droits fondamentaux* septembre 2014; *W. Maxwell et J. Massaloux, Freedom of Expression: not all Words were created Equal – French, European and US Perspectives, Communications Policy Research Conference, EuroCPR, mars 2002.*

[87] CJUE 24 nov. 2011, aff. C-70/10; W. Maxwell *A Regulatory Framework for Dealing with Online Copyright Infringement (OCI), Research Paper presented at the 41st Telecommunications Policy Research Conference (TPRC), Virginia, September 2012; W. Maxwell, Filtrage de l'Internet et blocage du Web par les FAI : une loi spécifique est nécessaire, Edition Multimédi@, 30 mai 2011*

la diffusion de différents types de contenus préjudiciables, chaque approche se concentrant sur différents types d'intermédiaires techniques[88]. Dans ma thèse de doctorat soutenue en 2016, j'ai tenté de définir une méthodologie cohérente pour ces différentes approches, fondée sur un bilan coûts/bénéfices en matière de protection des droits. Cette approche avait l'avantage de proposer une approche commune, quel que soit le type de contenus ou le type d'intermédiaire technique. Elle avait l'inconvénient d'être fondée un bilan coûts avantages qui est difficile, voire impossible, à appliquer aux droits fondamentaux en raison du caractère non-quantifiable de ces droits. Dans la thèse j'ai cité des exemples, par exemple en matière de protection de l'environnement, où des analyses d'impacts étaient utilisées pour évaluer des options de protection, et les droits et intérêts protégés - la préservation d'un écosystème par exemple - n'étaient pas quantifiables. Mais appliquée à la liberté d'expression sur internet, la méthode semblait artificielle, et construite sur l'hypothèse, contestable, que la liberté d'expression peut rentrer dans un bilan coûts/bénéfices.

c. Une approche par les risques imposée aux plateformes structurantes

Le chemin exploré par la thèse n'est pas mort, mais il prend une direction autre que celle que j'avais envisagée. Dans une nouvelle vague de législation européenne[89], les opérateurs de plateformes structurantes seront appelés à faire des études d'impact, et en fonction des risques identifiés, mettre en œuvre des moyens techniques et organisationnels pour réduire les risques à un niveau acceptable. Une approche par les risques est donc encouragée, mais au sein de chaque entreprise, sous le contrôle du régulateur. (Dans ma thèse, j'envisageais que l'analyse des risques serait conduite par le régulateur.)

Déléguer à un acteur privé la responsabilité d'effectuer une analyse des risques et de définir les moyens pour les atténuer est une pratique de régulation ancienne, utilisée notamment pour la régulation d'installation dangereuses[90] et la régulation d'institutions financières, notamment dans la lutte contre le blanchiment et le financement du terrorisme[91]. Les résultats de cette approche sont déjà visibles dans les déclarations publiées par l'ARCOM sur les moyens mis en œuvre par les plateformes pour lutter contre la manipulation de l'information, en application de la loi du 22

---

[88] W. Maxwell, *Smart(er) Internet Regulation Through Cost-Benefit Analysis - Measuring harms to privacy, freedom of expression, and the internet ecosystem*, Presses des Mines, 2017

[89] voy. notamment Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, SEC(2020) 432 final; Règlement 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

[90] Hopkins (2012). 'Explaining the "safety case"', op cit.

[91] Conseil de l'Europe, Comité d'Experts sur l'évaluation de mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme, Approche fondée sur les risques, https://www.coe.int/fr/web/moneyval/implementation/risk-based-approach, consultée le 10 octobre 2022

décembre 2018[92]. Cette loi impose aux principaux opérateurs de plateforme en ligne de prendre des mesures en vue de lutter contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité d'un des scrutins mentionnés au premier alinéa de l'article 33-1-1 de la loi du 30 septembre 1986.

En application de l'article 6-4-I. de la loi du n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique tel que modifié par la loi du 24 août 2021, les opérateurs de plateformes structurantes :

> "1° Procèdent chaque année à une évaluation des risques systémiques liés au fonctionnement et à l'utilisation de leurs services en matière de diffusion des contenus mentionnés audit premier alinéa et d'atteinte aux droits fondamentaux, notamment à la liberté d'expression. Cette évaluation tient compte des caractéristiques de ces services, notamment de leurs effets sur la propagation virale ou la diffusion massive des contenus susvisés ;
>
> « 2° Mettent en œuvre des mesures raisonnables, efficaces et proportionnées, notamment au regard des caractéristiques de leurs services et de l'ampleur et de la gravité des risques identifiés au terme de l'évaluation mentionnée au 1° du présent II, visant à atténuer les risques de diffusion de ces contenus, qui peuvent notamment porter sur les procédures et les moyens humains et technologiques mis en œuvre pour détecter, identifier et traiter ces contenus, tout en veillant à prévenir les risques de retrait non justifié au regard du droit applicable et de leurs conditions générales d'utilisation."

d. Une approche par les risques qui tolère des imperfections, notamment les faux positifs

Une approche similaire est imposée par le règlement européen sur la lutte contre la diffusion de contenus terroristes en ligne[93], par la proposition de Digital Services Act[94], et la proposition de règlement sur la lutte contre les abus sexuels sur enfants[95]. Cette dernière proposition obligerait les fournisseurs de services de communication et d'hébergement d'effectuer les analyses de risques concernant les abus sexuels sur enfants et de mettre en place des mesures techniques d'atténuation

---

[92] Les déclarations des opérateurs sont disponibles sur le site de l'ARCOM : https://www.arcom.fr/vos-services-par-media/internet-et-reseaux-sociaux/lutte-contre-la-manipulation-de-linformation-declarations-des-operateurs-de-plateformes-en-ligne-et-questionnaires-de-larcom

[93] Règlement 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

[94] Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, SEC(2020) 432 final;

[95] Proposition du 11 mai 2022 COM(2022) 209 final.

des risques. Dans le cadre de la proposition de règlement contre l'abus sexuel sur enfants, l'analyse de risques, et les mesures techniques d'atténuation seraient discutées avec les autorités spécialisées, et celles-ci pourraient ensuite demander à un tribunal de rendre certaines de ces mesures de détection obligatoires. Le problème des faux signalements de contenus relatifs aux abus sexuels sur enfants a été souligné dans un avis conjoint du CEPD et de l'EDPS[96]. Même si l'étude d'impact conduite par la Commission cite des niveaux de performance prédictive élevés pour certains outils de prédiction, aucune information n'est disponible sur les méthodes de tests et leur niveau d'efficacité en conditions opérationnelles. Le CEPD et l'EDPS soulignent les conséquences graves pour l'individu d'un faux signalement, car un faux signalement pourrait se retrouver ensuite dans les bases de données d'Europol.

La tension entre l'approche fondée sur les risques et l'approche fondée sur le respect des droits se manifeste dans le cadre faux positifs, à savoir les mesures techniques conduisant au blocage injustifié de contenus sur une plateforme. La CJUE dans l'affaire *Scarlet Extended* a considéré que le blocage à tort d'un contenu constituait une ingérence importante dans la liberté d'expression[97]. Or, on sait que le nombre de faux positifs générés par les outils automatiques de modération de contenus est élevé[98]. Le risque de faux positifs est également pris en considération par la CJUE dans l'affaire *Pologne c. Conseil européen*[99], par rapport à l'article 17 de la directive 2019/790 sur le droit d'auteur et les droits voisins dans le marché unique numérique.

La politique de gestion de contenus élaborée par une plateforme, et les moyens techniques utilisés pour appliquer cette politique, sont motivés par des choix commerciaux, mais également par des injonctions légales. Que ce soit pour la détection de violations de droit d'auteur[100], de contenus terroristes[101], de contenus de violences sexuelles contre les enfants[102], de désinformations[103], ou

---

[96] EDPB-EDPS Joint Opinion 04/2022, 28 juil. 2022

[97] W. Maxwell, L'Europe veut encadrer les algorithmes pour retirer les contenus illicites et éviter les « faux positifs ». Edition Multimédi@, Edition Multimédia SARL, 2021, pp.8-9. ⟨hal-03162122⟩

[98] W. Maxwell Applying Net neutrality rules to social media content moderation systems, Enjeux numériques, Annales des Mines, N° 18, juin 2022.

[99] CJUE, 26 avril 2022, aff. C-401/19.

[100] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC OJ L 130/92; CJUE, Pologne c. le Parlement européen et le Conseil européen, affaire C-401/19 26 avril 2022.

[101] Règlement 2021/784 sur du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne,

[102] Règlement (UE) 2021/1232 du Parlement européen et du Conseil du 14 juillet 2021 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne.

[103] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

d'autres contenus illicites[104], les législateurs européen et français encouragent, et parfois obligent, les plateformes à mettre en œuvre des moyens "raisonnables, proportionnés et effectifs" de lutte[105]. Qu'est-ce qu'une mesure raisonnable, proportionnée et effective ? Qu'il s'agisse de moyens humains ou algorithmiques, les mécanismes de retrait risquent de conduire à des sur-blocages (faux positifs) et à des sous-blocages (faux négatifs). Chaque type d'erreur aura des conséquences pour les droits et libertés individuels. Un sur-blocage créera une ingérence dans la liberté d'expression de la personne dont le contenu a été bloqué à tort ; un sous-blocage créera un dommage parfois irréparable pour la ou les victime(s) de violences en ligne. Un sous-blocage en matière de droit d'auteur créera des dommages économiques pour le titulaire du droit ; un sous-blocage en matière d'images de violences contre les enfants créera une atteinte grave à la dignité humaine. Ces impacts sont de nature différente, et devront être mis en équilibre avec les conséquences de sur-blocages sur la liberté d'expression. L'équilibre mis en place par la plateforme dans sa politique de gestion de contenus sera nécessairement imparfait, conduisant tantôt à des sur-blocages, tantôt à des sous-blocages. Le niveau "raisonnable, proportionné et effectif" des mesures doit composer avec ces imperfections. Une approche réglementaire fondée sur les risques (*risk-based*) s'accommode de ces imperfections. Dans une approche fondée sur les risques, l'objectif est d'atteindre une efficacité optimale, sans nécessairement chercher la perfection.

Dans l'ensemble de ces textes, une approche par les risques est clairement affirmée. On traite le risque de diffusion de contenus illégaux sur internet et le risque de manipulation des utilisateurs de plateformes comme on traiterait le risque d'un accident industriel. On demande aux plateformes d'évaluer les risques de ces accidents et de mettre en place des mesures efficaces et proportionnées pour les réduire. La loi ne définit pas la nature des mesures. Il incombe aux plateformes de les définir, et les pondérations effectuées par les plateformes seront nécessairement imparfaites. Comme je l'ai indiqué dans un récent article[106], déléguer la pondération de droits fondamentaux à un acteur privé soulève des difficultés par rapport à la Charte et le RGPD, car les moyens de détection de contenus en ligne créeront nécessairement des ingérences dans la liberté d'expression et dans le droit à la protection des données personnelles, et de telles ingérences doivent découler d'une loi définissant clairement les modalités et les limites des mesures imposées.

e. Thématique 2 : articles représentatifs

[104] Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République, art. 42.
[105] Voy. notamment la proposition de DSA, art. 27.
[106] W. Maxwell, The GDPR and private sector measures to detect criminal activity, Revue des Affaires européennes, Bruylant/Larcier, 2021; voy. également Bassini, Fundamental Rights and Private Enforcement in the Digital Age, 25 ELJ (2019), p. 182.

