SciencesPo

CHAIRE DIGITAL, GOUVERNANCE ET SOUVERAINETÉ

Le chiffrement est-il un droit fondamental ?

Une étude de cas sur la réglementation du CSAM dans l'UE

Stavroula Chousou, Julia Magaud,

Ludovica Pavoni & Morgan Williams

Approches comparatives de la réglementation des grandes technologies (printemps 2023)

Professeur Florence G'sell

Avril 2023

SciencesPo
CHAIRE DIGITAL, GOUVERNANCE ET SOUVERAINETÉ

Table des matières

Résumé iii
Introduction 1
1. Qu'est-ce que le chiffrement ? 2
1.1 Différents types de chiffrement 3
1.2 Le chiffrement de bout en bout (E2EE) 4
2. Avantages et risques liés au chiffrement 6
2.1 Les avantages liés au chiffrement 7
2.2 Les risques liés au chiffrement 8
3. Comment l'UE tente-t-elle de réglementer le chiffrement ? 11
3.1 Champ d'application juridique européen du chiffrement 11
3.2 Premiers pas vers la réglementation (1995-2016) 12
3.3 Premier débat européen sur le chiffrement : la prévention du terrorisme 13
3.4 Deuxième et actuel débat européen sur le chiffrement : le matériel pédopornographique 15
4. Cette proposition est-elle la bonne méthode pour lutter contre le chiffrement ? 17
4.1 Critiques législatives 17
4.2 Critiques politiques 19
4.3 Quelle est la suite des événements ? 21
5. Faut-il instaurer un droit fondamental au chiffrement dans l'UE ? 23
5.1 Qu'est-ce qu'un droit fondamental ? 23
5.1.1 Droits fondamentaux des pays membres de l'ONU en matière de cryptage 24
5.1.2 Droits fondamentaux liés au cryptage dans l'Union européenne 24
5.2 L'évolution des droits fondamentaux dans une UE numérisée 25
5.3 Mais qu'est-ce qui rendrait fondamental le droit au cryptage ? 27
6. Recommandations politiques 32
6.1 Recommandations en matière de politique législative 32
6.2 Recommandations techniques 33
Conclusion 35
Bibliographie 36

SciencesPo
CHAIRE DIGITAL, GOUVERNANCE ET SOUVERAINETÉ

Résumé

Deux débats politiques actuels se heurtent à un paysage juridique européen complexe et en pleine évolution : est-il possible de protéger les enfants et d'empêcher la diffusion de matériel pédopornographique lorsque la technologie de chiffrement de bout en bout (E2EE) rend les messages inaccessibles aux forces de l'ordre ? Alors que les contenus pédopornographiques continuent de proliférer sur les plateformes de messagerie en ligne, les débats politiques et les longues procédures judiciaires cherchent à créer des portes dérobées pour les procédures pénales et des obligations pour les entreprises de télécommunications et de médias en ligne de scanner leurs services pour y trouver des preuves de contenus pédopornographiques. Certains affirment que le cryptage à l'ère de la numérisation n'est pas à débattre, mais qu'il est plutôt fondamental. Le chiffrement protège la vie privée et la sécurité en ligne, deux droits fondamentaux incontestés. Mais le chiffrement est-il lui-même un droit fondamental ? Que se passe-t-il lorsqu'un droit fondamental permet de commettre des crimes contre les personnes les plus vulnérables de notre société ? Existe-t-il un moyen de protéger les enfants contre le CSAM tout en protégeant le droit à la confidentialité des communications en ligne pour tous ? En examinant le rôle du cryptage et le cadre réglementaire actuel dans l'UE, en mettant l'accent sur la proposition en cours d'élaboration visant à prévenir et à combattre les abus sur les enfants en filtrant les messages privés, nous établissons le caractère fondamental du cryptage dans la vie privée de tous les utilisateurs d'Internet, y compris les enfants.

Introduction

Chaque jour, des milliards d'utilisateurs communiquent par messagerie privée sur des plateformes telles que Facebook, Twitter et Signal. Malheureusement, la confidentialité de ces plateformes peut être exploitée à grande échelle, donnant lieu à du spam, du harcèlement, de la propagation de fausses informations, de la propagande terroriste et de la diffusion de matériel pédopornographique. D'une part, l'utilisation du chiffrement sur les plateformes protège la vie privée des utilisateurs et, d'autre part, les auteurs de ces actes échappent à l'application de la loi. Les gouvernements du monde entier ont proposé ou mis en œuvre des mesures exigeant l'accès aux données cryptées, arguant que celles-ci sont nécessaires à la prévention et à la détection des délits. Toutefois, cela soulève d'importantes questions sur l'équilibre entre la vie privée et la sécurité, ainsi que sur les droits des individus à protéger leurs informations personnelles. Dans l'Union européenne en particulier, les scandales de ces dernières années concernant le matériel pédopornographique en ligne ont suscité de vives inquiétudes quant aux moyens et aux procédures dont nous disposons pour protéger les enfants en ligne. L'ambivalence technologique de l'Union européenne s'est traduite par une multiplication des débats sur le rôle du chiffrement dans l'hébergement de criminels dangereux à cet égard. Mais ces craintes sont-elles fondées en ce qui concerne les aspects techniques et les fonctions du cryptage ? Et si c'est le cas, quelles sont les alternatives ? Le chiffrement est-il un mal nécessaire, une exigence *ad hoc* ou une clause de sécurité d'une société toujours numérisée ?

Dans cette analyse politique, nous examinerons si le chiffrement est un droit fondamental et les conséquences de cette décision sur l'approche de l'UE en matière de réglementation du chiffrement et de protection des enfants contre les logiciels malveillants. La structure du rapport est la suivante : expliquer ce qu'est le chiffrement (section 1) et découvrir les enjeux associés à la réglementation du chiffrement (section 2), présenter la chronologie des réglementations concernant le chiffrement dans l'UE (section 3) et leurs défauts (section 4), et enfin, clarifier si le chiffrement devrait être protégé en tant que droit

fondamental (section 5) et comment l'UE devrait plutôt aborder la réglementation du chiffrement (section 6).

1. Qu'est-ce que le chiffrement ?

Le chiffrement est le processus par lequel l'information est convertie en codes secrets qui cachent la véritable signification de l'information. L'OCDE le définit comme "la transformation de données par l'utilisation de la cryptographie pour produire des données inintelligibles (données cryptées) afin d'en assurer la confidentialité" (p. 9). En d'autres termes, il s'agit d'un moyen de brouiller les données afin que seules les parties autorisées puissent comprendre l'information ; en termes techniques, il s'agit du processus de conversion d'un *texte clair* lisible par l'homme en un texte incompréhensible, également connu sous le nom de *texte chiffré*.

Image 1 : Représentation schématique du fonctionnement du cryptage

Source : "Qu'est-ce que le chiffrement ? | Types de chiffrement". *CloudFlare*.

De cette description, on peut déduire que le chiffrement est un processus qui est presque intrinsèque à l'histoire du monde, étant donné qu'au fur et à mesure que la civilisation progressait, les méthodes de dissimulation d'informations délicates évoluaient également. Il existe des preuves de l'existence de méthodes de chiffrement qui remontent aux anciens Égyptiens, qui utilisaient des hiéroglyphes hyper-compliqués pour empêcher les personnes de niveau inférieur de comprendre les informations privilégiées, et aux Grecs, au huitième siècle avant J.-C., qui ont mis au point des méthodes pour confondre les informations provenant de leurs ennemis. Le mathématicien arabe Al-Kindi a réalisé des progrès significatifs dans le domaine du cryptage en étudiant les statistiques relatives à la fréquence des lettres dans un texte. Il en a rendu compte dans son livre *On Decrypting Encrypted Correspondence (Du décryptage de la correspondance cryptée)*, qui est considéré à

ce jour comme le premier ouvrage sur le sujet. D'autres stratégies de cryptage ont été observées au cours des siècles, mais nous avons assisté à un pic des technologies de cryptage dans les années 1900, avec des cryptages matériels développés par l'armée pour protéger les informations sensibles des services de renseignement étrangers. Pendant la Seconde Guerre mondiale, les technologies de cryptage ont connu des avancées significatives, comme en témoigne le décryptage de l'*Enigma* allemand par Alan Turing. (Schlesinger et Yanisky-Ravid, 2022, p. 574).

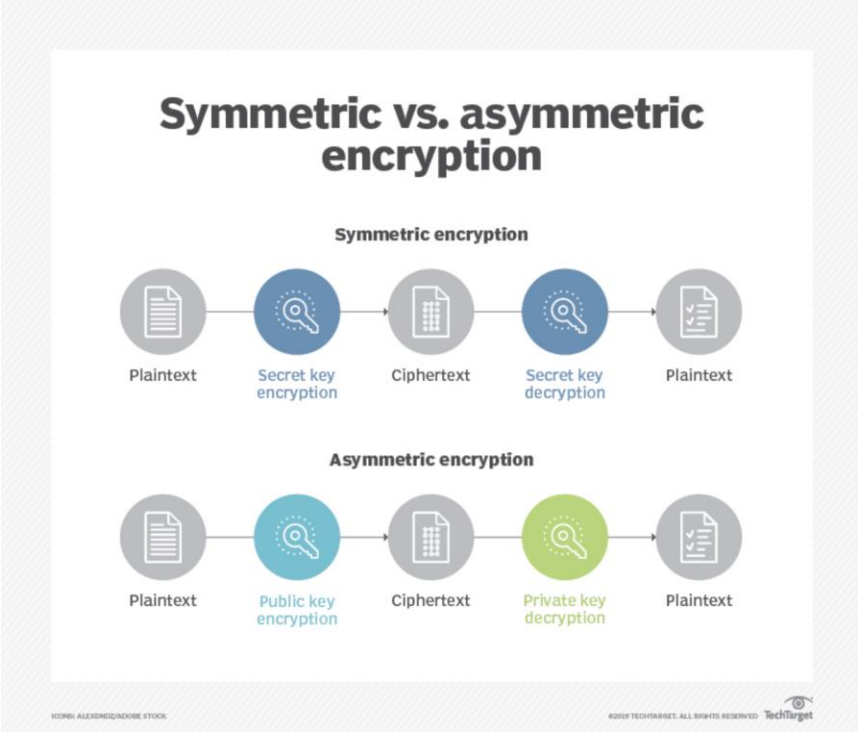
Lorsque le monde est entré dans l'ère de l'information et de la technologie, nous avons assisté à l'avènement de l'informatique de pointe qui a donné naissance à un nouveau type de protection : le chiffrement numérique. À mesure que les technologies informatiques ont progressé et que la disponibilité de l'informatique numérique s'est généralisée, il est de plus en plus évident que l'utilisation du chiffrement est passée d'un usage centré sur l'État à un accès à un éventail plus large d'acteurs et d'utilisateurs. En effet, après avoir été étroitement lié à la protection des secrets d'État et avoir été utilisé à des fins militaires, le chiffrement fait aujourd'hui partie du domaine plus large de la cryptographie, qui est largement accessible aux utilisateurs ordinaires. La technologie a progressé au point que l'utilisateur moyen peut utiliser des méthodes de cryptage potentiellement inviolables sans même s'en rendre compte.

1.1 Différents types de cryptage

Il existe deux types de cryptage, le cryptage symétrique et le cryptage asymétrique, également connu sous le nom de cryptage à clé publique. Ces deux types sont définis comme suit : (a) le **chiffrement symétrique** est une méthode plus ancienne qui est rapide car elle ne nécessite qu'une seule clé. En raison de ses meilleures performances et de sa rapidité, il est généralement utilisé pour le chiffrement en masse (par exemple, le cryptage des bases de données) et la clé secrète n'est généralement accessible qu'à la base de données elle-même, tandis que (b) le **chiffrement asymétrique** utilise deux clés distinctes, l'une pour le cryptage et l'autre pour le décryptage. Cette première clé est publique, utilisable par tous, tandis que la seconde est privée et seul le destinataire authentifié y a accès (Conrad et al., 2012).

