Anonymat et chiffrement, composantes essentielles de la liberté de communication[*]

Félix Tréguer[**]

Janvier 2018

Table des matières

[*] Ne pas diffuser. Article à paraître dans : Q. Van Enis & C. De Terwangne (Eds.), *L'Europe des droits de l'homme à l'heure d'Internet*. Bruxelles: Bruylant.

[**] Chercheur post-doctorant au CERI-SciencesPo.

En décembre 2014, la police espagnole lance l'opération Pandora : 400 policiers investissent alors plus d'une douzaine de domiciles privés et de centres sociaux dans les grandes villes du pays. Ils saisissent des livres, des tracts, du matériel informatique. Sur les onze personnes finalement arrêtées, quatre seront immédiatement libérées et placées sous surveillance. Quant aux sept autres, elles restent en prison, accusées de terrorisme. Pour justifier ce maintien en détention, le juge madrilène invoque dans son ordonnance leurs lectures subversives et le fait « qu'ils utilisaient des e-mails avec mesures de sécurité extrêmes, telles que l'utilisation d'un serveur RISE UP »[1].

Fondée à Seattle en 1999, Riseup est en réalité une organisation non gouvernementale dont le but est fournir aux militants des droits de l'homme et des luttes environnementales des outils de communication respectant les meilleures pratiques en matière de confidentialité, notamment via des solutions techniques de chiffrement des communications. Dans un communiqué publié en réaction à cette affaire, l'ONG dénonce alors une décision de justice qu'elle assimile à une « criminalisation kafkaïenne des mouvements sociaux » reposant sur « l'idée grotesque et extrêmement préoccupante selon laquelle se soucier de sa vie privée est assimilable à du terrorisme »[2].

L'affaire soulève en effet d'importantes questions : protéger son anonymat et la confidentialité de ses communications peut-il constituer un facteur légitime de suspicion ? À l'inverse, faut-il y voir l'exercice d'un droit, directement indexé à la liberté d'expression et à la vie privé ? Depuis 2013, les débats autour de la surveillance d'Internet par les grandes agences occidentales de renseignement ont conduit à une nouvelle vague de controverses sur ces thématiques. D'un côté, des organisations de défense des libertés publiques, des responsables d'organisations internationales, ainsi que des experts en sécurité informatique font du droit à l'anonymat et à la confidentialité des communications une composante essentielle de la liberté d'expression et du droit à la vie privée. C'est notamment le cas de David Kaye, rapporteur spécial des Nations Unies pour la liberté d'expression, qui écrit dans un rapport publié en 2015 :

> « Le chiffrement et l'anonymat, qui sont aujourd'hui les principaux instruments de la sécurité en ligne, permettent à chacun de protéger son intimité et de naviguer sur Internet et d'y lire, élaborer et échanger des idées sans risque d'immixtion. Ils per-

[1] *Spain : Judge orders the detention of 7 of the 11 arrested in Operation Pandora.* Déc. 2014. Disponible à l'adresse : http://www.x-pressed.org/?xpd_article=spain-judge-orders-the-detention-of-7-of-the-11-arrested-in-operation-pandora.

[2] Riseup. *Security is not a crime.* Jan. 2015. Disponible à l'adresse : https://help.riseup.net/en/security-not-a-crime.

> mettent également aux journalistes, aux organisations de la société civile, aux membres de groupes ethniques ou religieux, aux personnes persécutées en raison de leur orientation sexuelle ou de leur identité de genre, aux militants, aux universitaires, aux artistes, entre autres, d'exercer leur droit à la liberté d'opinion et d'expression »[3].

Pourtant, certains juges et responsables des services de police et de renseignement, de même que certaines associations qui combattent les discours de haine, voient dans l'anonymat une stratégie de dissimulation qui facilite des comportements criminels et délictueux. Ils estiment en conséquence que ce dernier devrait être étroitement circonscrit.

Le débat n'a évidemment rien de nouveau. Dès 1997, un rapport des autorités de protection des données personnelles européennes posaient déjà le débat en des termes similaires[4]. Au-delà d'Internet et du numérique, ces controverses sont en fait consubstantielles de l'émergence du droit à la liberté d'expression et du droit à la vie privée, garantis par la Convention européenne des droits de l'Homme, et donc de la liberté de communication. Anonymat, confidentialité des communications et chiffrement mettent en jeu des questions fondamentales sur les rapports entre pouvoir et sujets, État et citoyens.