W. Maxwell Applying Net neutrality rules to social media content modération systems, Enjeux numériques, Annales des Mines, N° 18, juin 2022.

W. Maxwell, O. Henrard, et P. Idoux Le distributeur de services audiovisuels à l'ère numérique : statut juridique et activité économique, avec Olivier Henrard, juin 2017, CSA Lab

W. Maxwell, *Smart(er) Internet Regulation Through Cost-Benefit Analysis - Measuring harms to privacy, freedom of expression, and the internet ecosystem*, Presses des Mines, 2017

W. Maxwell et T. Pénard, "Quelle régulation pour les plateformes numériques en Europe ? « Réalités Industrielles, Annales des Mines, p. 42, août 2016 ;

W. Maxwell, "La jurisprudence américaine en matière de liberté d'expression sur Internet" *Conseil d'État, Étude annuelle 2014 sur le numérique et les droits fondamentaux* septembre 2014.

W. Maxwell, *A Regulatory Framework for Dealing with Online Copyright Infringement (OCI), Research Paper presented at the 41st Telecommunications Policy Research Conference (TPRC), Virginia, September 2012.*

W. Maxwell et J. Massaloux, Freedom of Expression: not all Words were created Equal – French, European and US Perspectives, Communications Policy Research Conference, EuroCPR, mars 2002

3. Troisième thématique : La régulation des données à caractère personnel

Le contraste entre l'approche par les risques et l'approche fondée sur le respect des droits est particulièrement visible lorsque l'on compare la protection des données à caractère personnel aux États-Unis et en Europe.

a. États-Unis : une régulation des données à caractère personnel ancrée dans la protection du consommateur qui intègre une approche économique

Les États-Unis disposent d'une loi, le Privacy Act de 1974, qui protège les données à caractère personnel traitées par les administrations de l'État. Mais le niveau de protection outre-Atlantique est faible, et dispersée, pour les traitements de données par les acteurs privés[107]. Au niveau fédéral, les lois sur la protection des données à caractère personnel visent certains secteurs spécifiques – télécommunications, santé, finances, services vidéos - ou bien la protection des données des enfants. Seule la loi fédérale sur la protection des consommateurs, le FTC Act de 1914, s'applique à presque tous les secteurs de l'économie. L'article 5 du FTC Act interdit des pratiques trompeuses et déloyales. S'emparant de cette disposition, le régulateur américain, la FTC, a pu dans certains cas imposer aux acteurs puissants du numérique des obligations similaires à celles qui découlent du RGPD[108]. Tout traitement de données par une entreprise privée qui surprendrait le consommateur moyen, pourrait être qualifié de "déloyal" au titre de l'article 5 du FTC Act. La FTC a eu l'occasion de préciser ce qu'est une pratique "déloyale", et cette clarification s'appuie en grande partie sur une analyse économique. Pour la FTC, une pratique déloyale se définit à partir d'une analyse des bénéfices de la pratique contestée pour les consommateurs comparés aux préjudices subis par ceux-ci. La FTC ne tient pas compte de préjudices "évitables" par le consommateur. Ainsi, la FTC effectue une forme d'analyse coûts/avantages pour déterminer si une pratique est déloyale[109]. En France, l'existence d'une pratique déloyale dans le traitement des données à caractère personnel ne se résume pas à une formule mathématique sur les coûts et bénéfices de la pratique. L'approche est beaucoup plus qualitative, s'appuyant notamment sur le niveau de transparence, et les attentes

---

[107] W. Maxwell et C. Wolf, *So Close, Yet so far Apart: The EU and U.S. visions of a New Privacy Framework, Antitrust, Vol. 26, no 3, 2012.*

[108] W. Maxwell, Amende contre Facebool: comment la FTC américaine s'est transformée en "super CNIL". The Conversation, 2019.

[109] W. Maxwell, The Notion of 'Fair Processing' in Data Privacy Law (January 2, 2015)., in "Quelle protection des données personnelles en Europe?", Céline Castets-Renard (ed.), University of Toulouse, 2015, Available at SSRN: https://ssrn.com/abstract=2544623; "Principles based regulation of personal data: the case of 'fair processing'", International Data Privacy Law, Volume 5, Issue 3, August 2015, Pages 205–216

raisonnables des personnes concernées[110]. L'approche économique des États-Unis n'est pas surprenante, puisque la loi de protection utilisée par la FTC est une loi sur la concurrence et sur la protection des consommateurs.

b. Le RGPD combine une approche par les risques et une approche fondée sur le respect des droits

On pourrait s'attendre à ce que le RGPD privilégie une approche fondée sur le respect des droits, évitant ainsi une approche trop économique, fondée sur les risques. En réalité, l'approche fondée sur les risques est présente au sein du RGPD, à travers les principes de responsabilisation (*accountability*), de protection dès la conception (*data protection by design*), et les analyses d'impact[111]. Ces dispositions obligent les responsables du traitement à mettre en œuvre des mesures appropriées pour protéger efficacement les droits des personnes, compte tenu des risques, de l'état de l'art, et des coûts des mesures de prévention[112]. Il serait difficile d'imaginer une expression plus claire d'une approche par les risques, car le niveau des mesures de prévention sera déterminé en partie par une analyse des risques, et des coûts[113]. Les mesures doivent être suffisantes pour réduire les risques à un niveau acceptable[114].

En même temps, le RGPD incarne une approche fondée sur le respect des droits, en énonçant des principes (art. 5) et des droits pour les personnes (chapitre III) qui sont, eux, non-négociables. Cette apparente contradiction a été commentée par le groupe de travail article 29, prédécesseur du CEPD, dans une communication de 2014[115]. Selon le groupe de travail, les mesures techniques et organisationnelles pour protéger efficacement les droits peuvent varier selon le niveau de risques. En revanche, le respect des droits reste immuable :

---

[110] Ibid.; voy. également CNIL, dél. n° 2011-203 du 21 sept. 2011, CE, 12 mars 2014, n°353193

[111] W. Maxwell et S. Taieb, "L'accountability, Symbole d'une influence américaine sur le règlement européen des données personnelles?", Dalloz IP/IT, p. 123, mars 2016;

[112] CEPD,Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut, 20 octobre 2020.

[113] W. Maxwell et D. Ouandji, *Les mesures appropriées et analyses de risques dans le RGPD*, La Revue du DPO, Rétrospective 2018, Université Paris 1, mars 2019, pp 17-30.

[114] Groupe Art. 29 sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248, 4 oct. 2017.

[115] Groupe article 29, Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, 30 mai 2014

> "Les droits accordés aux personnes concernées par le droit de l'Union devraient être respectés sans regard pour le niveau des risques encourus par ces personnes en raison du traitement (par exemple, les droits d'accès, de rectification, d'effacement, d'opposition, de transparence, le droit à l'oubli, le droit à la portabilité).[116]"

Il n'y aurait donc aucune contradiction, puisque le respect des droits ne varie pas en fonction de l'analyse des risques. L'approche par les risques s'appliquerait uniquement aux mesures de prévention imposées par le RGPD. Celles-ci peuvent être déterminées en fonction d'une analyse des risques.

Les lignes directrices du groupe Article 29 en matière d'analyse d'impact font une distinction entre la gestion de risques pour les droits et libertés des personnes, et la gestion des risques pour d'autres sujets, "axée sur l'organisation" :

> "En termes de gestion des risques, une AIPD a pour objectif d'aider à «gérer les risques» pour les droits et libertés des personnes physiques en:
>
> - établissant le contexte: «compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque»;
> - appréciant le risque: «évaluer la probabilité et la gravité particulières du risque élevé»;
> - traitant le risque: «atténuer ce risque» et «assurer la protection des données à caractère personnel», et «démontrer le respect du présent règlement».
>
> Remarque: l'AIPD au sens du RGPD est un outil de gestion des risques pour les droits des personnes concernées et se place ainsi sous l'angle de leurs droits, comme c'est également le cas dans certains autres domaines tels que la sécurité sociétale, par exemple. À l'inverse, dans d'autres domaines encore (par ex. la sécurité de l'information), la gestion des risques est axée sur l'organisation.[117]"

Cette distinction n'exclut pas du champ de l'analyse d'impact le respect des droits fondamentaux. Elle précise seulement que l'impact sur les droits doit être apprécié du point de vue de la personne concernée.

---

[116] Ibid., p. 3.

[117] Groupe Art. 29 sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248, 4 oct. 2017, p. 20.

c. Le RGPD crée deux couches de protection : la protection juridique, et la protection technique et organisationnelle

En théorie, le RGPD assure la même protection des droits, quel que soit le niveau de risque. En pratique, il existe bien deux niveaux de protection : les “petits” risques seront protégés par les garanties légales offertes du RGPD : mise en jeu de la responsabilité de l’entreprise, amendes administratives, injonctions, dommages-intérêts. Les “grands” risques bénéficieront des mêmes garanties légales, mais bénéficieront en plus de mesures techniques et organisationnelles de prévention mises en place par le responsable du traitement en application du principe de responsabilisation. Les “grands” risques auront une couche supplémentaire - technique et opérationnelle - de protection.

Dans deux articles[118], j’ai tenté de faire un recoupement entre les exigences du RGPD en matière de mesures de prévention, et l’analyse économique du droit, et notamment la formule Hand qui aide à déterminer le niveau optimal des mesures de prévention. A un certain point, les mesures de prévention dépassent leur point d’utilité. Elles deviennent excessives :

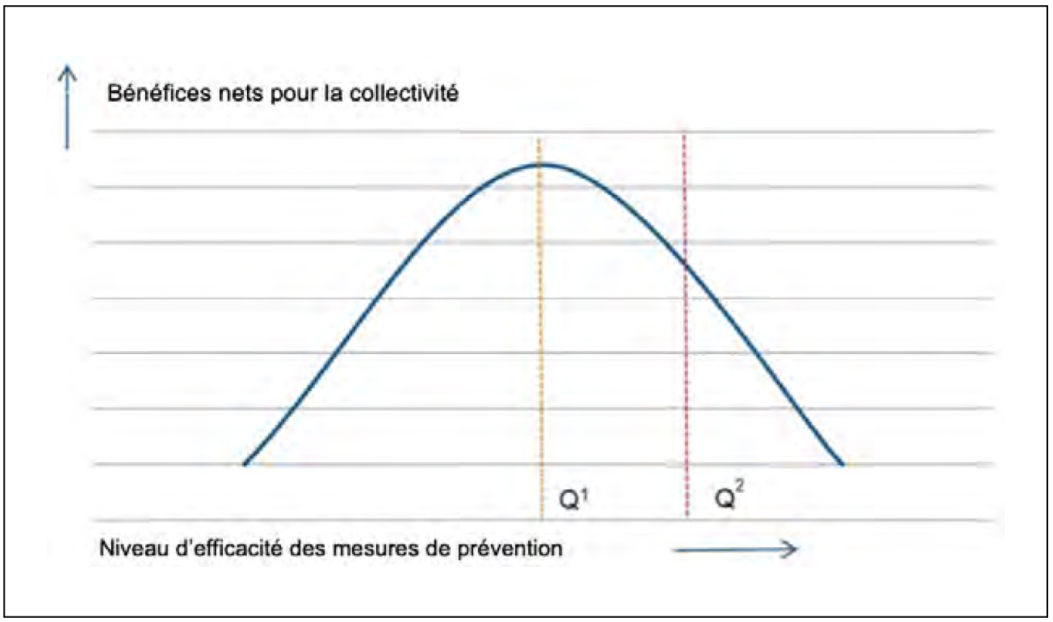

FIGURE 4 : MAXIMISATION DU BIEN-ÊTRE SOCIAL SELON LE NIVEAU D’EFFICACITÉ DES MESURES DE PRÉVENTION[83]

[118] W. Maxwell et C. Gâteau, *Les sources d'inspiration du Règlement Général sur la Protection des Données: la conformité, la réglementation de l'environnement, la responsabilité du fait des produits défectueux*, Annales des Mines, Enjeux Numériques, juin 2018. W. Maxwell et D. Ouandji, *Les mesures appropriées et analyses de risques dans le RGPD*, La Revue du DPO, Rétrospective 2018, Université Paris 1, mars 2019, pp 17-30.