La principale différence entre les deux est que le chiffrement symétrique ne nécessite qu'une seule clé, et toutes les parties utilisent la même clé secrète pour chiffrer et déchiffrer les informations. Le chiffrement asymétrique, quant à lui, nécessite deux clés distinctes, l'une utilisée pour le chiffrement et l'autre pour le déchiffrement (Prima Santoso et al., 2018, p. 2). Une deuxième différence entre les deux est la longueur des clés utilisées. Le chiffrement symétrique nécessite une clé plus courte, qui dépend bien sûr du niveau de sécurité requis, tandis que le chiffrement asymétrique nécessite des clés plus longues, étant donné que les deux clés différentes doivent être liées et suffisamment complexes pour ne pas être craquées.

Image 2 : Chiffrement symétrique et asymétrique



Source : Brush, K., Rosencrance, L., & Cobb, M. (2021, septembre). "Chiffrement asymétrique (cryptographie à clé publique)". TechTarget.

1.2 Chiffrement de bout en bout (E2EE)

Dans le cadre du présent document, nous nous concentrerons uniquement sur le chiffrement asymétrique, car il s'agit d'une grande famille qui comprend ce que l'on appelle le chiffrement de bout en bout (E2EE), qui est au cœur du débat sur la question de savoir si le chiffrement est un droit fondamental ou non. Le chiffrement de bout en bout est un processus

de chiffrement des données entre des dispositifs de sorte que seuls l'expéditeur et le destinataire peuvent voir le contenu du message. Cela signifie que cette méthode crypte les messages avant qu'ils ne soient envoyés et les décrypte après qu'ils ont été livrés[1] ; grâce à ce processus, les messages eux-mêmes et les données qu'ils contiennent sont sécurisés (Knodel et al., 2021). Les données chiffrées ne peuvent donc être lues que par les deux parties - l'expéditeur et le destinataire - et personne d'autre ne peut lire le message crypté, ni les pirates informatiques, ni les gouvernements, ni le serveur par lequel les données transitent.

Cette méthode de chiffrement peut sembler familière, et elle l'est en effet car elle est largement utilisée dans des applications auxquelles le commun des mortels accède quotidiennement. Les applications de messagerie telles que WhatsApp, Telegram et Signal utilisent toutes l'E2EE pour garantir la confidentialité des conversations entre les utilisateurs. Les fournisseurs de services de messagerie et toutes les grandes applications de communication, telles que Zoom, ainsi que les plateformes de médias sociaux ont également introduit cette méthode de cryptage pour garantir une communication sécurisée (Kamara et. al, 2022, p. 14). Pour mieux comprendre le fonctionnement de l'E2EE, nous donnons l'exemple suivant :

"Si nous considérons deux utilisateurs de WhatsApp qui s'envoient des SMS, nous savons que leurs messages - et donc leurs données - passent par un serveur WhatsApp lorsqu'ils sont transmis d'un côté à l'autre. L'E2EE se produit au niveau de l'appareil, ce qui signifie que les messages sont cryptés avant de quitter un appareil par une clé publique accessible à tous, mais qu'ils ne sont décryptés que par la clé privée du destinataire lorsqu'ils atteignent l'autre appareil."

En cryptant les informations au niveau de l'appareil et non au niveau du serveur, l'E2EE conserve les informations cryptées et le fournisseur de services lui-même ne peut pas intercepter ces données pour les décrypter. Cela signifie que les autorités chargées de l'application de la loi et les agences gouvernementales ne peuvent pas non plus accéder aux

[1] Si l'on relie le concept de l'E2EE au cryptage asymétrique, la clé publique est utilisée pour crypter les données et la clé privée, qui n'est disponible que pour le propriétaire, est utilisée pour décrypter les données.

données, même si elles en ont l'autorisation. Par conséquent, en utilisant l'E2EE, personne ne peut accéder aux données en dehors des deux parties, en théorie.

2. Avantages et risques liés au chiffrement

2.1. Vue d'ensemble

L'utilisation du chiffrement de bout en bout (E2EE) dans les services de messagerie instantanée, tels que WhatsApp, présente à la fois des risques et des avantages pour les utilisateurs finaux, les services de messagerie instantanée et les gouvernements. Les gouvernements, en particulier, sont menacés par l'E2EE parce qu'il crée des obstacles à la surveillance et à la répression des activités illégales sur l'internet. De leur côté, les services de messagerie instantanée souhaitent protéger la vie privée de leurs utilisateurs (Endely, 2018, p. 96). En fin de compte, qualifier l'E2EE de technologie "bonne" ou "nuisible" dépend de la priorité accordée par la partie prenante à la protection de la vie privée des individus par rapport à la sécurité publique. Cela dit, il n'est pas évident que la plupart des utilisateurs finaux comprennent exactement ce qu'est l'E2EE, les risques et les avantages associés à cette technologie, ainsi que les enjeux de ce débat (Kamara, 2022, p. 12). Cette section démêle les différents arguments qui entourent l'E2EE (voir tableau 1) et déboulonne les mythes récurrents.

Tableau 1. Avantages et risques de l'E2EE par partie prenante

Partie prenante	Avantages		Risques	
Utilisateurs finaux	I.	Amélioration de la protection de la vie privée	I.	Peut être utilisé à des fins illégales
	II.	Protection contre les violations de données	II.	Il peut être difficile de gérer différentes clés de chiffrement
	III.	Une communication digne de confiance		
	IV.	Libre expression		
Services de messagerie instantanée	I.	Protection contre les violations de données	I.	Il est plus difficile de contrôler les contenus nuisibles ou illégaux sur la plateforme
Gouvernements	I.	Protection contre les	I.	Difficile de contrôler les

		violations de données	activités criminelles
	II.	Promouvoir la liberté d'expression en ligne	

2.1 Avantages liés au chiffrement

Les avantages de l'E2EE se caractérisent par une sécurité renforcée et une protection contre les violations de données. À la suite des révélations de Snowden en 2013 et du scandale Cambridge Analytica en 2016, les utilisateurs de médias sociaux et de messageries instantanées sont de plus en plus conscients que leurs données personnelles risquent d'être utilisées à mauvais escient par les gouvernements et les grandes entreprises dans le cadre de violations de données (Song, 2020, p. 4). Le scandale Cambridge Analytica a révélé comment des gouvernements étrangers pouvaient exploiter les informations personnelles de plus de 50 millions d'utilisateurs de Facebook pour exploiter les profils psychologiques des utilisateurs et influencer les élections démocratiques. Nombre de ces utilisateurs de Facebook se sont sentis profondément perturbés par le fait que leurs informations personnelles étaient collectées et vendues sans leur consentement, ce qui, à son tour, a entamé leur confiance dans la plateforme de médias sociaux (Song, 2020, p. 5). En réponse, de nombreux services de messagerie instantanée ont été contraints de rassurer leurs entreprises et les particuliers sur la protection de leurs données contre la surveillance et les écoutes gouvernementales (Endely, 2018, p. 96). C'est probablement cette pression qui a motivé la décision de Meta de tester l'E2EE sur Facebook Messenger en 2022.

Les utilisateurs de services de messagerie instantanée avec E2EE peuvent être assurés que leurs conversations ne peuvent être lues que par eux-mêmes et par personne d'autre, y compris le fournisseur de services ou tout autre tiers. Les données étant cryptées aux deux extrémités, il est difficile pour les pirates ou les entreprises de les voler ou de les vendre. Avec l'E2EE, les consommateurs et les entreprises ont accès à un mode de communication fiable, où ils peuvent partager en toute confiance leurs informations personnelles ou confidentielles, telles que celles relatives à leurs antécédents médicaux ou à leurs finances. Outre les services de messagerie, l'E2EE permet de sécuriser les transactions en ligne, telles que les opérations bancaires ou le commerce électronique.

Les réglementations relatives à la protection des données, telles que le règlement général sur la protection des données (RGPD) dans l'Union européenne (UE) et la loi californienne sur la protection de la vie privée des consommateurs (CCPA) soulignent le rôle important du cryptage pour garantir la sécurité des consommateurs et des entreprises (Song, 2020, p. 6). Bien qu'aucune des deux réglementations n'exige explicitement le chiffrement, elles recommandent fortement aux services de messagerie de chiffrer les messages personnels. La CCPA va jusqu'à établir une sphère de sécurité qui permet aux entreprises d'éviter les sanctions financières si elles cryptent les données personnelles. Dans l'ensemble, les agences gouvernementales ont indiqué que le cryptage est préférable pour protéger la sécurité des données à caractère personnel. Toutefois, elles n'ont pas précisé le type de cryptage. Par conséquent, cette position n'est pas explicitement en conflit avec d'autres agences gouvernementales qui émettent des réserves quant à l'utilisation de l'E2EE.

Les défenseurs de l'E2EE soutiennent que la technologie favorise la liberté d'expression en empêchant l'ingérence des États et des entreprises (Kamara, 2022, p. 12 ; Song, 2020, p. 6 ; Grover, 2021, Introduction). Cet outil est particulièrement intéressant pour les personnes vivant dans des régimes autoritaires, où les groupes minoritaires, les journalistes, les chercheurs, les avocats et la société civile ont besoin d'un espace pour communiquer librement sans craindre la surveillance ou le harcèlement de l'État (Grover, 2021, Introduction). Compte tenu de l'importance croissante de la communication en ligne dans notre société, les interdictions générales de l'E2EE peuvent donner aux États une capacité sans précédent de contrôler et de surveiller les conversations et les données privées des citoyens. En conséquence, l'interdiction de l'E2EE exposerait les individus au risque d'être victimes de régimes oppressifs ou autoritaires (Song, 2020, p. 12). Au contraire, la préservation de l'E2EE protège et préserve "l'individualisme et la sécurité personnelle" (Song, 2020, p. 11).

2.2 Risques liés au chiffrement

La discussion opposée à l'E2EE est caractérisée par la criminalité et les menaces pour la sécurité publique. Étant donné la nature fermée de l'E2EE, il est impossible pour les

gouvernements de surveiller les activités criminelles et d'enquêter sur les crimes. Par conséquent, si les services de messagerie instantanée ne peuvent pas accéder aux conversations privées, les criminels ou les terroristes peuvent profiter de la confidentialité pour organiser des crimes (Kamara et. al, 2022, p. 15 ; Song, 2020, p. 7 ; Grover, 2021, Introduction).

Les détracteurs de l'E2EE font valoir que le secret peut constituer une menace pour la sécurité nationale, dans le cas d'attaques terroristes. Par exemple, les terroristes qui ont planifié les attentats de 2015 à Paris ont utilisé Telegram, un service de messagerie instantanée protégé par l'E2EE, pour organiser et diffuser leur propagande (Song, 2020, p. 8). Ces terroristes ont pu collaborer et déléguer des tâches en toute sécurité, ce qui a entraîné la mort de 130 personnes. Sans une plateforme de messagerie sécurisée, il aurait peut-être été plus difficile pour les terroristes de coordonner les différents groupes et de mener une attaque de cette ampleur. Il est possible que le gouvernement français ait été en mesure d'identifier des activités suspectes et d'empêcher l'attentat s'il avait eu accès à un canal de retour sur la plateforme de messagerie.

Les criminels et les non-criminels se voient attribuer les mêmes droits et privilèges en matière de protection de la vie privée et de sécurité sur les plates-formes de messagerie instantanée avec l'E2EE. Outre le fait qu'elle empêche l'identification des activités terroristes, cette technologie peut également être utilisée à mauvais escient par des criminels non terroristes, tels que les trafiquants de drogue ou les pédophiles, pour dissimuler leurs activités criminelles (Song, 2020, p. 8). Non seulement les plateformes de messagerie instantanée E2EE permettent aux criminels de collaborer sans surveillance ni risque de plages de données, mais il est impossible pour les plateformes de messagerie instantanée de fournir aux forces de l'ordre des preuves numériques pour enquêter sur le crime (Grover, 2021, Introduction). Ces arguments sont particulièrement pertinents dans le cadre de la procédure engagée par l'UE contre l'E2EE utilisé pour la distribution de matériel pédopornographique, qui sera examinée plus en détail ci-dessous.

En réponse à ces accusations, les partisans de l'E2EE font valoir que les criminels et les terroristes trouveront d'autres motifs de communication s'ils ne peuvent plus utiliser les

services de messagerie protégés par l'E2EE, tels que Telegram (Song, 2020, p. 8). Par conséquent, une interdiction générale de l'E2EE n'entraînerait pas une réduction significative des activités criminelles.