Mais de quoi s'agit-il au juste ? Pourquoi mêler ces différentes notions en tirant un trait d'union entre liberté d'expression et vie privée ? Classiquement, l'anonymat renvoie à la qualité de celui qui est « sans nom » – et donc par extension de celui qui communique sans révéler son identité officielle, son état civil. Il permet ainsi à des personnes pour qui l'expression, la protestation où la consultation d'une information seraient trop risquées – parce qu'ils s'exposeraient à des réprobations ou même à des sanctions de la part de leur famille, de leur milieu professionnel, de l'État – de le faire malgré tout. Le philosophe Geoffroy de Lagasnerie y voit ainsi la possibilité

[3] David Kaye. *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression sur le chiffrement et l'anonymat.* Rapp. tech. Genève : Conseil des droits de l'homme des Nations Unies, mai 2015. Disponible à l'adresse : https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/86/PDF/G1509586.pdf?OpenElement (visité le 19/10/2015).

[4] Voir le rapport du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel (groupe « Article 29 ») *L'anonymat sur Internet.* Rapp. tech. 3/97. Bruxelles : Commission européenne, 1997. Disponible à l'adresse : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_fr.pdf, p. 6 : « D'une part, la possibilité de rester anonyme est essentielle si l'on veut préserver les droits fondamentaux à la vie privée et à la liberté d'expression dans le cyberespace. D'autre part, la faculté de participer à des activités et de communiquer en ligne sans révéler son identité va à l'encontre d'initiatives lancées pour soutenir d'autres activités clés d'intérêt général tels que la lutte contre le contenu illégal et préjudiciable, la lutte contre les délits financiers ou les atteintes au droit d'auteur ».

« d'échapper à la façon dont le pouvoir nous lie à ce que nous faisons », une manière de « lever un tant soit peu, les mécanismes de l'assujettissement »[5]. La confidentialité des communications suppose quant à elle sinon l'anonymat, du moins l'assurance raisonnable que celles-ci ne seront pas soumises au regard de personnes non-autorisées. Elle inclut en particulier le respect du secret des correspondances privées. Quant au chiffrement, il désigne l'opération technique par laquelle, à travers une convention cryptographique, une écriture est encodée pour la rendre inintelligible aux personnes non-autorisées. Il renvoie donc à une méthode, à un dispositif technique, permettant d'assurer en pratique la confidentialité des communications et, dans certains cas, l'anonymat de celles-ci.

On le comprend, toutes ces notions sont étroitement liées en ce qu'elles ont trait aux usages stratégiques du secret par ceux qui communiquent. Dans ce chapitre, nous nous proposons donc de les aborder de front, au gré d'un parcours informé à la fois par l'histoire et le droit. Dans un premier temps, nous retraçons brièvement l'histoire des communications anonymes et confidentielles, du XVIIIè au XXè siècle. Nous revenons ensuite sur la construction d'un équilibre – précaire on le verra – entre un « droit à l'anonymat » sur Internet et d'autres droits et intérêts concurrents, notamment à travers les jurisprudences européennes. Dans la dernière partie, nous abordons les mutations récentes des systèmes de surveillance secrète pour souligner l'importance désormais cruciale du droit au chiffrement pour la liberté de communication.

1. Brève histoire de la communication anonyme et confidentielle

Commençons donc par quelques rappels historiques. En dépit de l'acuité des débats contemporains, l'anonymat et la confidentialité des communications sont en réalité des pratiques anciennes, directement influencées par l'évolution croisée du droit et des techniques de communication.

1.1. Une pratique ancienne, toujours menacée

Jusqu'au XVIII^{e} siècle en effet, l'anonymat est largement la norme. Ainsi, sur 396 ouvrages parus en 1696, 236 ne portent pas le nom de l'auteur[6][20]. À l'époque, en France, les autorités n'imposent pas son identifi-

[5] Geoffroy de Lagasnerie. *L'art de la révolte : Snowden, Assange, Manning.* Fayard, 2015, p. 191.

[6] «Anonymat et clandestinité aux XVIIe et XVIIIe siècles : actes de la journée de Créteil du 11 juin 1999». In : *La Lettre clandestine* 8 (1999). Sous la dir. de Geneviève

cation, l'ouvrage doit devant toutefois mentionner l'approbation du censeur et le privilège de copie accordé à l'imprimeur-libraire[7][55]. Mais tandis que s'organise le marché du livre, que les auteurs de la « République des Lettres » gagnent en notoriété et en audace, il est aussi de plus en plus l'objet d'usages stratégiques.