Sur ce graphe, le niveau optimal des mesures de prévention sur le plan économique se situe au niveau Q1, même si le niveau Q2 fournira un niveau supérieur de protection. La prise en compte des coûts et bénéfices sociétaux des mesures conduira à un niveau "approprié" inférieur à un niveau de 100%. Cette approche économique n'est pas expressément visée par le RGPD, mais elle l'est dans la norme ISO sur les études d'impact en matière de protection de la vie privée :

> « Il peut avoir des situations où les mesures de diminution des risques ont un impact sur les bénéfices que les parties prenantes peuvent réaliser du traitement des informations concernées. Dans ce cas, la personne rédigeant l'analyse d'impact devrait effectuer une analyse coûts/bénéfices pour déterminer si les risques pèsent plus lourds que les bénéfices ou vice versa. Dans le premier cas, l'entreprise devrait adopter les mesures de diminution des risques en cause. Dans le deuxième cas, l'entreprise devrait décider d'accepter les risques, dans les limites permises par la réglementation.[119] »

Cette référence à une approche économique dans la norme ISO n'est pas surprenante, car la norme ISO concerne surtout la protection de la sécurité informatique. Pour la prise en compte de risques pour les droits fondamentaux, l'approche économique se heurte à l'impossibilité de quantifier les dommages à un droit fondamental et mettre ces coûts en balance avec d'autres coûts. N'importe quelle violation des droits d'une personne peut, selon le contexte, avoir des conséquences importantes, pour la personne et pour la société. Même un faible risque pour les droits serait, de ce point de vue, intolérable[120].

d. Qu'est-ce qu'un risque "acceptable" pour les droits fondamentaux?

Le RGPD impose aux responsables du traitement de mettre en place des mesures pour réduire les risques à un niveau "acceptable", mais il n'existe à ma connaissance d'explication de ce que serait un risque "acceptable" en matière de violation de droits fondamentaux. Il serait sans doute impossible de définir à l'avance le caractère tolérable, et donc acceptable, d'une violation de ces droits. Cela relève de l'appréciation des juges en fonction de chaque situation. Pour les mesures de réglementation adoptées par l'État, le contrôle de la nécessité et de la proportionnalité de la mesure sera effectué par les tribunaux. Comme souligné par le CEPD, le caractère acceptable d'un risque résiduel pour la personne dépendra de l'impact sur celle-ci :

---

[119] ISO ISO/IEC 29134 :2017. *Information technology – Security techniques – Guidelines for privacy impact assessment*, juin 2017, p. 20

[120] Schroeder, op cit.

> "Un risque résiduel peut notamment être considéré comme élevé et inacceptable dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par ex:. un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) et/ou lorsqu'il semble évident que le risque se concrétisera (par ex.: dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée).[121]"

e. La coexistence d'une approche fondée sur le respect des droits et d'une approche par les risques dans la mise en œuvre de droit au déréférencement

Les arrêts de la CJUE sur le droit au déréférencement[122] aident à clarifier le rôle de l'approche par les risques. Une mise en équilibre de droits et intérêts a lieu à deux niveaux : d'abord, elle intervient dans l'existence du droit lui-même. Ensuite, une mise en équilibre intervient pour définir les mesures techniques et opérationnelles devant être mises en œuvre pour protéger le droit. L'approche par les risques est utilisée pour la deuxième mise en équilibre, pas pour la première.

(i) La mise en équilibre de droits pour déterminer l'existence d'un droit au déréférencement

L'existence même d'un droit à un déréférencement dépend d'une mise en équilibre de l'intérêt pour le public de pouvoir accéder à l'information par le biais d'un moteur de recherche, et de l'intérêt de l'individu de ne pas souffrir de préjudice en raison de la disponibilité aisée, à travers le moteur de recherche, de cette information.

Il est utile de rappeler que le droit à l'oubli concerne des informations publiées de manière légale sur le web. En ce qui concerne les informations publiées de manière illégale, leur déréférencement ne pose aucun problème car la publication d'origine est illicite. Le conflit entre protection des données à caractère personnel et la protection de la liberté d'accéder à l'information survient lorsque l'information à la source est publiée de manière licite, mais la personne concernée par la publication souhaite que celle-ci ne soit pas trouvable en cas de recherche effectuée utilisant son nom. Il peut s'agir d'un article d'un journal non-flatteur qu'une personne préférerait occulter en cas de recherche

[121] Groupe Art. 29 sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248, 4 oct. 2017

[122] CJUE, 13 mai 2014, aff. C-131/12; 24 sept. 2019, aff.C-507/17; W. Maxwell et C. Zolynski, Panorama - Protection des données personnelles. Recueil Dalloz, Dalloz, 2020.

à partir de son nom. Dans son arrêt Google Spain, la CJUE a fourni une méthodologie pour déterminer, dans un cas précis, si le droit au déréférencement existe ou pas. L'opérateur du moteur de recherche doit appliquer cette méthodologie, et, en cas de contestation, l'autorité de protection des données et/ou les tribunaux contrôleront la décision prise par l'opérateur. Bien qu'étant une mise en équilibre, il est difficile d'appeler cette méthode une approche par les risques, car le but n'est pas de peser les risques pour définir un niveau de prévention adéquat, et un niveau de risque résiduel acceptable, mais de se statuer sur l'existence même du droit.

(ii) La mise en équilibre d'effets bénéfiques et dommageables des mesures techniques pour rendre effectif le droit au déréférencement

Une fois le droit au déréférencement reconnu, il restait la question des moyens techniques appropriés pour rendre ce droit effectif. A ce stade, l'approche par les risques rentre en ligne de compte. Dans le litige qui opposait Google à la CNIL, la CNIL demandait un moyen technique qui aurait eu pour effet de déréférencer avec un niveau d'effectivité de 100%. Il serait impossible de contourner le dispositif. Ce moyen technique aurait eu pour conséquence de rendre le déréférencement effectif partout dans le monde, même dans des pays où l'existence du droit au déréférencement n'est pas reconnue. Google estimait que ces moyens seraient excessifs, entrant en interférence avec des lois et principes constitutionnels non-européens. Une mesure technique plus modeste, le géo-blocage, rendrait le droit au déréférencement effectif au sein de l'Union européenne, et ne rentrerait pas en conflit avec des droits étrangers. Le niveau d'effectivité serait moindre, même au sein de l'UE, car il serait toujours possible pour un internaute de contourner le mécanisme en déguisant son adresse IP. Le niveau de protection serait élevé, mais pas à 100%. Le CJUE a rendu une décision en faveur de Google, estimant que la solution de géo-blocage permettrait une protection adéquate du droit au déréférencement, sans créer d'interférences avec des droits étrangers. Cet arrêt suit la même logique que celle utilisée par la Cour dans l'arrêt Scarlet Extended[123] - un moyen de protection trop efficace peut créer des ingérences excessives dans d'autres droits.

Que ce soit dans l'arrêt *Scarlet Extended* ou dans l'arrêt *Google*, l'approche par les risques conduit à une effectivité de moins de 100% dans les mesures techniques de protection, sans pour autant mettre en cause l'existence et la protection du droit en tant qu'objet juridique, le droit d'auteur dans

[123] CJUE 24 nov. 2011, aff. C-70/10; W. Maxwell *A Regulatory Framework for Dealing with Online Copyright Infringement (OCI), Research Paper presented at the 41st Telecommunications Policy Research Conference (TPRC), Virginia, September 2012; W. Maxwell, Filtrage de l'Internet et blocage du Web par les FAI : une loi spécifique est nécessaire, Edition Multimédi@, 30 mai 2011.*

le cas de *Scarlet Extended*, et le droit au déréférencement dans le cas *Google*. La protection juridique ne se prête pas à une approche par les risques; la protection technique, si.

f. L'analyse de risques est imposée en matière de transferts internationaux par la CJUE dans l'arrêt Schrems II

Les révélations d'Edward Snowden de 2013 ont mis la question des interceptions de sécurité au centre du débat public, exposant non seulement les pratiques peu encadrées des services de renseignement américains, mais également celles d'autres pays, comme la France[124]. Le manque d'encadrement des pratiques américaines a conduit à l'annulation de l'accord "Safe Harbor" par la CJUE en 2015[125], et à l'accord "Privacy Shield" en 2020[126]. Le manque de précisions sur les mesures de protection a également conduit la CJUE à juger contraire à la Charte des droits fondamentaux la directive 2006/24 sur la conservation des données de connexion[127]. La CJUE a ensuite examiné, dans les affaires *La Quadrature du Net*[128] et *La Ligue des Droits Humains*[129], l'utilisation d'algorithmes pour la détection d'activités criminelles[130].