L'E2EE limite la capacité des plateformes de messagerie instantanée à modérer le contenu en cas d'activités illégales ou préjudiciables, telles que les discours haineux ou la cyberintimidation. En théorie, en tant qu'hébergeurs, les services de messagerie instantanée ont le pouvoir de modérer les contenus qui, bien que légaux, violent leurs directives communautaires ou leurs conditions de service. Les hôtes adoptent des approches différentes en matière de modération du contenu en fonction de leur base d'utilisateurs, de leur modèle commercial ou d'autres considérations (Kamara et. al, 2022, p. 8). D'un point de vue commercial, la diffusion de contenus illégaux ou préjudiciables sur leur plateforme crée des risques pour la réputation de l'entreprise. Toutefois, l'E2EE veille à ce que le service de messagerie instantanée n'ait pas accès au contenu partagé sur sa plateforme, ce qui l'empêche d'exercer une modération du contenu. Même s'il était possible pour les services de messagerie instantanée de filtrer les messages, il est difficile de distinguer les contenus illégaux ou préjudiciables des contenus qui n'enfreignent pas les lignes directrices de la communauté de l'hôte, car ils ne présentent pas de caractéristiques distinctes des contenus inoffensifs (Kamara et. al, 2022, p. 16).

Bien que l'E2EE soit censé accroître la sûreté et la sécurité, il existe des "failles et des risques inconnus" qui ont miné sa fiabilité (Song, 2020, p. 8). Comme la technologie continue d'évoluer, il est concevable que les progrès technologiques du logiciel s'accompagnent de pépins ou de faiblesses. Pour empêcher les tiers d'accéder aux messages, les plateformes de messagerie instantanée, telles que Telegram, ont mis en place une politique d'effacement des messages dès qu'ils sont décryptés, ce qui constitue une deuxième couche de sécurité. Cependant, en juin 2018, un service de messagerie en ligne, Signal, n'a pas chiffré une partie des messages déchiffrés. Bien que ces pépins techniques soient rares, ils démontrent que l'E2EE n'est pas toujours complètement sécurisé.

3. Comment l'UE tente-t-elle de réglementer le cryptage ?

3.1 Le champ d'application juridique européen du chiffrement

Le secteur de la science et de la technologie relève de la catégorie des **compétences partagées au sein de l'UE** (article 4 du TFUE[2]). Par conséquent, l'UE et les États membres sont en mesure de légiférer et d'adopter des actes juridiquement contraignants sur des questions connexes, telles que le chiffrement. Toutefois, les États membres ont la possibilité d'imposer leurs propres lois et dispositions nationales sur l'utilisation et l'accès au chiffrement, pour autant qu'elles n'entrent pas en conflit avec d'autres textes législatifs de l'UE, par exemple le GDPR, ses directives relatives au chiffrement, etc. Il en résulte une hétérogénéité accrue de la réglementation en matière de chiffrement et de graves lacunes numériques entre les États membres. L'élément d'hétérogénéité fait référence au fait que parmi les États qui ont une position juridique sur le chiffrement, il existe un large éventail de degrés d'alerte et d'importance attribuée. En outre, les États utilisent des approches et des outils très divers pour faire appliquer leurs réglementations. D'autre part, de nombreux pays n'ont pas encore de législation nationale sur le chiffrement, ce qui reflète leur niveau d'intégration numérique (Global Partners Digital, 2023). Plus précisément, seuls 11[3] des 27 États membres disposent d'une forme quelconque de disposition légale sur le chiffrement.

L'absence de compétence désignée de l'UE a entraîné une position européenne fragmentée sur la question, tant au niveau national qu'international, ce qui a permis l'émergence de deux grands débats : (1) l'un portant sur la position des entreprises de télécommunications et leur compétence en matière de déchiffrement des données dans le cadre d'enquêtes criminelles, et l'autre (2) portant spécifiquement sur la grave question des cas de maltraitance d'enfants dans l'espace numérique de l'UE. Cette question est d'autant plus problématique que les technologies de cryptage se développent rapidement, reflétant le besoin accru et l'urgence de protection et de respect de la vie privée.

---

[2] "Les États membres exercent leur propre compétence lorsque l'UE n'exerce pas, ou a décidé de ne pas exercer, sa propre compétence." https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12008E004&from=EN

[3] Irlande, France, Allemagne, Belgique, Pays-Bas, Danemark, République tchèque, Croatie, Grèce, Estonie et Finlande.

3.2 Les premiers pas vers la réglementation (1995-2016)

Au niveau européen, la première loi globale sur la protection des données a été la directive sur la protection des données (95/46/CE)[4] , adoptée en 1995. Cette directive n'abordait pas spécifiquement le cryptage, mais exigeait des États membres qu'ils prennent les mesures appropriées pour protéger les données à caractère personnel contre la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés, de manière accidentelle ou illicite. En 1999, l'UE a adopté la directive sur les signatures électroniques (1999/93/CE)[5] , qui fournit un cadre juridique pour l'utilisation des signatures et des certificats électroniques. La directive reconnaît l'utilisation de techniques cryptographiques, y compris le cryptage, dans les activités concernées. En 2002, avec la directive "vie privée et communications électroniques" (2002/58/CE)[6] , les États membres et les entreprises ont été tenus de garantir la confidentialité et la sécurité de leurs communications, des réseaux et des services sous-jacents. En 2006, l'UE a adopté la décision-cadre relative au mandat d'arrêt européen (2002/584/JAI)[7] , qui établit la procédure d'émission et d'exécution des mandats d'arrêt entre les États membres de l'UE. Cette décision impose aux États membres de s'assurer que toute demande d'interception de communications électroniques est autorisée par un tribunal ou un autre organe indépendant et que **l'interception est nécessaire et proportionnée**.

En 2008, l'UE a modifié la directive "vie privée et communications électroniques" avec le paquet télécoms (2009/140/CE)[8] , qui exige des États membres qu'ils veillent à ce que toute interférence avec les communications électroniques, y compris le cryptage, **soit autorisée par la loi, nécessaire, proportionnée et soumise à des garanties adéquates**. Le programme de Stockholm a été introduit en 2010[9] , définissant les priorités de l'UE en matière de justice et

[4] Disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01995L0046-20031120
[5] Disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01999L0093-20081211
[6] Disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219
[7] Disponible à l'adresse suivante : wur-lex.eu/Framework Decision on the European Arrest Warrant (2002/584/JHA)
[8] Disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/fr/ALL/?uri=CELEX:32009L0140
[9] Disponible à l'adresse suivante : eur-lex.europa.eu/ Stockholm Programme 2010-2014

d'affaires intérieures pour la période 2010-2014, appelant à des mesures pour renforcer la lutte contre les crimes graves et le terrorisme, y compris l'utilisation de l'interception et du décryptage des communications électroniques. En 2012, la directive sur la protection des données a été remplacée par le règlement sur la protection des données (UE) 2016/679[10] . Il exigeait des entreprises qu'elles mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données à caractère personnel, y compris le cryptage et la pseudonymisation.

Jusqu'en 2016, les lois et directives de l'UE favorisaient généralement l'utilisation du chiffrement comme moyen de protection des données à caractère personnel et des communications électroniques. Elles comprenaient des dispositions sur l'interception et le décryptage dans des circonstances spécifiques ; ces dispositions étaient assez ambiguës, car elles ne précisaient pas ce qui constituait exactement une nécessité ou une action proportionnée. Dans l'ensemble, les dispositions relatives au chiffrement manquaient jusqu'à présent de nuances techniques et de précision.

3.3 Un premier débat européen sur le chiffrement : la prévention du terrorisme

En 2016, de nombreux pays européens ont connu des attaques terroristes dévastatrices, dont les plus graves ont eu lieu à Paris et à Nice. Les experts ayant suggéré que les groupes terroristes privilégiaient des canaux de communication mieux cryptés pour leurs communications, la France s'est lancée dans une campagne nationale visant à rendre toutes les entreprises de télécommunications opérant dans sa juridiction conformes au principe de divulgation complète dans le cadre d'enquêtes criminelles. Au niveau de l'UE (Acharya et al., 2017), la France a proposé à la Commission européenne une loi qui obligerait les plateformes de communication à coopérer pleinement aux enquêtes judiciaires visant à traquer les terroristes en donnant aux autorités un accès total aux données requises (Reuters, 2016).

Cependant, le chiffrement était trop nouveau sur la scène politique européenne et la proposition de la France a été accueillie par une UE divisée. De nombreux pays européens,

[10] Disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

notamment l'Allemagne et les Pays-Bas, se sont démarqués de la position française en réaffirmant leur intention de ne pas saboter le développement de méthodes de chiffrement meilleures et plus efficaces (Benner & Hohmann, 2016). L'Allemagne a souligné son ambition de devenir un centre européen du chiffrement, ce qui n'est pas surprenant, car l'Allemagne suit une voie similaire à celle des États-Unis où, malgré la présence et l'activité de groupes terroristes, il existe une culture du piratage gouvernemental d'investigation (Acharya et al., 2017). Cependant, la France n'était pas la seule à avoir des exigences ; la Hongrie et le Royaume-Uni (alors européen) avaient leurs propres débats internes sur la légalité et les limites des services cryptés (Benner & Hohmann, 2016).

Dans ce contexte, l'Organisation européenne de cybersécurité (ENISA) a fermement soutenu sa position précédemment exprimée selon laquelle le renforcement des portes dérobées de chiffrement et la mise en œuvre de protocoles et de techniques de chiffrement actualisés constituent la seule mesure viable pour faciliter les enquêtes des services répressifs sans mettre en danger la vie privée des citoyens qui utilisent ces plateformes (Stupp, 2016), comme le précise la directive NIS de l'ENISA (ENISA, 2016). La même année, une autre référence réglementaire importante a été atteinte à cet égard. Le règlement général sur la protection des données (RGPD) a été adopté en 2016 et est entré en vigueur en mai 2018. Le GDPR exigeait des entreprises qu'elles mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données à caractère personnel. Ces mesures peuvent prendre la forme d'un chiffrement ou d'une pseudonymisation. Le GDPR est devenu la base du cadre de protection des données dans l'UE, cependant, comme indiqué dans la section 2.3, il n'y a pas de dispositions explicites qui obligent les services à utiliser le chiffrement. Le GDPR impose seulement aux entreprises et aux organisations d'appliquer les meilleures pratiques pour la protection des données personnelles qu'elles stockent et/ou traitent.

En effet, au cours de la période 2016-2019, l'UE a été confrontée à divers égards à son manque de réflexion préemptive. Néanmoins, ce débat a donné lieu à des efforts continus pour mettre à jour et renforcer les règles sur le chiffrement et les communications électroniques dans l'UE, en commençant en 2017 par une série de mesures non législatives

visant à explorer la question et à créer des ressources et des outils de formation pour les forces de l'ordre (DigitalEurope, 2020). Ces groupes de travail préliminaires ont lentement ouvert la voie à des règlements et directives plus précis.

3.4 Un deuxième et actuel débat européen sur le cryptage : les documents relatifs à des abus sexuels sur des enfants

Au cours des dix dernières années, le nombre de signalements d'abus sexuels d'enfants sur l'internet a considérablement augmenté. Les plaintes mondiales pour maltraitance d'enfants sont passées de 23 000 en 2010 à plus de 725 000 en 2019 (NCMEC, n.d.). Près de neuf URL sur dix signalées pour du matériel pédopornographique (CSAM) sont hébergées dans l'UE, ce qui en fait le continent où la concentration de CSAM est la plus élevée au monde (Koomen, 2021). En fait, Europol prévoit une augmentation significative des signalements de CSAM en 2020, souvent sur des réseaux peer-to-peer (IOCTA, 2020, p. 34-37). Ce phénomène est lié à la pandémie, car l'augmentation du nombre de criminels restant chez eux a entraîné une hausse de la demande de CSAM allant jusqu'à 25 % dans certains États membres de l'UE. Tragiquement, l'offre a augmenté pour répondre à cette forte hausse (Koomen, 2021). Plus de 94 % des incidents signalés concernaient le filtrage de contenu sur Facebook et ses applications, notamment Messenger, Instagram et WhatsApp. En 2020, Facebook a dévoilé ses projets de réseau social "axé sur la protection de la vie privée", y compris la mise en œuvre de l'E2EE dans l'ensemble de ses services, ce qui a empêché les forces de l'ordre et Facebook d'identifier 70 % des cas de CSAM sur Facebook (Koomen, 2021).