En effet, dans la période charnière où sont adoptées les grandes déclarations de droit des XVII^{e} et XVIII^{e} siècles – du *Bill of Rights* britannique (1689) à la Déclaration des droits de l'Homme et du Citoyen (1789) –, il s'enracine dans les pratiques de ceux qui s'expriment pour contester le pouvoir. Pour les grands philosophes des Lumières, de Descartes à d'Holbach en passant par Locke, Voltaire ou les contributeurs de *L'Encyclopédie*, l'anonymat permet aux auteurs de rogner un surcroît de liberté, de s'émanciper autant que faire se peut de la censure et de la surveillance des écrits.

Certes, il est une protection toute relative compte tenu du contrôle étroit des métiers de l'imprimerie par le pouvoir, et les précautions des auteurs ne suffisent pas toujours à les abriter de la répression. Il n'en demeure pas moins un outil indispensable au « combat philosophique », et notamment à la dénonciation de l'absolutisme. Ce sont en effet sous des noms d'emprunt que s'écrivent alors défenses les plus vigoureuses de la liberté d'expression, à l'image de celle portée par deux journalistes politiques anglais, Trenchard et Gordon, qui dans les années 1720 publient sous le pseudonyme de Caton des textes dans lesquels ils théorisent de façon visionnaire le rôle de « quatrième pouvoir » qui sera plus tard reconnu à la presse[8].

Enfin, outre ces élites subversives, le peuple lui-même entre en scène dans cette période charnière. À travers son étude de la répression policière de l'« opinion publique populaire » à Paris au milieu du XVIII^{e} siècle, l'historienne Arlette Farge a ainsi montré comment la satire et la moquerie avaient alors envahi l'espace urbain, notamment au travers des placards séditieux et anonymes[9].

Si l'anonymat est donc de mise dans les pratiques communicationnelles et simplement toléré en droit, la confidentialité des communications est quant à elle déjà protégée juridiquement. En France, dès 1742, une déclaration royale assimile le viol des correspondances au détournement des deniers publics et le réprime de la peine de mort. Puis, en 1775, un arrêt du Conseil du Roi vient rappeler que « tous les principes mettent la correspondance secrète des citoyens au rang des choses sacrées dont les tribunaux comme

---

Artigas-Menant et Antony McKenna.

[7] Artigas-Menant et McKenna, «Anonymat et clandestinité aux XVIIe et XVIIIe siècles».

[8] John Trenchard et Dr Thomas Gordon. *Cato's Letters*. Boston : Nabu Press, 2011.

[9] Arlette Farge. *Dire et mal dire. L'opinion publique au XVIIIè siècle*. Seuil, 1992, p. 99-100.

les particuliers doivent détourner les regards ». Cela n'empêche évidemment pas le « Cabinet noir » d'être officiellement chargé de cette fonction de surveillance des courriers.

À la veille de la Révolution, de nombreux cahiers de doléances dénonceront ces abus, associés à l'arbitraire féodal. Le secret des correspondances sera ainsi consacré avec la loi « concernant le secret & l'inviolabilité des Lettres » du 20 juillet 1791. L'exposé des motifs indique alors qu'il s'agit de mettre fins aux abus commis en différents lieux du territoire par des administrations locales faisant preuve d'un « zèle inconsidéré » en matière de surveillance postale. Le Code pénal de 1791, voté quelques semaines plus tard, criminalise même le viol du secret des correspondances et le condamne d'une peine de dégradation civique[10]. Rapidement, du fait des guerres révolutionnaires, le contrôle postal sera pourtant réactivé. Le 28 avril 1793, le Comité de Salut public adopte un arrêté qui rétablit la censure des correspondances. Face « aux ennemis de la République » qui « emploient dans cette guerre des moyens extraordinaires » et « trament au sein de la Patrie leurs complots », il est arrêté « que toute les lettres venant de l'étranger seront ouvertes »[11].

Pour s'en prémunir, il est toujours possible de recourir à l'art ancien de la cryptographie, la « science du secret ». Contrairement aux idées reçues, il semble que le chiffrement et autres codes secrets destinés à dissimuler le sens d'un message aient de tout temps fait l'objet d'usages triviaux et populaires. Certes, ces derniers demeuraient marginaux, puisque l'écriture fut pendant longtemps essentiellement réservée aux élites. Mais l'un des plus vieux documents connus adoptant un système de codage est une tablette en argile datant de l'Antiquité retrouvée en Irak, dans laquelle le potier avait dissimulé ses techniques de fabrication en jouant sur les consonnes.