Une approche fondée sur les risques n'est jamais évoquée dans ces décisions, qui se concentrent sur la nécessité et la proportionnalité des mesures. Néanmoins, il découle de l'arrêt Schrems II[131] que l'exportateur de données qui souhaite s'appuyer sur les clauses contractuelles types ou sur les règles d'entreprise contraignantes (BCR), devra effectuer une étude des risques dans le pays de destination et prévoir des mesures de protection supplémentaires pour diminuer les risques. Les recommandations du CEPD sur les mesures supplémentaires[132] sur les garanties essentielles européennes[133] sont destinées à aider les exportateurs à examiner la législation du pays de

---

[124] W. Maxwell, "Systematic government access to private-sector data in France." *International Data Privacy Law, 2014 Vol.4, N° 1* 13 février 2014 (Oxford)
[125] CJUE, Maximilian Schrems c. Data Protection Commissioner, affaire C-362/14, 6 octobre 2015.
[126] W. Maxwell et C. Zolynski, Panorama - Protection des données personnelles, juillet 2020-sept. 2022, Recueil Dalloz, à paraître.
[127] W. Maxwell et B. Fauvarque-Cosson, *Panorama: Droit de la protection des données personnelles*, Recueil Dalloz, n° 19, juin 2018.
[128] CJUE, 6 octobre 2020, *La Quadrature du Net*, aff. jointes C-511/18, C-512/18 et C-520/18
[129] CJUE, 21 juin 2022, Ligue des droits humains c. Conseil des ministres, aff. C-817/19.
[130] W. Maxwell et C. Zolynski, Panorama - Protection des données personnelles, juillet 2020-sept. 2022, Recueil Dalloz, à paraître; W. Maxwell, Le contrôle humain des systèmes algorithmiques - un regard critique sur l'exigence d'un humain dans la boucle, Mémoire original pour présenter l'habilitation à diriger des recherches de l'Université Panthéon-Sorbonne, (typoscript non-encore publié) 5 sept. 2022; W. Maxwell, Un contrôle humain efficace pour détecter les erreurs algorithmiques, in "Un droit de l'intelligence artificielle : entre règles sectorielles et régime général. Perspectives de droit comparé", C. Castets-Renard (ed.), à paraître.
[131] CJUE, 16 juil. 2020, C-311/18.
[132] CEPD, recom. 01/2020 18 juin 2021
[133] CEPD, recom. 02/2020 10 nov. 2020

destination, mais cette tâche reste complexe et, dans une certaine mesure, subjective[134]. Les "garanties essentielles" définies dans la recommandation du CEPD du 10 novembre 2020 définissent les droits qui ne peuvent faire l'objet d'aucun compromis. Ils tombent donc en dehors de toute approche par les risques.

g. Le partage des données mettra en tension l'approche par les risques et l'approche fondée sur le respect des droits[135]

La régulation des données prend une nouvelle dimension avec les diverses propositions de la Commission européenne centrées sur le partage des données. Avec sa *stratégie européenne pour les données*[136] et les propositions réglementaires qui en découlent[137], la Commission ambitionne la création d'un espace européen unique des données[138] qui sera lui-même composé d'espaces de données sectoriels dans des secteurs stratégiques et des domaines d'intérêt public[139] (énergie, agriculture, finance, santé, etc.)[140] progressivement eux-mêmes mis en place via des stratégies et initiatives sectorielles.

La Commission européenne souhaite libéraliser l'usage de données afin de favoriser le développement de nouveaux services innovants.[141] Ces données seraient aujourd'hui l'équivalent des réseaux de télécommunications dans les années 1990, une ressource sous-exploitée dont l'accès est nécessaire pour permettre le développement de services innovants. Les détenteurs de ces données - administrations, banques, opérateurs de télécommunications, d'énergie, postaux ou de transport - n'auraient pas les incitations, les moyens ou d'intérêt à investir ou développer ces nouveaux services innovants, dont certains pourraient faire concurrence aux services offerts par ces entreprises. Cette

---

[134] W. Maxwell et C. Zolynski, Panorama - Protection des données personnelles, juillet 2020-sept. 2022, Recueil Dalloz, à paraître.

[135] Cette section a été préparée avec l'aide d'Alexandre Humain-Lescop, doctorant à Télécom Paris.

[136] Communication de la Commission : Une stratégie européenne pour les données, COM(2020)66, 19 février 2020.

[137] Telles que le Data Governance Act dit « DGA » (Règlement (UE) 2022/868 sur la gouvernance européenne des données voté le 30 mai 2022), le Digital Markets Act dit « DMA » (Règlement (UE) 2022/1925 sur les marchés numériques votée le 14 septembre 2022), le Digital Services Act dit « DSA » (Proposition 2020/0361 (COD) du 15 décembre 2020 de règlement sur les services numériques), ou encore Data Act (Proposition 2022/0047 (COD) du 23 février 2022 de Règlement sur les données).

[138] Une stratégie européenne pour les données, op. cit. p5.

[139] Ibid. p26.

[140] Ibid. APPENDICE.

[141] Ibid. p1.

position de force des acteurs détenant la donnée pouvant mener à une situation de monopole où il serait impossible pour les nouveaux acteurs de s'insérer.[142]

Obliger le détenteur des données à accorder un accès à des parties utilisatrices de données se heurterait aux obstacles connus en droit des communications électroniques : ingérence dans le droit de propriété (même si l'idée générale d'un droit de propriété *stricto sensu* sur les données personnelles reste discutée, il existe néanmoins une possible propriété intellectuelle sur les données dérivées, calculées ou inférées à partir de données personnelles), ingérence dans la liberté d'entreprendre, menaces pour la sécurité des données et des systèmes. Ces obstacles ont déjà été rencontrés en matière d'accès aux réseaux de communications électroniques. La mise en place d'accords commerciaux et techniques, et la nécessité pour le demandeur d'accès de bénéficier du statut régulé d'opérateur de communications électroniques, ont permis d'encadrer ces risques.

Ce qui est nouveau aujourd'hui en matière d'accès aux données est l'existence d'un troisième acteur, l'individu concerné qui a confié ses données au détenteur d'origine. Il s'agit de la "personne concernée" en langage RGPD. Comment gérer cette relation triangulaire entre le détenteur de données qui les a recueillies, le futur utilisateur de données qui en demande l'accès, et la personne concerné entraînant des préoccupations d'ordre tant concurrentiel que liées à la protection de la vie privée[143] ? Dans cette mise en équilibre délicate, quelle est la place d'une approche par les risques?

En matière de services de paiement, le législateur européen a privilégié, via la deuxième directive européenne sur les services de paiement (dite DSP2)[144], un système de droit d'accès similaire à celui utilisé pour le changement d'opérateur téléphonique : la personne concernée, le client, a déjà une première relation contractuelle avec un service de paiement gestionnaires de comptes (telle qu'une banque) qui détient de par son activité des données de paiement du client. Le client va alors signer un contrat avec un tiers pour un autre service, un service d'initiation de paiement ou un service d'information sur les comptes. Via un droit d'accès[145], ce nouveau prestataire va alors pouvoir

---

[142] Comme mis en avant dans le cas des grandes plateformes numériques dans le rapport Stigler (Chicago Booth, Stigler Center, Stigler Committee on Digital Platforms, 16 novembre 2019).

[143] Direction générale du Trésor Français, Trésor-Eco, Protection de la vie privée et concurrence dans le numérique, N° 310, Juillet 2022.

[144] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (Texte présentant de l'intérêt pour l'EEE).

[145] Par une API (« *application programming interface* » ou « interface de programmation d'application » en français) que la CNIL définie comme « *une interface logicielle qui permet de « connecter » un logiciel ou un*

directement et gratuitement accéder aux données de paiement récoltées par le service de paiement gestionnaires de comptes. Ce mécanisme crée une relation complexe avec les bases légales prévue dans le RGPD, car le consentement fourni par le client au nouveau prestataire dans le cadre de la DSP2 ne constitue pas un consentement au sens du RGPD[146].

Il est à noter que la Commission européenne procède en ce moment même non seulement à l'examen des effets de cette directive[147], mais également à une réflexion[148] pour passer de cette situation actuelle d' « *open banking »,* concernant uniquement le partage de données de paiement, à une situation *d' « open finance »* qui pourrait concerner d'autre type de données financières telles que les données d'investissement, les données d'assurance, etc. La Commission européenne s'interroge ainsi sur ce système de droit d'accès face aux autres types de modèles de partage de données (modèle contractuel entre le détenteur et l'utilisateur, modèle de portabilité type RGPD, mais également modèle des intermédiaires de partage de données[149]) ainsi que sur ses modalités notamment en lien avec les questions de compensation, de responsabilité ou encore de bases légales.

Sur ce dernier point par exemple, un point d'attention particulier est donné à la question de la nécessité de baser le partage sur le consentement[150] de l'utilisateur ou non[151]. Dans les situations rendant le consentement nécessaire, il sera primordial de permettre à l'individu de mieux contrôler le sort de ses données tout en facilitant le partage de celles-ci, notamment à l'aide d'outils

---

service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités » (https://www.cnil.fr/fr/definition/interface-de-programmation-dapplication-api, consulté le 16/11/2022).

[146] CEPD, Lignes directrices 6/2020 relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, 15 décembre 2020.

[147] Commission européenne, « Services de paiement – réexamen des règles de l'UE ». https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules_en. Consulté le 16/10/2022.

[148] Dans le cadre de sa stratégie en matière de finance numérique du 24 septembre 2020 (COM(2021) 798 final).

[149] C'est en ce sens que l'existence d'un quatrième acteur, le service d'intermédiation de données du Data Governance Act, *op. cit*., doit être envisagé notamment par sa capacité à favoriser techniquement le partage de données ou d'aider à l'exercice des droits des personnes concernées (Article 10 a) et b)).

[150] Qu'il soit un consentement au sens du RGPD ou un consentement de nature contractuelle au sens de la DSP2 conformément à l'analyse du Comité Européen de la Protection des Données (EDPB, Lignes directrices 6/2020 relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD. 15 décembre 2020).

[151] Sans remettre en cause l'importance générale de donner à la personne concernée un pouvoir sur ses données personnelles, il serait par exemple peu raisonnable de conditionner un traitement de données personnelles à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) à la nécessité d'un consentement de la personne concernée par ce traitement. L'innovation dans ce secteur par la mutualisation des données entre acteurs et pourtant une piste de recherche sérieusement investie (Autorité de contrôle prudentiel et de résolution – ACPR, Expérimentation sur la mutualisation de données en LCB-FT, 2022, https://acpr.banque-france.fr/autoriser/fintech-et-innovation/experimentation-sur-la-mutualisation-de-donnees-en-lcb-ft, consulté le 16/10/2022).

techniques tels que des tableaux de bord ou d'autres solutions d'aide à la gestion du consentement. En effet, la nécessité d'un consentement spécifique de la personne concernée risque de rendre le partage de données plus compliqué à mettre en œuvre. A défaut de pouvoir remettre en cause ce caractère spécifique, la forme du consentement, et notamment sa lourdeur, seront déterminantes. De manière plus générale, la protection de l'individu passera également par la question de l'éventuel agrément des parties utilisatrices ou encore du cadre de responsabilité de chacune des parties prenantes au partage de données.

La question du consentement est donc centrale. Le doctorant CIFRE que j'encadre, Alexandre Humain-Lescop, qui travaille à la BPCE, examine la question du consentement, notamment par rapport à sa fonction. Une vision utilitariste du consentement considérerait que le consentement est simplement un moyen pour atteindre un objectif, la protection du client bancaire contre les utilisations préjudiciables de ses données, par exemple. Si le consentement n'est qu'un outil, les conditions de mise en œuvre du consentement pourraient être allégées en fonction des risques pour la personne. Une vision fondée sur les droits considérerait le consentement comme un droit à part entière, méritant une protection quelle que soit son utilité dans l'atteinte de tel ou tel objectif. Dans ce cas, un consentement plus élaboré, tel que prévu par le RGPD, serait un élément incontournable de tout schéma de partage de données.

h. Conclusions sur l'approche par les risques en matière de protection de données à caractère personnel

Le RGPD semble promouvoir à la fois une approche par les risques et une approche fondée sur le respect des droits. En réalité, il n'existe aucune contradiction entre ces deux approches, car l'approche par les risques se limite à la définition des moyens techniques et opérationnels devant être mis en œuvre par le responsable du traitement pour assurer l'effectivité des droits *sur le plan opérationnel*. L'approche par les risques ne touche ni à l'existence des droits définis par le RGPD, ni à leur protection *sur le plan juridique*. Les droits individuels restent entièrement protégés par la loi, par le régulateur et les tribunaux, même si leur protection technique serait moins que parfaite. Les deux approches coexistent, mais évoluent sur deux plans séparés. Pour Nemitz, il n'existerait pas de conflit entre l'approche fondée sur les risques, et le respect des droits. Le respect des droits reste absolu. Les analyses de risque servent à inculquer une culture de responsabilisation par rapport à la protection des droits[152].