Pour faire face à ces problèmes, la Commission européenne a lancé deux stratégies importantes en juillet 2020, l'une pour lutter spécifiquement contre les abus sexuels sur les enfants et l'autre pour mettre à jour la stratégie de l'Union européenne en matière de sécurité (Europa, 2020) d'une manière plus générale. Dans les deux cas, le chiffrement est considéré, du point de vue de la sécurité publique, comme un moyen pour les auteurs d'abus sexuels de "masquer *leur identité*" et de "*dissimuler leurs actions aux forces de l'ordre*" (Koomen, 2021). Plus précisément, la stratégie de lutte contre les abus sexuels commis sur des enfants comprend des réglementations sectorielles, des efforts opérationnels et des solutions

techniques, qui soulignent le rôle du secteur privé et appellent les entreprises à "*détecter et signaler les abus sexuels commis sur des enfants dans les communications E2EE".* La stratégie actualisée de l'Union européenne en matière de sécurité (2020) a confirmé que l'UE "*encouragera une approche qui maintient l'efficacité du chiffrement dans la protection de la vie privée et la sécurité des communications, tout en apportant une réponse efficace à la criminalité et au terrorisme*".

En septembre 2020, une fuite a révélé les détails de la réflexion de la Commission européenne sur les "solutions" techniques permettant de détecter le CSAM dans les communications E2EE. Le document était plus nuancé techniquement que la rhétorique passée dans les débats sur le chiffrement de l'UE, car il se concentrait sur le côté client, ou le côté fournisseur de technologie, et la détection du CSAM. Toutefois, le projet n'offrait pas de solution proposée - au lieu de cela, il mettait l'accent sur une option "la moins mauvaise", ce qui pouvait être une tactique persuasive, bien que quelque peu manipulatrice (Koomen, 2021).

Pour ce faire, la Commission européenne a lancé la Dérogation intérimaire pour la détection et la suppression du contenu de CSAM, qui comprend une disposition exigeant que les plateformes en ligne détectent et signalent les CSAM à l'aide d'outils automatisés (EPRS, 2021). Plus tard dans l'année, la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen a publié un rapport critiquant la disposition relative à la détection et au signalement des contenus de type CSAM, déclarant qu'elle n'était "pas proportionnée" et "présentait des risques pour les droits fondamentaux, y compris le droit à la vie privée" (EPRS, 2021). Le Parlement européen a adopté sa position sur la proposition, approuvant la disposition relative à la détection et au signalement des CSAM mais ajoutant plusieurs garanties, notamment l'exigence que tout outil automatisé utilisé pour la détection fasse l'objet d'une surveillance humaine[11] . Fin 2021, le Conseil de l'Union européenne a

[11] Service de recherche du Parlement européen, 2021 : "L'évaluation conclut que, bien que l'UE ait la compétence d'adopter le règlement proposé conformément à l'article 5 du traité sur l'Union européenne, l'impact de ces pratiques sur les droits de l'homme et les droits fondamentaux n'a pas été pris en compte de manière adéquate. Le règlement devrait fournir une base juridique claire pour ces pratiques, ainsi que des voies de recours efficaces pour les utilisateurs. Certaines technologies couvertes par la proposition de règlement ont un impact disproportionné et nécessitent donc des garanties supplémentaires qui ne sont pas disponibles dans la proposition sous sa forme actuelle.

arrêté sa propre position sur la proposition : il soutient la disposition relative à la détection et au signalement des CSAM, mais ajoute également des garanties, notamment l'exigence d'audits indépendants des outils automatisés utilisés pour la détection (avis conjoint EDPB-EDPS 4/2022). Ensuite, le Parlement, le Conseil de l'UE et la Commission ont entamé des négociations en trilogue sur la proposition - les négociations sont en cours au moment de la rédaction de ce document et un accord final n'a pas encore été trouvé.

4. Cette proposition est-elle la bonne méthode pour s'attaquer au problème du chiffrement ?

Nombreux sont ceux qui considèrent la proposition de règlement de l'UE visant à prévenir et à combattre les abus sexuels commis sur des enfants et les pratiques de manipulation psychologique comme une étape nécessaire dans la lutte contre la cybercriminalité, tandis que d'autres se demandent si la législation proposée est l'approche la plus efficace et la plus appropriée pour cibler ces contenus sensibles. Ce qui est le plus préoccupant, en particulier, c'est le mépris que la proposition semble avoir pour la sécurité du cryptage, qui est au cœur du débat entre vie privée et sécurité.

4.1 Critiques législatives

Avec la proposition de règlement visant à "prévenir et combattre les abus sexuels concernant les enfants", le Parlement européen et le Conseil ont entrepris d'harmoniser et de mettre en œuvre de nouvelles obligations pour les fournisseurs de services en ligne afin qu'ils analysent de manière sélective les messages privés des utilisateurs pour y déceler des comportements d'abus sexuels concernant les enfants et de manipulation psychologique. Selon la proposition, tout fournisseur de services de communication en ligne sélectionné, s'il reçoit un "ordre de détection" de l'UE, serait tenu d'analyser les messages de ses utilisateurs au moyen de technologies approuvées par l'UE. La proposition n'appelle pas à la fin des services cryptés en tant que tels, mais elle exige des entreprises qu'elles installent tout logiciel que l'UE juge nécessaire pour détecter le CSAM, ce qui rendrait l'E2EE - tel qu'il est conçu aujourd'hui - effectivement impossible. Selon l'art. 10, section 2, les fournisseurs sont obligés de : (a) "d'installer et d'exploiter des technologies permettant de détecter la diffusion de

matériel pédopornographique connu ou nouveau ou la sollicitation d'enfants", (b) de s'assurer que ces technologies sont "efficaces pour détecter la diffusion de matériel pédopornographique connu ou nouveau ou la sollicitation d'enfants [et] qu'elles ne permettent pas d'extraire d'autres informations de la communication concernée", (c) et qu'elles sont "les moins intrusives en termes d'impact sur les droits des utilisateurs à la vie privée et familiale, y compris la confidentialité des communications, et à la protection des données à caractère personnel".

En tant que telle, la proposition exige une technologie suffisamment étroite pour ne pas extraire d'autres informations de la communication concernée, tout en précisant que la technologie doit être capable de détecter les CSAM connus et nouveaux. Il s'agit en soi d'une contradiction puisque la proposition ne précise ni ne divulgue aucune information sur les technologies à mettre en œuvre, mais se contente d'énoncer des paramètres très vagues, laissant la place et la possibilité d'une surveillance plus généralisée. Le projet qui a fait l'objet d'une fuite présentait quant à lui un menu complet d'options sur la manière de maintenir le cryptage tout en garantissant la détection des CSAM. Malheureusement, le projet, bien qu'il soit technologiquement plus solide et plus sophistiqué, n'apporte pas de solution significative au difficile équilibre entre le cryptage et la détection du contenu. La proposition prévoit de détecter les CSAM *nouveaux* et *inconnus*, ce qui ouvre la porte à d'autres critiques, car les fournisseurs de services devraient analyser et détecter toutes les conversations afin de trouver de nouveaux cas de CSAM et, ce faisant, ils iraient à l'encontre de la proposition elle-même, qui appelle à une technologie "ciblée et spécifique". Par conséquent, la proposition ne fournit pas d'informations claires sur les technologies spécifiques à utiliser ni sur le processus permettant de s'assurer que les technologies sont efficaces tout en étant le moins intrusives possible.

En outre, la disposition (26) de la proposition met en évidence le sentiment général qu'il incombe à l'entreprise de trouver des moyens efficaces de préserver la vie privée et la protection tout en se conformant au principe de divulgation complète et de coopération aux fins de la détection du CSAM - en substance, cela revient à lui ordonner de faire l'impossible. L'imprécision de la proposition laisse beaucoup de place à l'indulgence. Cela rejoint l'une des

principales préoccupations de l'Association européenne des droits numériques : accorder trop de pouvoir aux grandes entreprises technologiques et permettre aux sociétés privées d'être responsables des mécanismes de surveillance et de censure, qui devraient plutôt relever de la responsabilité des autorités publiques.

La proposition met l'accent sur l'aspect technologique de la détection de CSAM, mais ne s'attaque pas efficacement à la racine du problème : les causes de l'abus sexuel des enfants. Elle met l'accent sur la surveillance et la criminalisation des comportements en ligne plutôt que sur la prévention, l'éducation et la réhabilitation des victimes d'abus. Une fois de plus, il s'agit d'une preuve que les institutions manquent de compréhension technique et produisent par conséquent des propositions et des lois qui sont vagues et imprécises, et donc inapplicables.

4.2 Les critiques politiques

Il n'est pas certain que la proposition de l'UE visant à réglementer les abus sexuels sur les enfants (également connus sous le nom de "contrôle du chat") soit l'instrument politique le plus efficace pour prévenir les MSTC et protéger les enfants contre les préjudices sur l'internet. Bien que l'intention de la proposition soit admirable, les enfants, comme les adultes, comptent sur l'E2EE pour assurer leur sécurité et leur vie privée face aux menaces évoquées à la section 2.2, telles que l'utilisation abusive des données par le gouvernement ou le secteur privé et les limites à la liberté d'expression. En affaiblissant ou en supprimant le cryptage, la proposition mettrait en péril l'autonomie des individus quant à l'utilisation de leurs données et l'assurance que leurs messages cryptés restent protégés des pirates informatiques et du gouvernement (Voge, 2022). Sans oublier que la proposition est largement impopulaire parmi les citoyens de l'UE (YouGov, 2021).

Bien que la proposition initiale affirme que ses exigences sont compatibles avec l'E2EE, l'Internet Society a constaté que ces exigences nécessiteraient la suppression ou l'affaiblissement du cryptage car il n'existe pas de technologies existantes qui puissent se conformer à ses exigences de filtrage (Voge, 2022). Ceci étant dit, les décideurs politiques ont pointé du doigt : 1) les portes dérobées de chiffrement et 2) l'analyse côté client pour détecter

les CSAM sans supprimer l'E2EE. Les portes dérobées de chiffrement permettent aux forces de l'ordre d'accéder aux messages chiffrés par un canal délibérément conçu par les développeurs de la plateforme. En théorie, la solution permettrait aux forces de l'ordre d'accéder aux messages cryptés. En pratique, elle crée des vulnérabilités qui peuvent être exploitées par des pirates, des criminels et d'autres acteurs hostiles, ce qui met *tous les* utilisateurs d'internet en danger (Voge, 2022 & Radauskas, 2023). Avec les portes dérobées de chiffrement, les internautes doivent croire naïvement que les agences gouvernementales et les forces de l'ordre sont inviolables.

La deuxième solution, l'analyse côté client, rompt l'E2EE en analysant les messages et les appareils des utilisateurs avant qu'ils ne soient cryptés et envoyés (Voge, 2022). À l'instar des portes dérobées de chiffrement, l'analyse côté client crée une nouvelle vulnérabilité qui peut être exploitée par des acteurs hostiles et mettre en péril la sûreté et la sécurité des utilisateurs. En outre, il s'avère extrêmement difficile, voire technologiquement impossible, d'identifier les cas de CSAM avec un niveau de précision élevé en utilisant le balayage côté client. Dans une étude d'impact commandée par le Parlement européen et présentée à la commission des libertés civiles, de la justice et des affaires intérieures, les chercheurs ont constaté qu'il y aurait un taux élevé de faux positifs pour les images de CSAM parce que *tous les* messages seraient scannés (Tar, 2023). Des images inoffensives provenant d'échanges entre adultes seraient signalées et transmises aux forces de l'ordre, ce qui pourrait mettre les internautes mal à l'aise. Par conséquent, cette solution créerait un arriéré pour les forces de l'ordre et porterait atteinte à la vie privée des utilisateurs, au lieu de faire progresser l'identification des cas de TCAM. Malgré les affirmations de la proposition, l'analyse d'impact n'est pas convaincue que la qualité de la détection s'améliorerait rapidement de manière significative, étant donné les décennies de recherche et de développement qui ont déjà été consacrées à l'identification des cas de CSAM avec une plus grande précision (Tar, 2023).