À partir du XVI^{e} siècle, le développement concomitant de l'imprimerie et des postes aboutit à la prolifération de traités sur l'art du chiffrement, non seulement pour les empereurs, espions et diplomates, mais aussi pour les commerçants et hommes d'affaires, pour les savants ou même pour les correspondances intimes, avec la volonté d'échapper aux cabinets noirs, ou plus simplement aux regards indiscrets. Il est aussi, déjà, un outil prisé des dissidents politiques. On sait par exemple que les « pères fondateurs » des États-Unis comme Benjamin Franklin, James Madison ou Thomas Jefferson chiffraient leurs correspondances. C'est d'ailleurs dans un courrier partiellement codé que, le 27 mai 1789, Madison exposera à Jefferson son idée

[10] Sébastien Laurent. *Politiques de l'ombre : État, renseignement et surveillance en France*. Paris : Fayard, 2009, p. 26-27.

[11] Roger Lévy-Guenot. «Le Contrôle Postal en 1793 : une grève de censeurs». In : *Annales révolutionnaires* 10.3 (1918), p. 389–395.

d'ajouter un Bill of Rights à la constitution américaine[12].

Au XIX^{e} siècle, le paradigme libéral consacre les apparences d'une plus grande liberté dans l'usage des moyens d'expression et de communication, mais celle-ci va de paire avec une sophistication croissante des formes de censure et de surveillance. Les régimes juridiques du télégraphe et de la presse illustrent les termes du compromis acceptable entre liberté de communication et impératifs policiers.

Ainsi, la télégraphie – avec l'ouverture progressive de son utilisation aux particuliers dans la seconde moitié du XIX^{e} siècle – marque-t-elle l'avènement des télécommunications « grand public ». Que dit alors la loi ? En France, le télégraphe n'est autorisé que pour les messages à caractère privé, et l'anonymat est proscrit : l'expéditeur est ainsi tenu de fournir son nom et d'attester de son adresse, bref de son identité. Le chiffrement est toutefois autorisé, notamment pour permettre aux usagers de protéger leur intimité vis-à-vis des techniciens chargés de la transmission des messages. Ce qu'on appelle alors les « dépêches secrètes » (ou « inintelligibles ») doivent être rédigées en signes romains ou en chiffres arabes. Ces codes sont supposés être facilement déchiffrables. Surtout, les bureaux gardent trace de toute communication : qui communique avec qui, à quelle heure – ce qu'on appellerait aujourd'hui les « métadonnées ». Un directeur des transmissions télégraphiques à Versailles loue ainsi, dans un écrit de 1870, la contribution du télégraphe à l'ordre public : « la télégraphie réalise pour la sécurité publique l'idéal de M. Vidocq, de terrible mémoire »[13].

Quant à la liberté de la presse, consacrée en France dans la loi de 1881 elle reste conditionnée à une « déclaration préalable » adressée à l'administration, ce qui permet de recueillir l'identité des responsables du journal pour faire valoir leur responsabilité civile ou pénale. Comme au XVII^{e} siècle, l'anonymat n'est donc toléré que pour l'auteur, mais pas nécessairement pour ceux qui le publient[14].

Au XX^{e} siècle, le relâchement de la surveillance des postes en temps de paix et le développement progressif des cabines téléphoniques ménagent à leur tour des possibilités de communications anonymes. Mais il faut attendre les années 1960 pour que l'anonymat et la confidentialité des communications fassent l'objet d'une double consécration, à la fois juridique et technique.

[12] John A. Fraser. «The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution». In : *Virginia Journal of Law and Technology* 2.2 (1997).

[13] J-M Villefranche. *La Télégraphie française : étude historique*. Palmé, 1870, p. 251.

[14] L'article 25 de la Constitution belge, consacrant la liberté de la presse, permet de viser le intermédiaires de la presse à défaut d'auteur identifié et domicilié en Belgique. Voy. Quentin Van Enis. *La liberté de la presse à l'ère numérique*. LGDJ, 2015, p. 358.

1.2. Reconnaissance juridique de l'anonymat en démocratie

Au plan juridique, la période est ainsi marquée par les progrès concomitants du droit à la vie privée et de la liberté d'expression. Alors que gagne la peur de voir les nouvelles technologies mises au service des technocraties pour surveiller les populations, on assiste en effet à un mouvement en faveur de la protection de la vie privée[15]. C'est dans ce contexte historique que s'inscrit par exemple la CEDH lorsqu'elle rend son arrêt *Klass et autres c. Allemagne* de 1978. Selon la Cour, la législation autorisant la surveillance des communications « crée par sa simple existence, pour tous ceux auxquels on pourrait l'appliquer, une menace de surveillance entravant forcément la liberté de communication entre usagers des services des postes et télécommunications et constituant par là une "ingérence d'une autorité publique" dans l'exercice du droit des requérants au respect de leur vie privée et familiale ainsi que de leur correspondance »[16].