[152] P. Nemitz, Constitutional democracy and technology in the age of artificial intelligence, Phil. Trans. R. Soc. A. 376, 2018, p. 12.

i. Thématique 3 : articles représentatifs

W. Maxwell et C. Zolynski, Panorama - Protection des données personnelles, juillet 2020-sept. 2022, Recueil Dalloz, à paraître.

W. Maxwell, The GDPR and private sector measures to detect criminal activity, Revue des Affaires européennes, Bruylant/Larcier, 2021

W. Maxwell et C. Zolynski, Panorama - Protection des données personnelles. Recueil Dalloz, Dalloz, 2020

W. Maxwell et C. Zolynski, Panorama - Protection des données personnelles, juin 2018 - juillet 2019. Recueil Dalloz, Dalloz, 2019.

W. Maxwell et C. Gâteau, *Les sources d'inspiration du Règlement Général sur la Protection des Données: la conformité, la réglementation de l'environnement, la responsabilité du fait des produits défectueux*, Annales des Mines, Enjeux Numériques, juin 2018.

W. Maxwell et B. Fauvarque-Cosson, *Panorama: Droit de la protection des données personnelles*, Recueil Dalloz, n° 19, juin 2018.

W. Maxwell et S. Taieb, "L'accountability, Symbole d'une influence américaine sur le règlement européen des données personnelles?", Dalloz IP/IT, p. 123, mars 2016;

W. Maxwell, "Principles based regulation of personal data: the case of 'fair processing'", International Data Privacy Law, Volume 5, Issue 3, August 2015, Pages 205–216,;

W. Maxwell, "Systematic government access to private-sector data in France." *International Data Privacy Law, 2014 Vol.4, N° 1* 13 février 2014 (Oxford)

W. Maxwell et C. Wolf, *So Close, Yet so far Apart: The EU and U.S. visions of a New Privacy Framework, Antitrust, Vol. 26, no 3, 2012.*

4. Quatrième thématique : la régulation de l'intelligence artificielle

La régulation de l'intelligence artificielle sera le théâtre d'une opposition musclée entre une approche par les risques et une approche fondée sur le respect des droits. La proposition de règlement européen AI Act privilégie une approche par les risques, fondée sur une analyse de risques et la définition de mesures de protection adaptées à ces risques. La proposition de règlement considère que l'analyse des risques doit prendre en considération des risques pour les droits fondamentaux, et construire des mesures de protection pour réduire ces risques à un niveau acceptable. La Commission encourage des normes harmonisées. Un système d'IA conforme au règlement pourra recevoir le marquage "CE".

a. Une proposition de règlement IA axée principalement sur l'approche par les risques

La tension entre les approches "risk-based" et "rights-based" est visible dans la proposition de règlement européen sur l'IA[153]. L'approche proposée par la Commission européenne soulève des critiques en raison de l'incompatibilité d'une approche par les risques et le respect des droits fondamentaux. Même si l'utilisation d'analyses d'impacts a été prévue par certains articles du RGPD, le RGPD contient également, et surtout, des principes normatifs fondés sur la protection des droits individuels[154]. La proposition de règlement européen sur l'IA s'inspire en revanche des principes de sécurité informatique, privilégiant une approche fondée sur la gestion des risques, incorporant notamment la formalisation des études d'impact[155]. Ce règlement pêcherait par l'absence de principes généraux et abstraits, privilégiant plutôt un contrôle au cas par cas par des méthodes d'évaluation d'impact[156].

La tension entre une approche fondée sur les risques et une approche fondée sur le respect des droits en matière de régulation de l'IA est exprimée ainsi par l'ONG Access Now :

> "Une approche par les risques implique d'évaluer la sévérité et la nature des risques relative à une situation précise et une menace reconnue. Cette approche est utile dans un

[153] Mantelero, A. (2022). Regulating AI. In: Beyond Data. Information Technology and Law Series, vol 36. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-531-7_4
[154] Benbouzid, Bilel, Yannick Meneceur, et Nathalie Alisa Smuha. « Quatre nuances de régulation de l'intelligence artificielle. Une cartographie des conflits de définition », *Réseaux*, vol. 232-233, no. 2-3, 2022, pp. 29-64; voy. également Groupe de Travail Art. 29, .
[155] Ibid., p. 45.
[156] Ibid., p. 48.

> environnement technique où les entreprises doivent évaluer leurs propres risques opérationnels. En revanche, la [proposition de la Commission européenne] demanderait aux entreprises d'évaluer leurs propres risques opérationnels et les mettre en balance avec les droits fondamentaux des citoyens. Cela conduit à une distorsion de ce qu'est un droit fondamental. Ces droits ne peuvent pas être mis en équilibre avec les intérêts d'entreprises.[157]"

La position exprimée par "Access Now" fait abstraction du fait que les analyses d'impact en droits fondamentaux existent déjà au sein du RGPD[158], et qu'elles contribuent à une prise de conscience des risques et à la création d'une culture responsabilité autour de la protection des droits[159].

Mes travaux de recherche, et les travaux des doctorants que j'encadre, à Télécom Paris visent à comprendre l'origine des risques pour les droits fondamentaux créés par les systèmes d'IA, et d'étudier la possibilité de réduire ces risques par des approches techniques et/ou par des approches humaines de gouvernance.
Dans l'arrêt *La Ligue des Droits Humains* la CJUE impose une analyse d'effectivité et de risques

Il découle de l'arrêt *La Ligue des Droits Humains* que l'exploitant de l'algorithme devra évaluer régulièrement l'effectivité de celui-ci dans sa tâche de prédiction d'activités suspicieuses, notamment afin de réduire le nombre de faux signalements générés par le système[160]. Même si la Cour n'utilise jamais le terme "analyse de risque", l'obligation d'évaluer, à intervalle régulier, la performance de l'algorithme, le nombre de faux positifs, et l'existence d'éventuelle discriminations, s'inscrit dans une approche de responsabilisation tout à fait similaire à celle prévue par le RGPD et qui, comme nous l'avons vu[161], s'analyse comme une approche par les risques.

b. Quatre programmes de recherche financés pour explorer la régulation de l'IA et les risques pour le respect des droits

---

[157] HIDVEGI F., DANIEL L., MASSE E., « The EU should regulate AI on the basis of rights, not risks, Access Now », fév. 2021, https://www.accessnow.org/eu-regulation-ai-risk-based-approach/ consulté le 19 octobre 2022, traduit par moi.
[158] Groupe Art. 29 sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248, 4 oct. 2017.
[159] Nemitz, Paul, Constitutional democracy and technology in the age of artificial intelligence, Phil. Trans. R. Soc. A. 376, 2018, p. 12.
[160] CJUE 21 juin 2022, aff. C-817/19.
[161] § II-3-b supra

(i) Le programme de recherche XAIforAML (financement ANR)

Quelques mois après mon arrivé à Télécom Paris, j'ai rédigé une proposition de recherche pour un l'ANR autour de l'utilisation d'algorithmes explicable pour la détection d'activités de blanchiment de capitaux et de financement du terrorisme (LCB-FT). La demande de subvention, qui s'élevait à 600 000€, nous permettait d'engager deux doctorants, un post-doc, la visite de professeurs étrangers, et l'organisation de colloques. La chaire de recherche a été créée avec le concours de PWC, l'ACPR-Banque de France, et Dataiku. Le Crédit Agricole a rejoint la chaire plus récemment.
La chaire nous permet d'examiner les enjeux d'explicabilité algorithmique dans un domaine à enjeu élevé pour les citoyens, puisqu'il s'agit de systèmes qui peuvent conduire à la dénonciation d'une personne, à son insu, à la police ou aux autorités de renseignement. Dans le cadre de cette chaire, j'encadre[162] une doctorante, Astrid Bertrand, et un post-doc, Rafik Belloum, sur l'utilisation d'outils d'explicabilité pour réduire les biais cognitifs. Nous avons organisé quatre ateliers publics avec l'ACPR sur l'utilisation de l'IA dans les services financiers[163], et avons publié plusieurs articles, dont deux qui traitent des questions juridiques liées à l'introduction de l'IA dans la génération de signalements anti-blanchiment, et notamment l'impact sur les droits fondamentaux[164]. Ces articles ont été présenté à deux conférences internationales[165], et le seront à une troisième conférence en décembre[166]. Ces articles mettent en évidence la coexistence malaisée entre outils automatiques de détection conçus dans un but d'efficacité dans la détection de la criminalité, et la mise en équilibre de droits fondamentaux. Ce sont des acteurs privés qui ont la responsabilité de concevoir des systèmes techniques et humains pour mettre en équilibre la lutte contre la criminalité et la protection des droits fondamentaux. Le législateur et le régulateur disent seulement que les systèmes doivent être efficaces pour détecter la criminalité, et respecter en même temps le RGPD et d'autres droits fondamentaux. Il incombe aux acteurs privés de trouver le bon équilibre.

---

[162] Je suis co-directeur de sa thèse. Le professeur David Bounie est directeur principal. Il sera remplacé bientôt par James Eagan, professeur en HCI (humain computer interactions)

[163] Voy. les actes des quatre webinaires : Les lundis de l'IA et la Finance, par l'ACPR-Banque de France et Télécom Paris : L'explicability de l'IA en finance, 9 novembre 2020; L'équité dans les algorithmes, 11 janvier 2021; Partage et mise en commun des données dans la finance, 8 mars 2021; AI regulation in the financial sector : crossed perspectives from Asia and Europe, 17 May 2021

[164] Astrid Bertrand, Winston Maxwell, Xavier Vamparys, Do AI-based anti-money laundering (AML) systems violate European fundamental rights?, International Data Privacy Law, Volume 11, Issue 3, August 2021, Pages 276–293, https://doi.org/10.1093/idpl/ipab010; Maxwell, W. The GDPR and private sector measures to detect criminal activity, Revue des Affaires européennes, Bruylant/Larcier, 2021.

[165] ICML 2020 Law and Machine Learning Workshop, Jul 2020, Vienne, Austria; Conférence de l'Academy or European Law on Artificial Intelligence and Financial Security

[166] Digital Investigative Measures – Towards Empirical Legal Assessment?; Final conference of the project Making Transparent the Invisible Surveillance (MATIS), jointly carried out by the Uni.Lu and VUB, 1er décembre 2022.