Des pays de l'UE, tels que l'Autriche, des agences et des membres du Parlement européen ont affirmé qu'en affaiblissant le cryptage, la proposition saperait la confiance dans les services de messagerie qui sont essentiels à "la vie familiale, médicale et financière", ainsi qu'à la démocratie (Antrag auf Stellungahme, 2022). Dans un avis conjoint, le Contrôleur

européen de la protection des données (CEPD) et le Conseil européen de la protection des données (CEPD) ont indiqué que la proposition va au-delà de ce qui est nécessaire et proportionnel compte tenu du taux d'erreur élevé associé aux technologies (2022, p. 6). En fait, le chiffrement joue un rôle important dans "la vie privée et la confidentialité des communications, la liberté d'expression ainsi que l'innovation et la croissance de l'économie numérique", qui dépendent de la confiance dans la protection de la vie privée offerte par le chiffrement (2022, p. 6). Par conséquent, les deux organismes estiment que les politiques devraient identifier des moyens plus efficaces d'équilibrer le compromis entre la lutte contre les abus et la protection des modes de communication sécurisés.

L'UE exploite un sujet hautement émotionnel, la diffusion de CSAM, comme moyen d'attirer moins de critiques sur l'affaiblissement du cryptage, de la même manière qu'elle a utilisé le terrorisme comme excuse pour saper la sécurité numérique dans le passé. Cependant, les citoyens européens ne sont pas aussi facilement influençables. Selon un sondage YouGov de 2021, 72% des Européens sont opposés à "la fouille automatique de tous les courriers et messages électroniques personnels de chaque citoyen en cas de contenu présumé suspect dans le cadre de la recherche de pédopornographie" (YouGov, 2021). Au lieu de cela, l'UE peut continuer à donner la priorité à des instruments politiques plus ciblés pour protéger les enfants contre les MSTC, tels que la prévention des abus sexuels à la source (plutôt qu'après la diffusion), l'amélioration de l'éducation, la fourniture de thérapies et de soutien, et la réduction des arriérés pour les forces de l'ordre dans le cadre de la "Stratégie 2020 de l'UE pour une lutte plus efficace contre les abus sexuels envers les enfants" (Negreiro, 2022, pg. 2). Ce faisant, il est possible que des instruments politiques ciblant la racine des préjudices subis par les enfants puissent empêcher la poursuite de la diffusion de la pédopornographie sans sacrifier la vie privée et la sécurité de tous les utilisateurs de l'internet.

4.3 Quelle est la suite des événements ?

Le paysage réglementaire de l'UE en matière de chiffrement se compose d'une combinaison d'outils législatifs et réglementaires, notamment des lois et règlements, des

directives et de la jurisprudence. Les tribunaux de l'UE, y compris la Cour de justice de l'Union européenne, ont également rendu des décisions sur des questions liées au chiffrement. Par exemple, dans un arrêt de 2020, la Cour de justice de l'Union européenne a estimé que les États membres de l'UE ne pouvaient pas exiger des fournisseurs de services de communications électroniques qu'ils mettent en œuvre une conservation générale et indiscriminée des données relatives au trafic et à la localisation, car cela serait incompatible avec le droit de l'UE et le droit à la vie privée.

Une autre réglementation importante qui aura un impact sur la réglementation du cryptage est l'adoption finale du règlement sur la vie privée et les communications électroniques (ePR), qui est actuellement en cours d'élaboration par l'UE et qui devrait remplacer l'actuelle directive sur la vie privée et les communications électroniques. L'ePR fournira des règles spécifiques pour la protection des données personnelles dans les communications électroniques et abordera également les spécificités de l'utilisation du cryptage. Les autres réglementations et lignes directrices qui traitent de l'utilisation du chiffrement dans l'UE sont le GDPR, la directive NIS 1 & 2 et les normes de l'Institut européen des normes de télécommunications (ETSI). Les normes de l'ETSI fournissent des lignes directrices, des spécifications techniques et des meilleures pratiques pour l'utilisation et la mise en œuvre du chiffrement dans divers domaines, tels que les télécommunications, les signatures électroniques et l'identification électronique. Les normes de l'ETSI sont peut-être l'outil réglementaire le plus spécifique en matière de chiffrement dont dispose l'UE, à l'exception du prochain règlement européen sur la protection des données (ePR).

Il est en effet difficile de réglementer le cryptage lorsque les parties concernées viennent d'horizons juridiques et culturels très différents et possèdent des niveaux de compréhension technique différents. Dans un sens, le chiffrement reflète un débat plus large, celui de la place de la technologie dans les normes de sécurité et d'éthique et de ce qui constitue une violation des droits fondamentaux dans un monde de plus en plus numérisé. Dans l'UE, ce manque d'unanimité a peut-être été renforcé par le fait que les considérations sur le chiffrement ont commencé assez tard et que les discussions qui les entourent ont été

déclenchées par des questions sociales politiquement chargées, plutôt que par la réglementation technologique elle-même.

Pour faciliter les discussions urgentes, les organisations européennes et internationales de la société civile et les acteurs de l'industrie se sont regroupés autour des thèmes du chiffrement et du CSAM, l'Association européenne des droits numériques soulignant cinq problèmes liés aux droits fondamentaux : (1) manque de clarté quant aux services couverts et à la base juridique des pratiques actuelles ; (2) absence d'évaluation d'impact et de consultations publiques essentielles ; (3) risque de normalisation des mesures exceptionnelles ; (4) renforcement du pouvoir des grandes entreprises technologiques, mettant les entreprises privées en charge des mécanismes de surveillance et de censure qui, en raison de leur impact sur les droits fondamentaux, devraient relever de la responsabilité des autorités publiques ; et (5) attaque potentielle contre le chiffrement (EDRi, 2022). Ces catégories générales seront des outils importants pour orienter les discussions et les efforts de réglementation à venir. Alors que les régulateurs du monde entier font pression pour des solutions technologiques au chiffrement, ce débat et les négociations à long terme mettent en évidence la complexité et les intérêts conflictuels en jeu et soulignent que le cœur du débat est en fait la fondamentalité débattue du chiffrement.

5. Devrait-il y avoir un droit fondamental au chiffrement dans l'UE ?

5.1 Qu'est-ce qu'un droit fondamental ?

Le concept de droits de l'homme fondamentaux a été établi pour la première fois dans la Déclaration universelle des droits de l'homme (DUDH), proclamée lors de l'Assemblée générale des États-Unis le 10 décembre 1948, afin d'énoncer pour la première fois des droits s'appliquant indistinctement à tous les peuples et à toutes les nations. La DUDH constitue donc une étape importante dans la protection des droits de l'homme, car elle définit certains droits comme étant "fondamentaux", ce qui implique qu'ils s'appliquent indistinctement à tous, qu'ils devraient être appliqués universellement et qu'ils devraient être hautement protégés contre toute violation. En fait, ces droits sont dits inaliénables, ce qui signifie qu'ils

ne peuvent être enfreints ou supprimés par aucune entité. La DUDH a ouvert la voie à des traités juridiquement contraignants tels que le Pacte international relatif aux droits civils et politiques (PIDCP) et le Pacte international relatif aux droits économiques, sociaux et culturels (PIDESC). (Nations unies, Déclaration universelle des droits de l'homme).

5.1.1 Droits fondamentaux des pays membres de l'ONU en matière de cryptage

La DUDH n'est pas un traité et n'est donc pas juridiquement contraignante, bien que certains affirment qu'elle est devenue contraignante en tant que droit international coutumier en raison de son invocation fréquente (Commission australienne des droits de l'homme). Les droits énumérés dans la DUDH, qui sont les plus pertinents pour le sujet du cryptage, sont les suivants : (a) le droit à ce qu'il **n'y ait pas d'immixtion arbitraire dans leur** vie **privée, leur** vie quotidienne, leur domicile ou leur correspondance et (b) le **droit à la protection de la loi contre de telles immixtions** ou de **telles** atteintes (article 12 de la DUDH) ; (c) le **droit à la liberté d'opinion et d'expression**, y compris le droit de **ne pas être inquiété pour ses opinions** et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées (article 19 de la DUDH) ; (d) le **droit de prendre part librement à la vie culturelle de la communauté** (article 27 de la DUDH).

5.1.2 Les droits fondamentaux liés au cryptage dans l'Union européenne

Dans l'Union européenne, les droits fondamentaux sont inscrits dans trois documents : (1) la Convention européenne des droits de l'homme (1950), (2) les Libertés fondamentales de l'Union européenne (1986) et (3) la Charte des droits fondamentaux de l'Union européenne (2000). La Charte des droits fondamentaux établit notamment tous les droits personnels, politiques et économiques des citoyens de l'UE. Bien que les tribunaux nationaux doivent appliquer les lois de l'Union européenne, lorsque la violation d'un droit fondamental est signalée, il appartient aux tribunaux nationaux de trancher la question, car la Charte sert de complément aux systèmes juridiques nationaux (Parlement européen). Les droits consacrés par la Charte qui sont les plus pertinents pour le cryptage sont le droit au **respect de la vie privée et familiale** (Art. 7) ; la **protection des données personnelles** (Art. 8) **;** la

liberté d'expression et d'information (Art. 11) ; la **liberté de réunion et d'association** (Art. 12) ; la **non-discrimination** (Art. 21) **; et** la **protection des consommateurs (**Art. 38).

5.2 L'évolution des droits fondamentaux dans une UE numérisée

L'émergence des technologies numériques a conduit à la redéfinition de certains droits fondamentaux et à l'établissement de nouveaux droits. Tout d'abord, avec l'intensification de la collecte et de l'utilisation des données, en particulier des données personnelles, des préoccupations sont apparues quant au droit des individus à la protection de leurs données et au caractère fondamental et inaliénable de celles-ci. Le **droit à la protection des données à caractère personnel** est considéré comme découlant logiquement du droit fondamental au respect de la vie privée (Conseil d'État français, 2016). En effet, l'article 8, paragraphe 1, de l'UE et l'article 16, paragraphe 1, du TFUE stipulent que toute personne a droit à la protection de ses données à caractère personnel. Le GDPR découle de cette idée de la protection des données personnelles en tant que droit fondamental et s'attaque à certains des nouveaux problèmes de vie privée et de données engendrés par les nouvelles technologies pour lesquelles aucun droit n'a encore été défini. Un exemple est le "droit à l'oubli" ou "droit à l'effacement" de l'article 17, qui permet à une personne de demander aux organisations d'effacer ses données à caractère personnel lorsqu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été obtenues (Department of Justice Office of Privacy and Civil Liberties, 2022).

Deuxièmement, l'article 7 de la Charte de l'UE sur la vie privée a été modifié afin de mieux protéger les communications privées. L' article 7 stipule désormais que "*toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses* ***communications***" (Journal officiel de l'UE C 303/17 - 14.12.2007). Le terme "*correspondance*" a été remplacé par "*communications*" pour tenir compte des progrès technologiques, ce qui indique le rôle et l'importance de la technologie dans les communications privées en ligne. Bien que l'article 7 ne soit pas un droit absolu, la confidentialité des communications reste un élément important des droits fondamentaux dans l'UE et il ne doit pas être porté atteinte à "l'essence du droit".

Un autre exemple de l'impact de la numérisation sur les droits individuels est l'**appel à la reconnaissance d'un droit fondamental à l'accès à l'internet**. En effet, une grande partie de la population a accès à l'internet dans les pays développés, mais certains groupes ont encore du mal à accéder à l'internet, par exemple en raison du coût de l'internet plus rapide (Custers, 2022) ou du manque d'infrastructures. Garantir le droit à l'accès à l'internet signifie garantir à tous la possibilité de s'informer et de s'exprimer en ligne. Bien que l'UE ne reconnaisse pas l'accès à l'internet comme un droit, il est de plus en plus reconnu au niveau national sur la base du fait qu'il découle du droit à la liberté d'expression (Conseil d'État français, 2016). La France a fait de l'accès à l'internet un droit de l'homme, le Conseil constitutionnel ayant jugé que la liberté d'expression garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen " implique la liberté d'accéder à ces services " (arrêt n° 2009-580 DC du 10 juin 2009, §12). De même, l'accès à l'internet à haut débit avec des connexions d'au moins 1 Mbit/s pour tous les citoyens est un droit constitutionnel en Finlande depuis 2010. En Grèce et en Espagne, le droit à l'accès à l'internet est également reconnu dans une certaine mesure (Custers, 2022). Plus généralement, en 2016, l'ONU a suggéré la reconnaissance d'un droit fondamental à l'accès à l'internet afin de protéger contre la censure gouvernementale et la perturbation délibérée de l'accès à l'internet par les gouvernements (Custers, 2022).