L'anonymat et la confidentialité des communications se voient également indirectement consacrés comme des outils indispensables au rôle de « chien de garde » dévolu à la presse à travers la protection des sources journalistiques. Axiome central de la déontologie des journalistes depuis le début du XX^{e} siècle – on parle alors plus généralement du « secret professionnel » associé à leur profession –, celle-ci réalise d'importants progrès à partir des années 1970. A la suite de la publication en 1971 des *Pentagon Papers* fuités par le lanceur d'alerte Daniel Ellsberg – qui jettent une lumière crue sur la guerre du Vietnam –, la Cour suprême des États-Unis rend l'année suivante l'arrêt *Branzburg v. Hayes*, qui en dépit de certains ambiguïtés reconnaît le droit d'un journaliste à protéger l'anonymat de ses sources [17].

En Europe, hormis quelques avancées encore plus précoces en Suède, il faut attendre 1994 pour que la conférence ministérielle du Conseil de l'Eu-

[15]Gloria González Fuster. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer Science & Business, 2014.

[16]CEDH, 6 septembre 1978, *Klass et autres c. Allemagne*, n° 5029/71, §41.

[17] En 1972, la Cour suprême est saisie d'une affaire dans laquelle Paul Branzburg, un reporter d'un journal local dans le Kentucky, est sommé par les autorités judiciaire de l'État de révéler l'identité de deux individus consommateurs de hashish qui l'ont aidé à rédiger un article sur le sujet. Ce dernier refuse, indiquant qu'il a promis à ces deux personnes le respect total de l'anonymat, et invoque la protection du Premier amendement. Dans une décision très serrée (5 contre 4), la Cour refusa de reconnaître un droit constitutionnel absolu à la protection des sources. Néanmoins, afin de contraindre un journaliste à révéler l'identité de ses sources, les juges posent des critères relativement exigeants : le gouvernement doit « démontrer de manière convaincante une relation substantielle entre l'information recherchée [l'identité des sources] et un sujet d'intérêt d'État impérieux et convaincant ». Cour suprême des États-Unis, 29 juin 1972, *Branzburg v. Hayes*, 408 U.S. 665 (1972). Quelques années plus tard, la Cour protégera également le secret des sources journalistiques dans le cadre des perquisitions et saisies (*Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).

rope, réunie à Prague, évoque la protection des sources journalistiques. Dans une résolution, le Conseil estime alors que « la protection de la confidentialité des sources d'information utilisées par les journalistes » constitue un prérequis pour que les médias puissent « contribuer au maintien et au développement d'une démocratie véritable »[18]. Puis, en 1996, la CEDH amorce un mouvement jurisprudentiel favorable à ce principe, en reconnaissant aux journalistes le droit de refuser de témoigner afin de protéger leurs sources. Dans la célèbre affaire *Goodwin c. Royaume-Uni*, elle fait ainsi de la protection de la confidentialité des communications entre les journalistes et leurs sources « l' une des pierres angulaires de la liberté de la presse » et de la capacité des médias à informer le public sur des questions d'intérêt général[19].

Quasiment au même moment, la Cour suprême des États-Unis va plus loin : alors qu'en Europe, la protection des sources journalistiques induit une reconnaissance de l'anonymat qui reste contrebalancée par la responsabilité du journaliste ou du journal, elle, consacre expressément l'anonymat des personnes qui s'exprimeraient sans le « filtre » journalistique, restant en cela fidèle à sa conception horizontale et radical-démocratique de l'espace public[20]. Ainsi, en 1995, dans une décision invalidant une loi de l'État de l'Ohio qui entendait proscrire les écrits politiques anonymes, la Cour estime que l'anonymat constitue « un bouclier contre la tyrannie de la majorité » en ce qu'il protège les individus hétérodoxes et leurs idées « des représailles » dont est capable une « société intolérante »[21]. Pour les juges, « les pamphlets anonymes ne constituent pas une pratique pernicieuse ou frauduleuse, mais une vénérable tradition de plaidoyer et de dissidence », laquelle est protégée par le Premier amendement.

[18]Comité des Ministres du Conseil de l'Europe. *Résolution n°2 sur « les libertés journalistiques et les droits de l'Homme »*. Rapp. tech. Prague : Conseil de l'Europe, 1994. Disponible à l'adresse : https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=411457&SecMode=1&DocId=517430&Usage=2.