La lutte contre le blanchiment est quasi-exclusivement dictée par une approche par les risques. La loi oblige les banques à concevoir les mesures techniques et organisationnelles pour détecter les risques qui émergent d'une analyse conduite par chaque banque de ses propres risques liés à son type de clientèle et d'activités bancaires. Chaque risque de blanchiment identifié dans l'analyse de risque doit ensuite trouver une solution au sein des scénarios algorithmiques mis en place par la banque. Sinon, la banque s'expose à des sanctions. Cette étude des risques se focalise uniquement sur les risques liés au blanchiment des capitaux et au financement du terrorisme. La protection des droits fondamentaux n'entre pas en ligne de compte. L'étude de risques en matière de droits fondamentaux relève d'une autre législation - article 35 du RGPD - et d'un autre régulateur - l'autorité de protection des données personnelles. L'étude de risques effectuée au titre de la législation LCB-FT n'est pas coordonnée avec l'étude de risques du RGPD. Dans nos articles, nous préconisons une coordination accrue entre régulateurs afin de tenir compte, dans la conception des outils de détection, des risques pour les droits fondamentaux.

Dans la détection d'activités criminelles telles que le financement du terrorisme, l'efficacité d'un algorithme peut être évaluée selon plusieurs paramètres. Ces paramètres peuvent entrer en conflit. Par exemple, un système de détection d'activités criminelles peut prioriser la détection d'événements suspicieux de manière à minimiser le nombre de faux négatifs, à savoir des activités vraiment criminelles qui échappent à la détection. Ce choix augmentera automatiquement le nombre de faux positifs, à savoir les personnes suspectées à tort d'activités criminelles. Le paramétrage du niveau de faux positifs par rapport aux faux négatifs a un impact direct sur l'efficacité du système dans la détection d'activités criminelles. Jusqu'à un certain seuil[167], un nombre élevé de faux positifs est souhaitable pour l'efficacité dans la détection d'activités criminelles. A l'inverse, un nombre élevé de faux positifs diminue l'efficacité en matière de protection des droits. Les critères de performance sont diamétralement opposés selon le point de vue que l'on adopte : les autorités de police d'un côté et les autorités de protection des droits et libertés individuelles de l'autre.

On a vu que l'approche économique de la régulation[168] permet de maximiser le bénéfice net pour la société de mesures de prévention, mais cette approche s'appuie sur une quantification des coûts. Cet équilibre nécessiterait une quantification des bénéfices et des coûts liés à la détection de la criminalité versus la protection des droits à la protection des données et à la présomption

[167] Au-delà d'un certain seuil, un nombre élevé de faux positifs peut nuire à l'efficacité de la détection car les enquêteurs seront submergés.
[168] supra § I-3-b

d'innocence. Cette quantification est périlleuse, voire impossible, lorsqu'il s'agit de droits fondamentaux[169]. Une approche par les risques peut également se satisfaire d'une analyse qualitative, et c'est ce qui est prévu dans le cadre d'analyses d'impact RGPD sur les droits fondamentaux[170]. Mais même avec une analyse qualitative, il s'agit de comparer deux droits et intérêts de nature différente : la sécurité publique, d'un côté, et la protection des droits individuels, de l'autre. Cette mise en équilibre relève de choix politiques issus de débats démocratiques. Elle relève du législateur. Nos recherches dans le cadre du programme XAIforAML ont mis en évidence une aberration dans la mesure où cette mise en équilibre est confiée par la loi aux entreprises régulées. Si on lui demande d'arbitrer, un acteur privé va agir en fonction de sa perception des risques de sanctions. Dans la lutte contre le blanchiment de capitaux, les acteurs perçoivent un risque plus élevé venant du régulateur financier que celui venant de l'autorité de protection des données à caractère personnel. Par conséquent, les acteurs privilégient généralement les critères d'efficacité venant du régulateur financier, un phénomène appelé *gold plating*[171].

Après ces études des systèmes de détection d'activités criminelles par rapport aux droits fondamentaux, nos travaux dans le programme XAIforAML se sont penchés sur le rôle précis de l'explicabilité. La doctorante Astrid Bertrand a étudié les différentes formes d'explicabilité et leur efficacité par rapport à l'objectif de faire comprendre le fonctionnement de l'algorithme à un public donné. Astrid Bertrand a partagé son temps entre Télécom Paris et l'ACPR, où elle a conçu des tests pour mesurer l'impact de différentes approches d'explication sur la compréhension de la personne qui reçoit l'explication. Ces travaux ont donné lieu à un article qu'Astrid Bertrand a présenté à la l'université d'Oxford en août dernier[172].

En parallèle de ses travaux sur l'efficacité de différentes formes d'explicabilité, Joshua Brand, ingénieur d'étude qui commencera son doctorat en janvier, étudie les fondements éthiques de l'explicabilité. Son premier papier, "Clarifying the Moral Foundation of Explainable AI", constitue une

---

[169] J'ai exploré cette question dans ma thèse : W. Maxwell. *Smart(er) Internet Regulation Through Cost-Benefit -- Analysis Measuring harms to privacy, freedom of expression, and the internet ecosystem*, Presses des Mines, 2017; Maxwell, Winston, A Method to Assess Regulatory Measures Designed to Limit Access to Harmful Content on the Internet (October 4, 2016). Available at SSRN: https://ssrn.com/abstract=3558490

[170] wp 248, op cit.

[171] W. Maxwell, A. Bertrand and X. Vamparys, Do AI-based anti-money laundering (AML) systems violate European fundamental rights? International Data Privacy Law, Volume 11, Issue 3, August 2021, Pages 276–293.

[172] How Cognitive Biases Affect XAI-assisted Decision-making: A Systematic Review, Proceedings of the AAAI/ACM Conference on Artificial intelligence, Ethics, and Society, Aug 2022, Oxford, United Kingdom.

revue de la littérature sur le rôle des explications dans ce qui est juste, et dans le respect de l'autonomie humaine. Ce papier fera bientôt l'objet d'une publication[173].

Enfin, dans une approche plus technique, Tiphaine Viard, maîtresse de conférence, étudiera l'utilisation des réseaux graphes pour augmenter la compréhension des signalements d'activités suspicieuses. Tiphaine Viard et moi encadrons le travail d'une doctorante, Dilia Olivo, sur ce sujet. La thèse de Dilia Olivo comprend un axe technique et une axe sur les droits fondamentaux. Elle examinera notamment l'impératif d'explicabilité réitéré par la CJUE dans sa décision du 21 juin 2022 sur la directive européenne les le traitement des données de passagers (PNR)[174].

En plus des articles mentionné ci-dessus, nos recherches dans le cadre du programme XAIforAML a donné lieu à des articles de vulgarisation[175]. J'ai également présenté les résultats de nos recherches à l'ANR lors de la revue d'étape le 10 février 2022, et ai préparé le rapport intermédiaire, en intégrant des demandes de modifications. Je gère les relations avec les partenaires de la chaire, Crédit Agricole, PWC, ACPR et Dataiku, et notamment l'organisation de comités de pilotage.

(ii) Le projet LIMPID sur les systèmes de reconnaissance d'image dignes de confiance (financement ANR)

Le deuxième projet ANR dans lequel j'ai un rôle d'encadrement concerne le projet **LIMPID Leveraging Interpretable Machines for Performance Improvement and Decision**, ANR 20-CE23-0028 sur les systèmes de reconnaissance d'images dignes de confiance. Pour ce projet, je suis responsable du volet régulation, ce qui signifie que j'ai rédigé la partie de la proposition ANR concernant le volet régulation et son intégration dans les volets techniques. J'ai recruté une doctorante pour ce volet, Mélanie Gornet, que je supervise avec la professeure Florence d'Alché. Ce projet combine une

---

[173] Brand, Joshua L.M. "Clarifying the Moral Foundation of Explainable AI." *The Digital Constitutionalist* (2022). *Forthcoming*.

[174] La directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière; CJUE 21 juin 2022 aff. 817/19 La Ligue des droits humains, point 195.

[175] A. Bertrand, W. Maxwell, X. Vamparys, « Financement du terrorisme : Mettre l'intelligence artificielle et le partage de données au centre du dispositif de lutte », Le Monde, 19 juin 2021.W. Maxwell, X Vamparys, Netherlands welfare case sheds light on explainable AI for AML-CFT, Compliance & Enforcement, New York University, April 7, 2020; A. Bertrand, W. Maxwell, X. Vamparys, More AI, less box-ticking, says FATF in AML/CFT report, Télécom Paris blog, 13 July 2021; A. Bertrand, The US Anti-Money Laundering Act 2020 supports the deployment of technological innovation and machine learning, Telecom Paris blog, June 11, 2021; A. Bertrand, L'explicabilité des algorithmes au service de la lutte contre le blanchiment d'argent, Télécom Paris blog, 27 oct. 2020; A. Bertrand, The ACPR's guidelines on explainability : clarifications and ambiguities, Télécom Paris blog, Aug. 28, 2020.

approche mathématiques appliquées, et une approche de régulation. Le projet vise à définir les exigences en matière de biais et d'explicabilité d'un système de reconnaissance d'image pour les infractions routières, et d'un système de reconnaissance faciale pour l'authentification des voyageurs à la frontière. Définir les exigences revient à définir les principes généraux de ce qu'est un système équitable et transparent, et ensuite traduire ces principes en spécifications plus précises, en tenant compte de l'état de l'art en matière de contrôle de biais et d'explicabilité. On cherche à faire converger les exigences réglementaires d'un côté, et les solutions techniques, de l'autre, sachant à l'avance qu'une convergence totale est improbable.

Pour ce projet je co-encadre une doctorante, Mélanie Gornet, avec la professeure Florence d'Alché-Buc (professeure en mathématiques appliquées). Mélanie Gornet travaille actuellement sur un article sur le marquage CE - une mesure envisagée par le futur règlement européen sur l'IA - et l'équité. Compte tenu de la complexité, et de la nature contestable, du concept d'équité algorithmique, comment imaginer une norme et un marquage CE qui attesteraient du caractère non-discriminatoire d'un algorithme ? Une telle approche nous paraît impossible, ce qui met de nouveau en lumière la tension entre une approche fondée sur le respect des droits, et une approche fondée sur les risques. Notre approche est résumée dans l'article "Intelligence artificielle: normes techniques et droits fondamentaux, un mélange risqué[176]". La tâche de définir un niveau de discrimination "acceptable" est impossible pour plusieurs raisons. D'abord, il existe plusieurs définitions de discrimination – l'équité de groupe, l'équité individuelle, et l'équité d'opportunité – incompatibles entre elles[177]. Deuxièmement, la protection contre les discriminations algorithmiques dépend de la possibilité de tester l'algorithme par rapport à certains groupes de la population, alors que le choix même de ces groupes de la population, et la disponibilité de données étiquetées par rapport à ces groupes, restent contestables. Enfin, admettre un niveau "acceptable" de discrimination revient à accepter une discrimination occasionnelle, ce qui heurte une vision plus absolue de la protection des droits. La discrimination ne se prête pas au même type de régulation que la sécurité informatique, par exemple.