Dans l'ensemble, l'ère numérique a soulevé diverses questions concernant la définition des droits fondamentaux, leur application et la nécessité de nouveaux droits fondamentaux. Par exemple, les correspondances privées sont de plus en plus partagées sur le même support que la presse et les entreprises, et les États s'interrogent sur leur droit à censurer la parole et cherchent à identifier de nouveaux moyens de lutter contre les contenus illégaux en ligne. Comme les textes constitutionnels ne manquent jamais de le reconnaître, les droits fondamentaux peuvent être limités dans une mesure raisonnable. La question est donc de savoir ce qu'est un motif raisonnable pour limiter ces droits.

Lorsque l'on évalue les droits susmentionnés à la lumière de la proposition de CSAM, il apparaît que la proposition porte effectivement atteinte au droit fondamental des individus à la protection des données, aux communications privées (EDPB-EDPS, 2022) et pourrait

menacer leur droit à l'accès à l'internet en tentant d'affaiblir ou d'éliminer le cryptage des plateformes de messagerie en ligne. En plus d'enfreindre le droit à la protection des données, la proposition du CSAM serait probablement en contradiction avec les précédents établis par *Schrems* et *Digital Rights Ireland et Seitlinger et autres*, où la Cour a statué qu'accorder aux forces de l'ordre ou au gouvernement l'accès aux communications électroniques serait contraire à l'article 7, le droit au respect de la vie privée et familiale. Bien que l'article 7 ne mentionne pas explicitement le cryptage, l'analyse de la jurisprudence suggère que la protection des communications confidentielles, y compris le cryptage, devrait être protégée par la Charte des droits fondamentaux de l'UE.

5.3 Mais qu'est-ce qui rendrait fondamental le droit au chiffrement ?

Les droits reconnus dans la DUDH sont universellement reconnus comme des droits fondamentaux, mais ceux-ci peuvent varier d'une région ou d'une nation à l'autre, car les nations ont des références, des valeurs et des systèmes différents pour établir les droits fondamentaux. En effet, ces droits peuvent être énoncés dans une constitution nationale, un pacte international ou identifiés par le biais d'une procédure légale régulière[12] dans des pays comme les États-Unis.

En fait, les États-Unis offrent une conception intéressante de la fondamentalité. La plupart des droits fondamentaux, y compris le droit à la liberté d'expression (premier amendement), le droit de se réunir pacifiquement (premier amendement) et le droit de ne pas être soumis à des perquisitions et saisies déraisonnables (quatrième amendement), sont inscrits dans la déclaration des droits de la Constitution. Aux États-Unis, les droits fondamentaux (par opposition aux droits de l'homme) découlent d'une série de tests juridiques spécifiques[13] destinés, entre autres, à déterminer le fondement historique, la protection historique des "droits fondamentaux" potentiels et la profondeur de

[12] L'application régulière de la loi est un principe constitutionnel américain qui permet aux tribunaux d'établir et de protéger certains droits fondamentaux, même s'ils ne sont pas énumérés dans la Constitution.
[13] Cela s'explique par le fait que les droits fondamentaux sont hautement protégés aux États-Unis. Toute loi restreignant ces droits fait l'objet d'une évaluation minutieuse dans le cadre de la procédure d'examen minutieux (c'est-à-dire que la loi est supposée être invalide à moins qu'un argument puisse démontrer que la loi est vitale pour atteindre un "intérêt étatique impérieux" et qu'elle est étroitement adaptée à ce résultat).

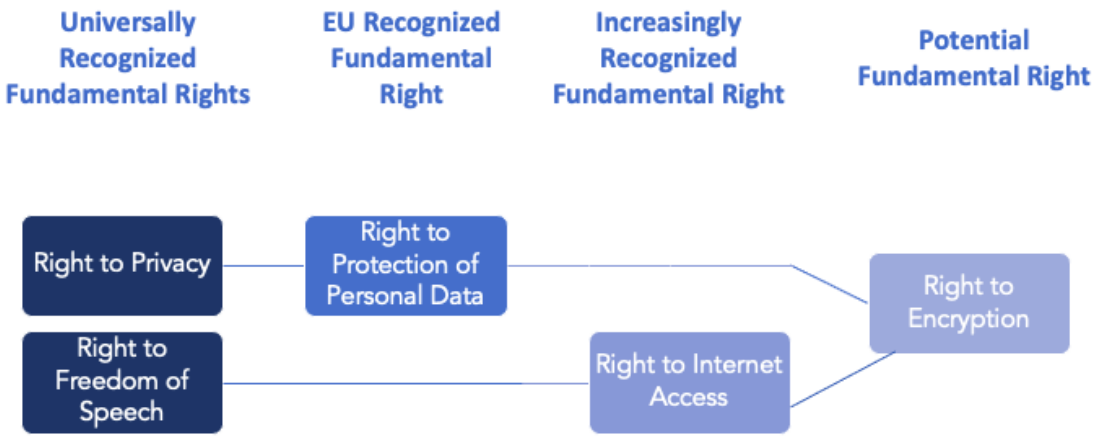
l'enracinement d'un droit dans les traditions et les consciences américaines. C'est ainsi que le droit à la vie privée - qui ne figure pas dans la Déclaration des droits - a été étendu en tant que droit fondamental par la Cour suprême, à la suite de l'affaire *Union Pacific R. Co. v. Botsford* en 1891. À la suite d'une jurisprudence ultérieure, ce droit à la vie privée en est venu à inclure notamment (a) le droit de **ne pas voir ses affaires personnelles divulguées** ou rendues publiques ; le droit d'être laissé en paix ; (b) **le droit contre l'intrusion indue du gouvernement** dans les questions et décisions personnelles fondamentales.

Dans le cadre de cette note d'information consacrée à un cas européen, nous nous appuierons sur une définition plus large, moins centrée sur la culture et l'histoire, de la notion de "fondamentalité". Dans son article de 1987 intitulé "*What Makes a Right Fundamental", le* professeur de sciences politiques Daniel N. Hoffman affirme essentiellement que l'argument requis pour soutenir qu'un droit est fondamental est que n'importe quelle personne pourrait le trouver fondamental à un moment donné. Plus précisément, Hoffman affirme que ce qui rend un droit fondamental dépend de la pondération des trois questions suivantes : (1) "Le droit est-il spécifiquement identifié comme fondamental par un texte ou une autorité de référence, ou est-il logiquement impliqué par un droit ainsi reconnu ?" (Hoffman, 1987, p. 527) ; (2) "Le droit est-il empiriquement nécessaire à la réalisation d'un droit fondamental reconnu ?" (Hoffman, 1987, p. 527) ; (3) "La possession du droit fait-elle partie de ce que signifie être une personne, de sorte qu'aucune personne attachée à la dignité humaine ne pourrait raisonnablement préférer vivre dans une société dans laquelle le droit ne serait pas reconnu ?" (Hoffman, 1987, p. 527). Qu'est-ce que cela signifie pour le cryptage ? Nous examinerons chaque question afin de conclure si oui ou non le chiffrement pourrait être reconnu comme un droit fondamental.

Tout d'abord, nous devons déterminer si le droit au chiffrement est spécifiquement identifié comme fondamental par un "texte ou une autorité de référence, ou logiquement impliqué par un droit ainsi reconnu". Bien que le droit au chiffrement lui-même ne soit pas identifié dans un texte fondamental et qu'aucune "autorité de contrôle" ne semble reconnaître le droit au chiffrement en tant que tel, le HCR, par exemple, souligne l'importance de protéger la confidentialité des communications dans le monde numérique pour défendre

le droit à la vie privée, la liberté d'association et la liberté d'expression en utilisant des mesures telles que le chiffrement et l'anonymat (Assemblée générale des Nations unies, Conseil des droits de l'homme, 2019). En effet, la liberté d'utiliser des technologies de chiffrement semble impliquée par le droit à la vie privée, à la liberté d'expression et le droit de participer librement à la vie culturelle de la communauté, respectivement Art.12, Art. 19 et l'article 27 de la DUDH appliqués au monde numérique (Kühnel et al., 2015). En outre, comme indiqué précédemment, le chiffrement est une technologie qui permet de protéger les conversations personnelles en ligne et permet aux individus de s'exprimer librement dans les communications en ligne sans crainte de persécution et/ou de restriction de leur accès aux plateformes numériques. Par conséquent, le chiffrement semble permettre le droit à la protection des données à caractère personnel (un droit fondamental) et le droit à l'accès à l'internet (un droit fondamental qui est de plus en plus reconnu parmi les membres de l'UE). On pourrait donc conclure que le droit au chiffrement est logiquement lié au droit à la liberté d'expression et à la vie privée et qu'il devrait être un droit fondamental.

Image 3 : Représentation du lien entre le droit au chiffrement et les droits fondamentalement reconnus, notamment le droit à la vie privée et le droit à la liberté d'expression.



La deuxième question de Hoffman est de savoir si le droit au cryptage est empiriquement nécessaire à la réalisation d'un droit fondamental reconnu - une question qui porte sur le lien intrinsèque entre le cryptage et les quatre droits susmentionnés.

Premièrement, l'article 12 de la DUDH stipule que les individus ont le droit de ne pas être dérangés dans leur correspondance. Appliqué aux communications électroniques, cela signifie que l'État ne doit pas intercepter et contrôler ce que vous envoyez ou recevez. Cela étant dit, dans le monde d'aujourd'hui, même dans les sociétés démocratiques, les entreprises et les États semblent mener des activités qui ne seraient pas autorisées dans le monde hors ligne. Par exemple, les États surveillent parfois les communications en ligne de leurs citoyens et les entreprises ont tendance à vendre des données. En effet, à bien des égards, les communications numériques sont beaucoup plus faciles à intercepter que les conversations hors ligne ou la correspondance écrite. Par exemple, les courriels passent souvent à travers les filtres anti-spam et il n'y a aucun moyen de savoir que leur confidentialité a été violée (Assemblée générale des Nations unies, Conseil des droits de l'homme, 2019).

En outre, si le droit à la protection des données personnelles et le droit à l'accès à l'internet sont considérés comme des droits fondamentaux, l'absence de chiffrement ou un chiffrement affaibli porte fortement atteinte à ces droits, tant pour les groupes vulnérables que pour l'ensemble de la population. En effet, alors que nous vivons dans des sociétés de plus en plus numérisées, le droit au chiffrement apparaît comme une protection importante des individus contre l'État. Dans sa résolution 42/15, le Conseil des droits de l'homme des Nations unies appelle les États à ne pas interférer avec l'utilisation des technologies de chiffrement et à élaborer des législations protégeant les communications numériques individuelles (Assemblée générale des Nations unies, Conseil des droits de l'homme, 2019). Au-delà des interdictions de chiffrement, même la mise en œuvre d'un accès dérobé au chiffrement à des fins légitimes a été critiquée par le rapporteur spécial des Nations unies sur la liberté d'expression en 2015 (Ferrari, 2022) et par Europol, qui affirme qu'elle menace la vie privée nécessaire à la protection du droit à la liberté d'expression. On peut donc conclure que la garantie du droit au chiffrement est une condition préalable à la garantie des quatre droits fondamentaux susmentionnés dans le monde numérique.

La dernière question de Hoffman est de savoir si la possession du droit au chiffrement est impliquée dans ce que signifie être une personne, de sorte qu'aucune personne ne pourrait raisonnablement préférer vivre dans une société dans laquelle ce droit ne serait pas

reconnu. Étant donné que le droit au chiffrement semble impliqué par quatre droits fondamentaux - deux universellement reconnus (droit à la vie privée et à la liberté d'expression), un droit fondamental reconnu par l'UE (droit à la protection des données) et un droit fondamental de plus en plus reconnu (droit à l'accès à l'internet) - et qu'il est nécessaire à leur réalisation, il faudrait un contre-argument vraiment solide pour empêcher l'émergence d'un droit au chiffrement. En effet, un individu n'envisagerait de vivre dans une société sans chiffrement que si le droit au chiffrement causait plus de tort que de bien.