[19]CEDH [GC], 27 mars 1996, *Goodwin contre Royaume-Uni*, n°17488/90. Dans cette affaire, un jeune journaliste britannique travaillant dans la presse économique avait reçu de la part d'une source confidentielle des informations sur la mauvaise santé financière de l'entreprise. Il contacte cette dernière, qui refuse de réagir officiellement, et lui indique que la publication de ces informations auraient de graves conséquences sur un plan de financement qu'elle s'apprête à lancer. Pour empêcher la publication de ces informations et connaître l'identité de la source, l'entreprise saisit la justice. Le juge britannique accepte. Il ordonne une mesure de censure et somme le journaliste de révéler l'identité de son informateur. À défaut, ils sera condamné à une amende de 5000 livres (plus de 3500€) pour outrage à la cour (« *contempt of court* »). En appel, la Chambre des Lords confirme cette condamnation. Le journaliste saisit donc la CEDH qui lui donnera raison.

[20]Marcela Iacub. *De la pornographie en Amérique : La liberté d'expression à l'âge de la démocratie délibérative*. Fayard, 2010.

[21]Cour suprême des États-Unis, 19 avril 1995, *McIntyre v. Ohio Elections Commission* , 514 U.S. 334.

1.3. La cryptographie, ou la revendication par la technique du droit au secret des communications

Outre cette consécration juridique, les innovations techniques intervenues entre les années 1970 et 1990 vont également permettre de dessiner un projet politique subversif fondé sur la cryptographie. Alors que cette dernière était devenue une science réservée au monde militaire, des mathématiciens et informaticiens vont tenter, à partir des années 1970, d'œuvrer à sa réappropriation politique. À l'époque, la *National Security Agency* (NSA) avait lancé un appel à projet pour le développement d'un standard en matière de chiffrement, qu'elle cherchera délibérément à affaiblir pour être en mesure de casser plus facilement les codes. Cet épisode suscite alors l'intérêt de chercheurs en mathématiques qui, au gré de leurs travaux, vont sortir la cryptographie moderne de son giron militaire, et poser les bases théoriques de sa démocratisation à l'ère numérique[22].

Le génie est sorti de sa bouteille. À la toute fin des années 1980, au sein de la mouvance des « cypherpunks », des militants passionnés d'informatique font de la cryptographie un art ouvertement contestataire. Elle est investie non seulement pour permettre protéger la confidentialité des communications, mais également comme un outil grâce auquel il devient possible de systématiser les fuites de documents classifiés, et donc d'opérer une remise en cause radicale des secrets d'État[23]. La mailing-list éponyme des cypherpunks sera d'ailleurs l'une des matrices intellectuelles du jeune Julian Assange, futur fondateur de WikiLeaks, au début des années 1990. Il y côtoie notamment Philip Zimmermann, inventeur du logiciel *Pretty Good Privacy* – qui permet d'authentifier les courriers électroniques et d'en chiffrer le contenu –, ainsi que les développeurs des premiers outils d'anonymisation sur Internet, tels que des *re-mailers*, ces serveurs-relais qui permettent de masquer l'émetteur d'un message. L'anonymat est déjà une valeur essentielle au sein de la mouvance hacker, et un moyen essentiel pour assurer au plan technique la confidentialité des correspondances numériques qui prévaut alors sur les réseaux postaux ou téléphoniques[24].

[22] Henry Corrigan-Gibbs. «Keeping Secrets». In : *Stanford Magazine* November/December (2014).

[23] Andy Greenberg. *This Machine Kills Secret : How Wikileakers, Hacktivists, and Cypherpunks are Freeing the World's Information*. Virgin Books, 2012.

[24] Comparant la communication privée sur Internet au moyens de communications traditionnels, le groupe de travail « Article 29 » de la Commission européenne souligne en 1997 : « L'existence d'une option d'anonymat dans le domaine du courrier électronique est capitale si l'on compare ce service à d'autres techniques traditionnelles de communication "un à un". Le service postal traditionnel est, en effet, nettement plus respectueux de la confidentialité, car l'envoi d'un courrier normal peut se faire dans l'anonymat le plus complet. Le fournisseur du service postal ne peut recueillir aucune donnée transactionnelle permettant d'identifier l'émetteur du message (...) ». *L'anonymat sur Internet*, p. 7.

Alors qu'Internet est en passe de se démocratiser, les agences de renseignement et de police vont toutefois tenter de préserver leur mainmise sur ces techniques, déclenchant un conflit politique et juridique resté dans les mémoires comme la première « *Crypto War* »[25]. En 1993, le *New York Times* révèle ainsi que la NSA souhaite s'octroyer la capacité de déchiffrer l'ensemble des données et communications informatiques, au travers d'une puce de chiffrement dotée d'une « porte dérobée ». Aux États-Unis tout comme en France où un régime d'autorisation préalable est nécessaire pour tout usage de la cryptographie, le droit est également mobilisé pour empêcher la diffusion sur les réseaux des logiciels de chiffrement, au travers du régime applicable à l'exportation des « biens à double usage » (c'est-à-dire aux applications à la fois civiles et militaires). C'est grâce à la mobilisation des premiers mouvements de défense des libertés publiques dans l'environnement numérique – mais aussi en raison de l'influence du secteur privé qui a besoin du chiffrement pour développer le commerce électronique – que ces projets seront tenus en échec. Le droit applicable sera d'ailleurs partiellement libéralisé dans la deuxième moitié des années 1990[26].