Les systèmes de reconnaissance faciale souffrent tous de différences de performance dans la reconnaissance de différents types de visages. Les mesures peuvent être prises pour éliminer

[176] M. Gornet et W. Maxwell, Intelligence artificielle: normes techniques et droits fondamentaux, un mélange risqué, The Conversation, 28 sept. 2022 https://theconversation.com/intelligence-artificielle-normes-techniques-et-droits-fondamentaux-un-melange-risque-189587

[177] W. Maxwell et S. Clémençon, Why facial recognition algorithms can't be perfectly fair, The Conversation, 20 juillet 2020, https://theconversation.com/why-facial-recognition-algorithms-cant-be-perfectly-fair-142608

certaines catégories de biais, mais il existera toujours des différences résiduelles dans la qualité des prédictions algorithmiques. Certains groupes de personnes souffriront de plus de faux négatifs (un refus erroné d'authentification) que d'autres, et seront donc pénalisés car ils devront faire la queue pour attendre un contrôle humain de leur passeport. A quel moment est-ce que cette différence de traitement devient problématique, sachant que le seul moyen d'atteindre un niveau zéro de discrimination est de réduire la performance prédictive de l'algorithme à un tel point qu'il serait complètement inutile. Il existe donc un équilibre entre la performance prédictive de l'algorithme et son niveau de discrimination. Les mesures anti-biais créent des coûts, notamment dans la diminution de l'utilité du système en raison de la baisse de son pouvoir prédictif. Les coûts évités grâce à ces mesures anti-biais sont des cas d'erreurs discriminatoires, qui deviennent plus rares grâce à l'augmentation des mesures de prévention. A un certain moment, l'ajout d'une mesure supplémentaire de prévention sera contre-productif, car elle évitera un faible nombre de cas de discrimination supplémentaires. Éliminer tous les cas de discrimination aurait un coût exorbitant, car cela rendrait le système inutilisable. Le problème est de trouver le point d'équilibre.

Est-ce l'existence de certains cas rares de discrimination algorithmique signifie que le risque résiduel est inacceptable ? Selon le groupe de travail Art. 29 (maintenant le CEPD), un risque, même faible, de violation d'un droit peut constituer un risque résiduel inacceptable :

> "Un risque résiduel peut notamment être considéré comme élevé et inacceptable dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par ex:. un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) et/ou lorsqu'il semble évident que le risque se concrétisera (par ex.: dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée).[178]"

Cette vision conduirait à l'abandon de tout système algorithmique qui produirait, même dans des cas rares, des discriminations ayant des conséquences importantes sur les personnes. Une autre vision conduirait à admettre l'existence de risques résiduels de discrimination, mais d'assortir le système d'autres mesures de protection, le contrôle humain par exemple, pour réduire l'impact de ces risques résiduels. Cette approche a été privilégiée par la CJUE dans son arrêt La Ligue des droits humains du 21 juin 2022[179]. Dans mon mémoire original pour l'HDR, je remets en question cependant la

[178] WP 248 précité, p. 22.
[179] CJUE 21 juin 2022 aff. 817/19 La Ligue des droits humains,

possibilité pour un contrôle humain individuel de détecter ces discriminations[180]. La solution proposée par la CJUE apparaît dès lors problématique.

Selon les professeurs Kahneman, Sibony et Sunstein, les décisions humaines sont souvent plus erronées et discriminatoires que les décisions algorithmiques[181]. La question du risque "acceptable" de discrimination algorithmique pourrait tenir compte du niveau de risque qui existerait en l'absence de l'algorithme. Ces questions sont loin d'être résolues, et dépendent en partie de la vision que l'on adopte. Une approche par les risques pourrait se traduire par une réduction du nombre de discriminations au niveau le plus faible possible compte tenu de l'état de l'art, et entourer le système d'autres moyens de protection pour réduire l'impact des risques résiduels. Une approche fondée sur la protection des droits insisterait sur l'inacceptabilité de toute discrimination, quelle qu'elle soit. Dans sa décision du 21 juin 2022, la CJUE adopte les deux approches en même temps. La Cour annonce que l'algorithme doit être exempte de toute discrimination. Elle dit aussi que l'opérateur doit prévoir un contrôle humain individuel notamment pour détecter des décisions discriminatoires[182].

(iii) Le programme de recherche financé par la CDC sur un moteur de recommandation d'intérêt public

Le groupe Caisse des Dépôts (CDC) participe financièrement (300K€) au programme Operational AI Ethics, en particulier le volet qui se concentre sur les algorithmes d'intérêt public. La question des algorithmes d'intérêt public a récemment fait l'objet d'une publication du Conseil d'État[183]. Nos travaux de recherche consistent dans un premier temps à proposer des mesures de biais pour la plateforme "Mon Compte Formation". Les tests de biais conduits par la CDC vérifient si le moteur de recherche des formations propose certaines formations plus souvent à des femmes qu'aux hommes. Dans l'année qui vient, la CDC souhaite explorer d'autres mesures de biais, par exemple vérifier si les textes proposés par les organismes de formation pour décrire les formations contiennent des biais de genre. Ensuite, nous examinerons la conception d'un moteur de recommandation qui tiendrait

[180] W. Maxwell, Le contrôle humain des systèmes algorithmiques - un regard critique sur l'exigence d'un humain dans la boucle, Mémoire original pour présenter l'habilitation à diriger des recherches de l'Université Panthéon-Sorbonne, 5 sept. 2022.
[181] C. R. Sunstein, "Governing by Algorithm? No Noise and (Potentially) Less Bias" Harvard Public Law Working Paper No. 21-35, 2021, SSRN 3925240; D. Kahneman, O. Sibony, C. Sunstein, "Noise - Pourquoi nous faisons des erreurs de jugement et comment les éviter", Odile Jacob, 2021.
[182] CJUE 21 juin 2022 aff. 817/19 La Ligue des droits humains, points 197 et 206.
[183] Conseil d'Etat, Intelligence artificielle et action publique : construire la confiance, servir la performance, Étude adoptée le 31 mars 2022, publiée le 30 août 2022.

non seulement compte des termes de requête exprimés par le demandeur de formation, mais qui serait capable de proposer des formations adaptées au profil du demandeur, et qui répondraient en plus à des objectifs l'intérêt public, tel que la formation de salariées dans certains secteurs en tension. Nous examinerons si un moteur de recommandation en matière de formation professionnelle peut tenir compte d'objectifs d'intérêt général en plus des intérêts exprimés par le demandeur de formation, et si la plateforme peut donner des "coups de pouce" (*nudge*) pour orienter le citoyen en recherche de formation vers un secteur particulièrement important pour l'économie française.

L'étude du Conseil d'État fait état des nombreuses utilisations d'algorithmes par l'État, y compris des algorithmes utilisée pour prioriser les enquêtes et contrôles selon une approche fondée sur les risques[184]. L'utilisation d'algorithme servirait à rendre l'action de l'État plus efficace, notamment en permettant d'optimiser l'emploi des ressources publics[185]. Le Conseil d'État adopte à la fois une approche fondée sur le respect des droits, et une approche fondée sur les risques. Les deux se complètent.

En ce qui concerne une approche fondée sur le respect des droits, le Conseil d'État propose le principe de primauté humaine :

> "Les SIA publics se conçoivent comme des outils au service de l'humain, ce qui suppose qu'ils répondent à une finalité d'intérêt général et que l'ingérence dans les droits et libertés fondamentaux qui résulte de leur mise en service ne soit pas disproportionnée au regard des bénéfices qui en sont attendus. En outre, l'humain doit se porter garant du bon fonctionnement du SIA en le supervisant (grâce à des mesures techniques, juridiques, de formation et de gouvernance), y compris en cas de recours à un outil d'aide à la décision, l'humain étant en général prompt à entériner les résultats proposés par la machine (biais d'automatisation). Enfin, l'humain doit anticiper le risque d'un dysfonctionnement du système, en limitant sa dépendance, et en assumer les conséquences, l'erreur de la machine n'étant, indirectement, qu'une erreur humaine.[186]"

Le principe de primauté humaine peut être considéré comme une approche fondée sur le respect des droits parce que la garantie humaine proposée par le Conseil d'État ("l'humain doit se porter

[184] voy. Conseil d'Etat Intelligence artificielle et action publique : construire la confiance, servir la performance, op cit, ainsi que Conseil d'Etat, Les pouvoirs d'enquête de l'administration, Etude, avril 2021.
[185] Intelligence artificielle et action publique, op. cit., p. 77.
[186] Ibid., p. 9.

garant du bon fonctionnement du SIA") s'impose sans exceptions, quel que soit le niveau de risque créé par le système. Il s'agirait d'un droit non-modifiable en fonction des risques.
En ce qui concerne la discrimination, le Conseil d'État semble accepter une approche par les risques, car les cas de discriminations doivent être minimisés notamment par la mise en place d'un système de gestion de risques :

> "Les concepteurs des SIA doivent choisir, parmi les différentes conceptions de l'équité, celle qui guidera le fonctionnement des systèmes et formaliser ce choix, dans le respect du principe d'égalité. Ils doivent en outre veiller à prévenir les discriminations involontaires, enjeu particulièrement prégnant pour les SIA d'aide à la décision fondés sur l'apprentissage machine. Entraînés sur de vastes jeux de données susceptibles de renfermer des biais, ces systèmes peuvent les reproduire et produire des résultats pénalisants pour certaines catégories de personnes. Ce principe implique la mise en place d'un système de gestion des risques comportant une analyse critique à toute étape (entraînement et déploiement), une sensibilisation des agents chargés des SIA à cette problématique spécifique voire une plus grande représentativité sociale des équipes de conception.[187]"

On retrouve la logique de mesures de prévention adoptées en fonction de l'analyse de risques.

Nos travaux sur les moteurs de recommandation d'intérêt public devront nécessairement tenir compte de ces deux approches, qui peuvent paraître contradictoires, mais qui en réalité se complètent.

J'encadre une doctorante CIFRE (Alicia Breidenstein) sur ces questions, et nous souhaitons recruter un deuxième doctorant. Je travaille sur ce projet avec la professeure Valérie Beaudouin, professeure en sociologie du numérique, et Matthieu Labeau, maître de conférence en machine learning.

(iv) Contribution à la chaire de recherche Digital Finance

Je contribue à la chaire de recherche Digital Finance sur le volet IA et crime financier. Cette recherche recoupe les travaux effectués au niveau de la chaire XAI for AML. Dans le cadre de la chaire Digital Finance j'encadre une doctorante (Dilia Olivo) sur l'utilisation des graphes pour rendre les signalements algorithmiques plus transparents. J'encadre également, avec le professeur David

[187] Ibid.

Bounie, un doctorant (Xavier Vamparys) préparant une thèse sur l'effet transformatif de l'IA sur l'assurance, et sur le principe de solidarité.

c. Travaux interdisciplinaires de recherche sur l'explicabilité algorithmique

Peu après mon arrivée à Télécom Paris, j'ai entrepris l'écriture d'un article interdisciplinaire sur l'explicabilité algorithmique, avec huit autres co-auteurs. J'étais le rapporteur pour ce travail collectif, qui a abouti sur la publication de deux articles interdisciplinaires sur l'explicabilité des algorithmes : "Flexible and context-specific AI explainability - a multidisciplinary approach"; "Identifying the 'right' level of explanation in a given situation". J'ai présenté ces articles au First International Workshop on New Foundations for Human-Centered AI (NeHuAI), Santiago de Compostella, Spain, September 4, 2020, CEUR Workshop Proceedings, Vol. 2659, p. 63.