Cependant, les groupes de défense et les institutions reconnaissent que l'utilisation du cryptage est nécessaire à la protection des droits de l'homme en ligne et hors ligne. Les conséquences d'un chiffrement affaibli peuvent menacer la dignité et la sécurité humaines en facilitant les activités criminelles et les violations des droits fondamentaux par l'État (accès aux informations et communications privées des personnes, exposition des sources des journalistes, soumission des défenseurs des droits de l'homme à l'action du gouvernement, etc.) Les groupes à risque, notamment les minorités sexuelles et de genre, sont particulièrement exposés aux violations de la vie privée. Ces violations de la vie privée en ligne peuvent se traduire par des abus et des violences hors ligne, mais aussi par l'impossibilité pour ces groupes d'obtenir des informations cruciales sur des sujets considérés comme tabous. Comme l'ont souligné le HCR en 2017 et le rapporteur spécial des Nations unies sur la liberté d'expression, la capacité de ces groupes à utiliser le cryptage et l'anonymat est essentielle à l'exercice de la liberté d'expression. (Ferrari, 2022) Par conséquent, la protection du chiffrement semble essentielle à la protection d'un large éventail de droits fondamentaux et, de manière générale, à une meilleure qualité de vie pour les individus (Ferrari, 2022). Il semble donc incohérent - si l'on a le choix - que l'on préfère vivre dans une société où le chiffrement est interdit - d'autant plus que le fait d'avoir le droit au chiffrement n'oblige pas l'individu à exercer ce droit en utilisant des technologies de chiffrement.

En définitive, sur la base des questions soulevées par Daniel Hoffman pour déterminer si un droit est fondamental, le droit au chiffrement devrait être reconnu comme un droit fondamental en raison du fait qu'il découle logiquement de la protection des autres droits fondamentaux et qu'il est nécessaire à leur réalisation. En définitive, nous estimons que, tous

facteurs confondus, une personne raisonnable ne préférerait pas vivre dans un monde dépourvu du droit au chiffrement.

6. Recommandations politiques

Après avoir établi que le chiffrement devrait effectivement être considéré comme un droit fondamental, la proposition de l'UE pour la détection des comportements de CSAM et de grooming devrait être reformulée, ou mieux, devrait présenter des solutions technologiques plus détaillées qui garantiraient l'intégrité du chiffrement.

6.1 Recommandations en matière de politique législative

L'UE doit adapter son approche de la réglementation afin de responsabiliser les grandes entreprises technologiques tout en protégeant les droits fondamentaux des citoyens. Comme nous l'avons vu précédemment, le chiffrement peut être considéré comme un droit fondamental selon les normes de l'UE, mais la Charte des droits fondamentaux de l'UE ou le cadre réglementaire actuel ne protège pas explicitement le droit au chiffrement, ce qui peut entraîner une ambiguïté juridique. L'UE peut envisager d'officialiser le chiffrement en tant que droit fondamental protégé par l'article 8 de la Charte. L'approche actuelle de la réglementation en matière de protection des données a été critiquée parce qu'elle utilise des politiques neutres sur le plan technologique qui peuvent être difficiles à mettre en œuvre. Par conséquent, pour renforcer le rôle du chiffrement dans la protection de la vie privée, les réglementations existantes en matière de protection des données, telles que la directive "vie privée et communications électroniques" et le règlement GDPR, peuvent être mises à jour pour spécifier clairement que le chiffrement est un moyen de se protéger contre le traitement illégal des données.

Si l'ambition de la Commission est de protéger les droits fondamentaux des enfants à la vie privée et à la sécurité contre les sévices sexuels à l'encontre des enfants, elle devrait se concentrer sur ses efforts actuels visant les causes profondes des sévices sexuels à l'encontre des enfants. Par exemple, la "Stratégie 2020 de l'UE pour une lutte plus efficace contre les

abus sexuels concernant les enfants" a défini plusieurs actions visant à améliorer le cadre juridique, la prévention et la réponse multipartite aux MCS (Negreiro, 2022, p. 2). Dans le cadre de cette stratégie, la Commission prévoit d'actualiser en 2023 la directive sur la maltraitance des enfants (2011/93/CE) afin de remédier aux faiblesses apparues lors de sa transposition en droit fédéral. Quant au Parlement, il s'est penché sur les activités préjudiciables dans l'environnement numérique dans sa résolution de 2021 sur la politique d'éducation numérique. La combinaison de ces instruments politiques pourrait avoir un impact plus mesurable sur la sécurité des enfants sur l'internet, par rapport aux risques associés à l'affaiblissement du cryptage.

6.2 Des recommandations techniques

Si la Commission souhaite aller de l'avant avec la proposition CSAM, elle peut envisager plusieurs propositions techniques visant à fournir certaines formes de détection de contenu dans l'E2EE tout en préservant le droit des utilisateurs au cryptage et à la vie privée.

Tout d'abord, nous recommandons d'accorder une attention particulière au **signalement** et à l'**intervention de l'utilisateur** par le biais de l'**affranchissement des messages**. Il s'agit d'un moyen pour les fournisseurs de services d'authentifier que l'expéditeur d'un contenu signalé est bien responsable de l'envoi du contenu perçu comme problématique. Cela se produit parce que la plateforme peut voir les identités de l'expéditeur et du destinataire et peut vérifier les rapports à l'aide de cryptogrammes spécialement construits qui prennent en charge l'affranchissement des messages (Tyagi et al., 2019, p. 3). Grâce à cette approche, il serait possible de signaler un contenu à la fois dans le cadre d'un chat individuel crypté et dans le cadre d'un chat de groupe (Kamara et. al, 2022, p.27). Toutefois, à l'heure actuelle, des recherches supplémentaires sont nécessaires pour déterminer les techniques les plus efficaces et les plus efficientes pour encourager les utilisateurs à signaler des contenus.

Deuxièmement, nous recommandons l'**analyse des métadonnées**, à savoir l'analyse des "données sur les données", qui, appliquée aux messages cryptés, pourrait fournir des informations précieuses sur la taille du fichier, l'expéditeur, le type de fichier et d'autres

informations similaires qui permettraient une analyse significative dans la détection du contenu. En particulier, en appliquant des techniques d'**apprentissage automatique** à l'analyse des métadonnées, il serait possible de disposer d'un outil capable d'identifier les contenus gênants en analysant la quantité ou les dimensions des messages, et si le volume ou les dimensions ne correspondent pas à la norme établie par les fournisseurs pour un comportement de messagerie typique, il serait alors possible d'intervenir et de vérifier la nature du contenu partagé (Kamara et. al, 2022, p.21). De même, des modèles ML pourraient être formés sur le comportement des utilisateurs interdits afin de pouvoir détecter les modèles de partage de contenus interdits. Toutefois, avant d'utiliser l'analyse des métadonnées et le ML, il convient de mener des études plus approfondies, car cette méthode est susceptible de présenter des risques d'atteinte à la vie privée[14] , mais il existe un consensus sur le fait que si l'analyse des métadonnées est limitée aux appareils des utilisateurs, leur vie privée est préservée et l'assurance de l'E2EE est maintenue (Kamara et. al., 2022, p.22).

Troisièmement, nous recommandons le **cryptage homomorphique**, car il est susceptible de concilier les préoccupations en matière de sécurité et de respect de la vie privée, puisqu'il permet d'effectuer des calculs sur des données cryptées sans les décrypter au préalable[15] (NSPCC, 2021, p. 18). Toutefois, cet outil prometteur a des coûts de calcul très élevés et nécessite des modifications et une formation spécifique pour chaque utilisation (Hamza et al., 2022, p. 532).

Ces propositions techniques s'opposent toutes à toute modification des schémas de chiffrement sous-jacents des fournisseurs de services ou à toute atteinte aux garanties de confidentialité et de sécurité de l'E2EE et soutiennent toutes le chiffrement en tant que droit fondamental.

[14] Il existe des preuves que l'analyse des métadonnées précédentes a été utilisée pour révéler des données sensibles telles que l'identité de l'expéditeur ou du destinataire de messages cryptés. Pour de plus amples informations sur le sujet, veuillez consulter le site suivant :
Greschbach, B., Kreitz, G. et Buchegger, S. (2012). The devil is in the metadata-New privacy challenges in Decentralised Online Social Networks. *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, 333-339. https://doi.org/10.1109/PerComW.2012.6197506

[15] En effet, il convertit les données en *texte chiffré* qui peut être analysé et travaillé comme s'il était toujours sous sa forme originale, le *texte en clair*.

Conclusion

La proposition de l'UE visant à prévenir et à lutter contre la maltraitance des enfants en filtrant les messages privés part d'une bonne intention. Toutefois, en l'état actuel de la technologie, il serait impossible d'appliquer le règlement sans compromettre ou éliminer l'E2EE sur les plateformes de messagerie en ligne. Les avantages collectifs du chiffrement sur la vie privée, la confiance et la démocratie peuvent l'emporter sur les risques liés à la création d'un bouclier pour les pédophiles, les terroristes ou d'autres criminels, qui trouveront d'autres moyens de commettre leurs méfaits. Par conséquent, le règlement ne s'attaquera guère aux causes profondes de la criminalité. Sur la base de l'analyse de la section 5, nous avons établi que le chiffrement devrait être considéré comme un droit fondamental dérivé du droit fondamental de l'UE à la vie privée (article 8), entre autres. En revanche, l'UE pourrait envisager des politiques axées sur la prévention ou le CSAM, ainsi que des propositions techniques visant à protéger l'intégrité du chiffrement sans créer de portes dérobées ou de vulnérabilités susceptibles d'être exploitées par des pirates informatiques.

Bibliographie

"Brève histoire des droits de l'homme". *Centre de ressources sur les droits de l'homme de l'Université du Minnesota*, http://hrlibrary.umn.edu/edumat/hreduseries/hereandnow/Part-1/short-history.htm. Acharya, B., Bankston, K., Schulman, R. et Wilson, A. (2017). Décryptage du débat européen sur le chiffrement : France. *Open Technology Institute.* https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf

Benner, T. et Hohmann, M. (2018, 28 janvier). *Comment l'Europe peut réussir le chiffrement*. POLITICO. Récupéré, à partir de https://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology/

Brush, K., Rosencrance, L. et Cobb, M. (2021, septembre). "Chiffrement asymétrique (cryptographie à clé publique)". *TechTarget.* https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography

Conrad, E., Misenar, S. et Feldman, J. (2012). Domaine 5 : Cryptographie. In E. Conrad, S. Misenar, & J. Feldman (Eds.), *CISSP Study Guide (Second Edition)* (pp. 213-255). https://doi.org/10.1016/B978-1-59749-961-3.00006-6.

Conseil D'Etat Français, 2016, *Les droits fondamentaux à l'ère du numérique*, https://www.conseil-etat.fr/Media/actualites/documents/reprise-_contenus/etudes-annuelles/fundamental-rights-in-the-digital-age.pdf .

Conseil de l'Europe, *Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telle qu'amendée par les Protocoles n° 11 et 14*, 4 novembre 1950, STE 5, disponible à l'adresse : https://www.refworld.org/docid/3ae6b3b04.html [consulté le 10 avril 2023]

Conseil de l'Union européenne, "Lettre franco-allemande concernant la coopération entre les services répressifs et les fournisseurs de services de communications électroniques", 7 novembre 2016, http://data.consilium.europa.eu/doc/document/ST-14001-2016-INIT/en/pdf.

"Résolution du Conseil sur le chiffrement - La sécurité par le chiffrement et la sécurité malgré le chiffrement, Conseil de l'Union européenne, 24 novembre 2020, https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf.

Custers, Bart. (2022). Nouveaux droits numériques : Imaginer des droits fondamentaux supplémentaires pour l'ère numérique. *Computer Law & Security Review, 44*, p. 105636, https://doi.org/10.1016/j.clsr.2021.105636.