2. Les intermédiaires techniques d'Internet face à l'expression anonyme

Au-delà de l'enjeu du chiffrement, Internet apparaît rapidement comme le vecteur d'une démocratisation spectaculaire de l'expression publique anonyme. Pour les premières « communautés virtuelles » qui se constituent autour de Usenet et autres salons de discussion en ligne, la communication anonyme (ou pseudonyme) est l'occasion de nouer des relations sociales plus horizontales, d'endosser des identités fictives. Autant d'expériences émancipatrices décrites avec sarcasme dans le célèbre cartoon du *New Yorker* en 1993 : « *on the Internet, nobody knows you're a dog* ». Mais l'anonymat apparaît aussi comme un obstacle à la répression des abus de liberté d'expression. C'est autour de cette problématique fondatrice que s'édifie une partie des règles juridiques spécifiques à Internet, notamment s'agissant du rôle et de la responsabilité des « intermédiaires techniques » du réseau, et auxquelles se heurtent aujourd'hui encore juges et législateurs.

[25] Steven Levy. *Crypto : How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. 1st edition. London : Penguin Books, 2001.

[26] Bertrand Warusfel. «Dix ans de réglementation de la cryptologie en France : du contrôle étatique à la liberté concédée». In : *Annuaire français de relations internationales* 1 (2000), p. 657–661.

2.1. Autour de l'anonymat, des débats fondateurs du droit de l'Internet

Au milieu des années 1990, en France, le régime juridique alors applicable à la communication sur Internet est celui mis en place pour le Minitel dans les années 1980, et qui s'applique à tout ce qu'on appelle alors les « services télématiques », eux-mêmes subordonnés à la loi du 30 septembre 1986 sur l'audiovisuel. Aussi les sites Internet sont-ils soumis à l'article 43 de ce texte, qui prévoit une obligation de déclaration préalable auprès du procureur de la République et du Conseil supérieur de l'audiovisuel (CSA). Quant à l'article 37 de la loi, il impose de tenir à disposition du public sur le site Web l'identité de son responsable. Des obligations qui, en pratique, ne sont guère respectées, notamment par les nombreux sites amateurs[27].

Pour contourner l'obstacle de l'anonymat, les premières affaires judiciaires relatives à Internet visent donc les « intermédiaires techniques » que sont les fournisseurs d'accès à Internet (FAI) ou les hébergeurs, plutôt que les auteurs des propos litigieux. C'est d'ailleurs vrai aux États-Unis comme ailleurs en Europe. Ainsi, en Allemagne, l'ancien directeur de l'opérateur Compuserve comparaît en avril 1997 devant le tribunal de Munich pour avoir permis la diffusion de contenus à caractère pédopornographiques, zoophiles et violents. Il est condamné l'année suivante à deux ans de prison avec sursis et une importante amende[28]. L'affaire fait scandale, car en droit des télécommunications, le principe est que les opérateurs qui transportent l'information sur leurs réseaux jouissent d'une exonération de responsabilité. Mais de nombreux juges et auteurs de doctrine estiment que pour conjurer le « non-droit » auquel ils assimilent Internet, il convient d'appliquer aux intermédiaires techniques une responsabilité de type éditorial, ce qui conduit à faire peser sur ces acteurs une grande insécurité juridique.

En France, une affaire parmi bien d'autres illustre ces dérives. Elle concerne le service d'hébergement gratuit mis en place par Valentin Lacambre, alors l'un des fers de lance de l'Internet militant : Altern.org. À partir de 1997, les procès s'enchaînent. Valentin Lacambre doit par exemple répondre d'atteinte au droit à l'image en raison de la diffusion par l'un des sites qu'il héberge – et dont l'éditeur est anonyme – de clichés photographiques déjà parus dans la presse et représentant le mannequin Estelle Hallyday. Plutôt que de faire identifier l'internaute responsable via les données techniques en possession d'Altern, la plaignante préfère cibler l'hébergeur en

[27] Lionel Thoumyre. «Responsabilités sur le Web : une histoire de la réglementation des réseaux numériques». In : *Lex Electronica* 6.1 (2000).