Ces articles interdisciplinaires mettent en évidence les nombreux compromis, et exercices de mise en équilibre, nécessaires pour rendre l'explicabilité pertinente dans un cas donné. Les approches de l'explicabilité doivent tenir compte des caractéristiques de la personne recevant l'explication, les enjeux de la recommandation algorithmique, les dégradations de performance découlant éventuellement de l'explicabilité, et de l'environnement réglementaire. L'explicabilité algorithmique se prête bien à une analyse par les risques, car l'explicabilité n'est pas un droit absolu. Il peut le devenir, notamment pour les décisions algorithmiques ayant des impacts importants sur les personnes, et les décisions administratives individuelles. Le besoin d'explicabilité, et son caractère de "droit" pour l'individu, augmente avec le niveau d'impact sur la personne.

d. Animation du groupe interdisciplinaire Operational AI Ethics

L'écriture de deux articles interdisciplinaires sur l'explicabilité nous a permis de créer un groupe interdisciplinaire d'enseignants chercheurs de six disciplines : maths appliquées, statistiques, sciences informatiques, économie, sociologie, droit, autour de questions liées à l'IA éthique. Nous avons organisé nos travaux autour de cinq thématiques : l'explicabilité, l'équité, la responsabilité, la gouvernance, et l'IA d'intérêt général. Le groupe s'est étendu à 14 enseignants-chercheurs permanents, et six doctorants.

Je codirige ce groupe avec Tiphaine Viard, professeure associée en sciences informatiques.

e. Thématique 4 : articles représentatifs

W. Maxwell, Le contrôle humain des systèmes algorithmiques - un regard critique sur l'exigence d'un humain dans la boucle, Mémoire original pour présenter l'habilitation à diriger des recherches de l'Université Panthéon-Sorbonne, (typo script non-encore publié) 5 sept. 2022

W. Maxwell, Un contrôle humain efficace pour détecter les erreurs algorithmiques, in "Un droit de l'intelligence artificielle : entre règles sectorielles et régime général. Perspectives de droit comparé", C. Castets-Renard (ed.), à paraître.

W. Maxwell, "La régulation des algorithmes aux États-Unis : quelles leçons pour l'Europe ?", in Bertrand B. (dir.), La politique européenne du numérique, Bruxelles, Bruylant, 2022

W. Maxwell, The GDPR and private sector measures to detect criminal activity, Revue des Affaires européennes, Bruylant/Larcier, 2021.

W. Maxwell, A. Bertrand and X. Vamparys, Do AI-based anti-money laundering (AML) systems violate European fundamental rights? International Data Privacy Law, Volume 11, Issue 3, August 2021, Pages 276–293.

W. Maxwell, La CJUE dessine le noyau dur d'une future régulation des algorithmes : Cour de justice de l'Union européenne, 6 octobre 2020, aff. C-511/18, La Quadrature du Net. Légipresse, Dalloz, 2020, pp.671-675. ⟨hal-03110335⟩

W. Maxwell, V. Beaudouin, I. Bloch, D. Bounie, S. Clémençon, F. d'Alché-Buc, J. Eagan, P. Mozharovskyi, et J. Parekh, Flexible and Context-Specific AI Explainability: A Multidisciplinary Approach, (March 23, 2020) arXiv: 2003.07703

CONCLUSION

1. La législation européenne sur les activités numérique : un exemple d'hybridation de l'approche par les risques et de l'approche fondée sur le respect des droits ?

De Gregorio et ses co-auteurs présentent la coexistence d'une approche par les risques, et d'une approche fondée sur le respect des droits comme une "constitutionnalisation" de la régulation des acteurs du numérique, une hybridation des deux approches conduisant à un "constitutionnalism optimisé"[188]. Selon les auteurs, l'approche par les risques utilisée dans la régulation des activités numériques en Europe s'infuse de principes constitutionnels de protection des droits. Les auteurs décrivent la présence de l'approche par les risques dans le RGPD, dans le règlement DSA, et dans la proposition de règlement sur l'AI, en caractérisant l'influence de l'approche par les risques dans chaque texte. Pour le RGPD, il s'agirait selon les auteurs d'une approche "*bottom up*", du bas vers le haut, car la définition des risques, et des mesures mises en place pour les réduire, est confiée entièrement au responsable du traitement . Le responsable du traitement assume donc entièrement la responsabilité d'éventuels défaut dans son système de gestion des risques. Pour le règlement DSA, l'approche par les risques apparaît de manière hybride. Les plateformes structurantes sont certes appelées à effectuer une analyse de risques, mais cet exercice est effectué sous le contrôle étroit du régulateur, en l'occurrence la Commission européenne. Enfin, la proposition de règlement sur l'intelligence artificielle intègre l'approche par les risques de manière "*top down*", du haut vers le bas. Le règlement établit lui-même la liste d'applications IA à haut risque et impose aux fournisseurs de ces applications des obligations de gestion de risque renforcées. L'article de De Gregorio et ces co-auteurs présente la présence croissante de l'approche par les risques dans la régulation des activités numériques comme une tendance à insuffler des principes constitutionnels européens dans la législation applicable aux activités numériques.

2. La responsabilité comme clé de lecture de la coexistence de l'approche par les risques et de l'approche fondée sur le respect des droits

La vision hybride de l'approche par les risques et de l'approche fondée sur le respect des droits est particulièrement pertinente pour le règlement européen DSA, dans la mesure où les plateformes structurant qui mettent en place des mesures pour lutter contre un certain type de contenus ne seront pas elles-mêmes responsables des violations de droits fondamentaux qui découlent

[188] De Gregorio, Giovanni and Dunn, Pietro, The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age (March 31, 2022). 59(2) Common Market Law Review 2022, 473-500, Available at SSRN: https://ssrn.com/abstract=4071437 or http://dx.doi.org/10.2139/ssrn.4071437

d'éventuelles failles dans leur système. La responsabilité allégée des hébergeurs pour les contenus postés par les utilisateurs est préservée en grande partie par le règlement DSA. Ainsi, si un système automatique de modération de contenus laissait passer des contenus dommageables, des "faux négatifs", la plateforme ne serait pas, de manière générale, responsable pour les préjudices causés par ce contenu qui a échappé à la détection. La plateforme pourrait être responsable de ne pas avoir mis en place des outils suffisamment efficaces, comme elle s'est engagée à faire dans son analyse de risques, mais elle ne sera pas responsable pour le contenu lui-même.

Le cas des faux positifs est plus complexe. Un faux positif va constituer une violation de la liberté d'expression de la personne qui a posté le contenu. Cette violation découle directement de l'outil mise en place par la plateforme dans la cadre de son programme de gestion de risques. On peut s'interroger sur l'éventuelle responsabilité directe de la plateforme pour cette violation des droits de l'utilisateur découlant directement de l'outil automatique. Pour l'utilisateur, cette responsabilité sera difficile à mettre en œuvre, car la plateforme aura spécifié dans ses conditions d'utilisation qu'elle n'est pas responsable des retraits éventuellement injustifiée de contenus postés par les utilisateurs, et que ceux-ci disposent d'un outil de réclamation permettant de rectifier la situation.

Le cas de responsabilité au titre du RGPD permet une lecture plus claire des relations entre l'approche par les risques et l'approche fondée sur le respect des droits. Le responsable du traitement reste responsable du respect des droits des individus, même dans les cas qui auraient échappé aux mesures de protection mises en place après l'analyse des risques. Ainsi, la responsabilité pour une violation des droits n'est pas affectée par les mesures de prévention mises en place par le responsable du traitement. La responsabilité pour le non-respect d'un droit constitue une barrière de sécurité derrière l'approche par les risques, au cas où une violation échapperait aux dispositifs techniques et organisationnels.

En ce qui concerne le futur règlement sur l'intelligence artificielle, il est trop tôt pour savoir si le régime de responsabilité agira comme un mur de sécurité derrière le système de gestion des risques, comme pour le RGPD, ou si l'on sera en présence d'une situation plus complexe, comme pour le règlement DSA.

3. Des approches fusionnées dans le cadre du travail du législateur, mais séparées dans le cadre des mesures de prévention mises en place par les entreprises

Pour conceptualiser la coexistence entre une approche par les risques, et en approche fondée sur le respect des droits, il faut distinguer deux situations : La première situation est celle du législateur qui essaie de pondérer des droits et intérêts de nature différente pour arriver à un équilibre. Le législateur souhaitera atteindre un objectif - économique, social - efficacement tout en respectant les droits fondamentaux. L'approche par les risques, et l'approche fondée sur le respect des droits, seront toutes les deux présentes dans cette recherche d'équilibre par le législateur. L'équilibre fixé par le législateur sera ensuite soumis à un contrôle de proportionnalité par les tribunaux.

La deuxième situation, et celle qui nous préoccupe dans ce mémoire de synthèse, concerne l'approche par les risques adoptée par les acteurs privés, ou par les régulateurs en charge d'appliquer une législation. Dans cette situation, les analyses de risques seront préparées en partie avec le respect des droits fondamentaux en tête. L'approche fondée sur le respect des droits va influer sur la préparation de l'analyse de risques, et cette influence est justement l'objectif du législateur. Mais on ne peut pas dire que l'approche par les risques et l'approche fondée sur le respect des droits fusionnent dans cette situation.

L'approche par les risques va se nourrir de l'approche fondée sur le respect des droits, mais pas l'inverse. La barrière entre les deux approches est poreuse dans un seul sens. L'approche fondée sur le respect des droits ne va jamais être influencée par l'analyse de risques effectués par l'entreprise privée. L'approche par le respect des droits va garder son autonomie et son intégrité.

L'aspect autonome de l'approche fondée sur le respect des droits devient claire si l'on considère la violation d'un droit garanti par le chapitre III du RGPD. Dans ce cas, le responsable du traitement peut éventuellement être sanctionné de ne pas avoir mis en place des mesures appropriées en application de l'article 25 du RGPD. Le responsable du traitement peut également être sanctionné, ou au moins être tenu responsable, pour le non-respect d'un droit de la personne concernée. Pour ce deuxième fondement de responsabilité, le caractère approprié des mesures de prévention mises en place par le responsable du traitement n'effacera ni la violation, ni la responsabilité qui en découle. Les deux types de responsabilité sont tout à fait distinctes et l'approche par le risque n'aura aucun impact sur le deuxième type de responsabilité.

Cette vision d'une protection à double couche, une première couche technique et organisationnelle fondée sur les risques, et une deuxième couche juridique fondée sur le respect des droits, semble bien s'adapter au RGPD. Elle pourrait également s'appliquer à des recommandations et décisions

d’un régulateur comme la CNIL chargé d’appliquer une loi. Le régulateur adoptera une recommandation fondée sur une analyse de risques qui tient compte également de la protection des droits. Une entreprise qui applique la recommandation mais viole un droit individuel ne pourra pas s’exonérer du fait qu’elle a appliqué la recommandation.

Il est trop tôt pour savoir si cette vision “double couche” pourra expliquer la coexistence d’une approche par les risques et une approche fondée sur les droits dans le règlement DSA et le futur règlement européen sur l’IA.