DigitalEurope. (2020, 16 mars). Chiffrement : Trouver l'équilibre entre la vie privée, la sécurité et l'accès légal aux données. DigitalEurope. https://digital-europe-website-

v1.s3.fr-par.scw.cloud/uploads/2020/03/DIGITALEUROPE-Position-on-Encryption-Policy-.pdf

EDPB-EDPS. (2022). Avis conjoint 4/2022 sur la proposition de règlement du Parlement européen et du Conseil établissant des règles pour prévenir et combattre les abus sexuels concernant les enfants. *Conseil européen de la protection des données*. Extrait de https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf

EDRI20. (2022, 16 août). *La proposition de la Commission européenne sur le CSAM en ligne ne parvient pas à trouver les bonnes solutions pour lutter contre les abus sexuels sur les enfants*. Droits numériques européens (EDRi). Consulté sur le site https://edri.org/our-work/european-commissions-online-csam-proposal-fails-to-find-right-solutions-to-tackle-child-sexual-abuse/

ENISA. (2023, 13 mars). *Directive NIS*. ENISA. Consulté le 13 avril 2023, à l'adresse suivante : https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

EPRS. (2021). Proposition de la Commission relative à la dérogation temporaire à la directive "vie privée et communications électroniques" aux fins de la lutte contre les abus pédosexuels en ligne. *Parlement européen*. Consulté sur https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662598/EPRS_STU(2021)662598_EN.pdf

Commission européenne. (2020). Solutions techniques pour détecter les abus sexuels sur les enfants dans les communications cryptées de bout en bout. *Politico*. Extrait de https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf

Commission européenne, 2021, *Protéger les droits fondamentaux à l'ère numérique - Rapport annuel 2021 sur l'application de la Charte des droits fondamentaux de l'UE*, https://commission.europa.eu/system/files/2021-12/1_1_179442_ann_rep_en_0.pdf. Consulté le 19 avril 2023.

Commission européenne. (2022). *Union européenne de la sécurité*. Commission européenne. Consulté sur https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en#:~:text=The%20European%20Security%20Union%20saims,a%20whole%2Dof%2Dsociety%20approach

Ferrari, Veronica. "Qu'est-ce que le cryptage et pourquoi est-il essentiel pour les droits de l'homme ? *Association for Progressive Communications*, 23 septembre 2022, https://www.apc.org/en/news/what-encryption-and-why-it-key-human-rights.

Global Partners Digital. (2023). *Carte mondiale des lois et politiques en matière de cryptage*. Global Partners Digital. Extrait de https://www.gp-digital.org/world-map-of-encryption/

Grover, G., Rajwade, T. et Katira, D. (2021). Le ministère et la trace : subvertir le cryptage de bout en bout. *NUJS Law Review, 14*(2), 1-27.

Hamza, R. et al. (2022). Towards secure big data analysis via fully homomorphic encryption algorithms. *Entropy, 24*(4), 519-536. https://doi.org/10.3390/e24040519

Hoffman, Daniel N. "What Makes a Right Fundamental". *The Review of Politics*, vol. 49, no. 4, 1987, pp. 515-529, https://doi.org/10.1017/s0034670500035440. Consulté le 16 avril 2023.

"Droits de l'homme". *Nations unies*, Nations unies, https://www.un.org/en/global-issues/human-rights.

IOCTA. (2020). Évaluation de la menace que représente la criminalité organisée sur Internet. *Europol.* https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Kamara, S., Knodel, M., Llansó, E., Nojeim, G., Qin, L., Thakur, D., & Vogus, C. (2022). Outside looking in : Approaches to content moderation in end-to-end encrypted systems. *arXiv preprint arXiv:2202.04617*.

Knodel, M., Baker, F., Kolkman, O., Celi, S., & Grover, G. (2021). *Définition du chiffrement de bout en bout (IETF Active Internet-Draft)*. IETF. https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition/

Koomen, M. (n.d.). *Le débat sur le chiffrement dans l'Union européenne : mise à jour 2021*. Consulté le 13 avril 2023 sur le site https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217

Kühnel, M., Schweda, S., & Härting, S. (2015). OHCHR. Le *chiffrement du point de vue des droits de l'homme*, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/MarcoKuhnel.pdf. Consulté le 18 avril 2023.

NCMEC. (n.d). Qu'advient-il des informations contenues dans un CyberTip ? *National Center for Missing & Exploited Children.* https://www.missingkids.org/gethelpnow/cybertipline

Negreiro, M. (2022). Lutter contre les abus sexuels des enfants en ligne. *Parlement européen.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf

NSPCC. (2021). Cryptage de bout en bout : Understanding the impacts for child safety online. *Société nationale pour la prévention de la cruauté envers les enfants.* https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf

OCDE, Recommandation du Conseil concernant les lignes directrices pour la politique en matière de cryptographie, OECD/LEGAL/0289

"Document de synthèse : An Introduction to Encryption in Europe", Encryption Europe, janvier 2021, https://encryptioneurope.eu/positionpaper/.

Prima Santoso, P., Rilvani, E., Budi Trisnawan, A., Adiyarta, K. Napitupulu, D., Sutabri, T., & Rahim, R. (2018). Revue systématique de la littérature : Comparison study of symmetric key and asymmetric key algorithm (Étude comparative des algorithmes à clé symétrique et à clé asymétrique). *IOP Conference Series : Materials Science and Engineering, 420*, 012111. doi:10.1088/1757-899X/420/1/012111

"Loi sur la protection de la vie privée de 1974. *Department of Justice Office of Privacy and Civil Liberties*, 4 oct. 2022, https://www.justice.gov/opcl/privacy-act-1974.

"Protéger les droits fondamentaux au sein de l'Union". *Les droits fondamentaux dans l'UE*, https://www.europarl.europa.eu/about-parliament/en/democracy-and-human-rights/fundamental-rights-in-the-eu.

Radauskas, G. (2023, 31 janvier). *La proposition de l'UE visant à lutter contre la maltraitance des enfants en ligne ...* La proposition de l'UE pour lutter contre la maltraitance des enfants en ligne mettrait les enfants plus en danger, selon un expert. Consulté le 21 avril 2023 sur https://cybernews.com/editorial/eu-plans-combat-online-child-abuse-risk-to-encryption/

Reuters. (2016, 23 août). La *France et l'Allemagne font pression pour une loi européenne sur le cryptage après les attentats*. Reuters. Consulté le 13 avril 2023 sur https://www.reuters.com/article/europe-attacks-france-germany-idUSL8N1B41UM

Schlesinger, S. W. et Yanisky-Ravid, S. (2022). The right to data encryption. *San Diego Law Review, 59*, 569-598. https://digital.sandiego.edu/cgi/viewcontent.cgi?article=3444&context=sdlr

Song, S. (2020). Keeping Private Messages Private : End-to-End Encryption on Social Media. In *Boston College Intellectual Property and Technology Forum* (Vol. 2020, pp. 1-12).

Stupp, C. (2016, 30 mars). L'*agence de cybersécurité de l'UE s'oppose aux demandes de portes dérobées pour le cryptage*. www.euractiv.com. Consulté à l'adresse suivante : https://www.euractiv.com/section/digital/news/eu-cybersecurity-agency-slams-calls-for-encryption-backdoors/

Tar, J. (2023, 13 avril). *EU Parliament Study Slams Online Child Abuse Material Proposal*. www.euractiv.com. Consulté le 21 avril 2023 sur le site https://www.euractiv.com/section/law-enforcement/news/eu-parliament-study-slams-online-child-abuse-material-proposal/

"The Bill of Rights to the U.S. Constitution (La Déclaration des droits de la Constitution des États-Unis). *Union américaine pour les libertés civiles*, https://www.aclu.org/other/bill-rights-us-constitution.

Tyagi, N., Grubbs, P., Len, J., Miers, I. et Ristenpart, T. (2019). Asymmetric Message Franking (affranchissement asymétrique des messages) : Content Moderation for Metadata-Private End-to-End Encryption. In : Boldyreva, A., Micciancio, D. (eds) Advances in Cryptology - CRYPTO 2019. CRYPTO 2019. Lecture Notes in Computer Science(), vol 11694. Springer, Cham. https://doi.org/10.1007/978-3-030-26954-8_8

Assemblée générale des Nations unies Conseil des droits de l'homme, Le droit à la vie privée à l'ère numérique (27 septembre 2019) UN Doc A/HRC/RES/42/15

"Constitution des États-Unis, Déclaration des droits, Déclaration d'indépendance. *United for Human Rights*, https://www.humanrights.com/what-are-human-rights/brief-history/declaration-of-independence.html.

"Déclaration universelle des droits de l'homme. *Nations unies*, Nations unies, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Voge, Callum. "Proposition de la Commission européenne pour prévenir et combattre les abus sexuels sur les enfants. *Internet Society*, 19 août 2022, https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-eu-proposal-to-prevent-and-combat-child-sexual-abuse/.

Nous ne pouvons pas risquer que l'UE devienne un havre de paix pour les pédophiles et les prédateurs sexuels en ligne. Manifeste sur les droits de l'enfant. (2021, 22 janvier). Consulté sur le site https://www.childrightsmanifesto.eu/we-cannot-allow-the-eu-to-become-a-safe-haven-for-paedophiles-and-sexual-predators-online/

"Que signifie la liberté d'expression ? *Tribunaux des États-Unis*, https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does.

"Qu'est-ce que le cryptage ? | Types de cryptage". *CloudFlare.* https://www.cloudflare.com/en-gb/learning/ssl/what-is-encryption/

"Qu'est-ce que la Déclaration universelle des droits de l'homme ? *Commission australienne des droits de l'homme*, https://humanrights.gov.au/our-work/what-universal-declaration-human-rights.

YouGov. *Poll : 72% of Citizens Oppose EU Plans to Search All Private Messages for Allegedly Illegal Material and Report to Police*, 4 Nov. 2021, https://www.patrick-breyer.de/en/poll-72-of-citizens-oppose-eu-plans-to-search-all-private-messages-for-allegedly-illegal-material-and-report-to-the-police/.

A propos des autrices :

Stavroula (Stavrina) Chousou est en première année de master en politiques publiques, spécialisée dans les technologies numériques, les nouvelles technologies et les politiques publiques. Après avoir obtenu un diplôme de premier cycle en relations internationales et européennes à l'université du Pirée, elle a effectué un stage de recherche à l'Institut des affaires internationales d'Athènes. Elle s'est principalement concentrée sur l'utilisation et l'impact de la technologie dans la guerre ukrainienne en cours, ainsi que sur la concurrence croissante des États pour la suprématie technologique en matière d'IA et d'informatique quantique. À Sciences Po, Stavrina explore de nouvelles approches combinant des outils techniques et politiques afin d'équilibrer les préoccupations éthiques et sécuritaires dans les technologies émergentes.

Morgan Williams est en première année de Master en politiques publiques, spécialisée dans le numérique, les nouvelles technologies et les politiques publiques. Après avoir obtenu une licence en économie à l'Université du Maryland, Morgan a passé deux ans en tant que jeune associée de l'OCDE où elle a contribué à plusieurs volets du programme de recherche sur l'IA et le travail, l'innovation, la productivité et les compétences (AI-WIPS), ainsi qu'à des recherches sur l'économie de plateforme et l'externalisation domestique. À Sciences Po, Morgan s'intéresse principalement à l'intersection entre la technologie, le travail et les réglementations américaines et européennes.

Ludovica Pavoni est en première année de Master en politiques publiques, spécialisée dans le numérique, les nouvelles technologies et les politiques publiques. Tout en poursuivant ses études de premier cycle en affaires internationales à l'Université John Cabot, Ludovica a fait un stage dans une société de capital-risque spécialisée dans l'IA, la VT et l'AR. À partir de cette expérience, Ludovica a concentré ses intérêts et ses recherches sur la meilleure façon d'aborder les avancées technologiques et sur la meilleure façon d'aborder l'application du big data au secteur public.

Julia Magaud est en première année de Master en politiques publiques, spécialisée dans le numérique, les nouvelles technologies et les politiques publiques. Après avoir terminé sa licence en Humanités politiques à Sciences Po, Julia a travaillé sur un projet de recherche liant une entreprise d'IA aux conseils d'arrondissement de Londres afin d'améliorer la planification urbaine. Julia s'intéresse particulièrement aux villes intelligentes et à la numérisation du secteur public afin d'améliorer la prestation des services publics.

À propos de la chaire Digital, gouvernance et souveraineté :

La Chaire Digital, Gouvernance et Souveraineté de Sciences Po a pour mission de créer un forum unique réunissant des entreprises techniques, des universitaires, des décideurs politiques, des acteurs de la société civile, des incubateurs de politiques publiques ainsi que des experts de la régulation numérique. Hébergée par l'Ecole d'affaires publiques, la Chaire adopte une approche multidisciplinaire et holistique pour rechercher et analyser les

transformations économiques, juridiques, sociales et institutionnelles induites par l'innovation numérique. La Chaire Digital, Gouvernance et Souveraineté est dirigée par **Florence G'sell**, professeur de droit à l'Université de Lorraine, professeur à l'Ecole d'Affaires Publiques de Sciences Po et professeur invitée à Stanford en 2023.

Les activités de la chaire sont soutenues par :