[28] Il sera cependant acquitté l'année suivante. «Ex-CompuServe boss acquitted». In : *BBC* (nov. 1999).

partant du principe qu'il sera davantage solvable. Après un procès perdu en première instance, Lacambre saisit la Cour d'appel de Paris, présidée par la magistrate Marie-Françoise Marais. Dans sa décision le 10 février 1999, elle se montre encore plus sévère, rendant le jeune homme responsable de tous les contenus qu'il héberge, quand bien même il en ignorerait l'existence :

> « Considérant qu'en offrant, comme en l'espèce, d'héberger et en hébergeant de façon anonyme, sur le site ALTERN.ORG qu'il a créé et qu'il gère toute personne qui, sous quelque dénomination que ce soit, en fait la demande aux fins de mise à disposition du public ou de catégories de publics, de signes ou de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondances privées, Valentin Lacambre excède manifestement le rôle technique d'un simple transmetteur d'informations »[29].

Parce qu'il permet l'anonymat, Lacambre est donc déclaré responsable de la publication des photos litigieuses. Il se voit condamné à une peine de 300 000 francs d'amende, soit environ 45 000 euros. Cette jurisprudence le contraint à contrôler l'intégralité des sites hébergés et des contenus publiés, ce qui lui est matériellement impossible. Il est donc obligé de mettre la clé sous la porte, rendant la totalité des sites hébergés indisponibles. Ce sont près de 47 000 sites Internet qui disparaissent d'un coup, dont nombre de sites amateurs et militants.

2.2. La recherche d'un point d'équilibre : permettre l'identification des auteurs anonymes d'infractions

À l'époque, les défenseurs des libertés dénoncent ces tentatives visant à faire des intermédiaires techniques l'équivalent d'un directeur de publication, pointant le risque de voir ces acteurs exercer le rôle de censeur et donc d'extra-judiciariser la répression de la liberté d'expression. Pour eux, c'est à la personne responsable de la mise en ligne d'un contenu litigieux, et donc à l'auteur ou à l'éditeur, d'endosser la responsabilité civile ou pénale, et non à l'intermédiaire technique, ce dernier ne devant intervenir que pour censurer un contenu à la suite d'une décision judiciaire.

Ce dilemme va alors faire l'objet d'une construction juridique fragile mais dont se dégage quelques principes cohérents. Le Conseil d'État français en donne la formule dès 1998 dans son étude annuelle consacrée à Internet. Pour les auteurs, « il importe de trouver un équilibre entre la préservation

[29] CA Paris, 10 février 1999, Estelle Hallyday c. Valentin Lacambre.

de l'anonymat des individus sur les réseaux et la nécessité de pouvoir retrouver leur identité lorsqu'ils commettent des infractions ». Or, comme ils le soulignent, « l'anonymat qui protégerait l'auteur de messages illicites est très relatif ; en réalité [...], il n'y a pas de réel anonymat sur le réseau et les "traces" laissées par les utilisateurs au cours de leur navigation permettent souvent de remonter à la source de l'infraction ». Aussi recommandent-ils d'imposer aux intermédiaires techniques « des obligations de conservation des données de connexion [...] afin de faciliter les enquêtes judiciaires par une meilleure "traçabilité" des utilisateurs des réseaux »[30]. Ces données de connexion renvoient en particulier à l'adresse IP (pour *Internet Protocol*), l'équivalent pour Internet de l'adresse postale, qui permet de retrouver le titulaire de l'accès Internet correspondant.

Dans le même esprit, le Comité des ministres du Conseil de l'Europe adopte le 28 mai 2003 une « déclaration sur la liberté de la communication sur l'internet ». Quoique rappelant le principe selon lequel, « afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations et d'idées, les États membres devraient respecter la volonté des usagers de l'internet de ne pas révéler leur identité », le texte souligne qu' « un équilibre doit être trouvé entre le respect de la volonté des usagers de l'internet de ne pas divulguer leur identité et la nécessité pour les autorités chargées de l'application de la loi de retrouver la trace des responsables d'actes délictueux ».

C'est à ce point d'équilibre que les quelques règles de droit spécial adoptées au début des années 2000 pour encadrer la liberté d'expression sur Internet tentent de parvenir. D'abord, il est reconnu aux intermédiaires techniques une exemption de responsabilité. La directive européenne 2000/31/CE sur la société de l'information consacre ainsi le principe selon lequel les fournisseurs d'accès et hébergeurs ne sont pas responsables des activités illicites conduites par les utilisateurs de leurs services, en tous cas tant que l'existence d'un contenu illégal ne leur a pas été notifiée. Ils n'ont en outre aucune « obligation générale » de surveiller les activités de leurs utilisateurs[31]. Dans ses considérants, la directive prend également soin de préciser qu'elle « ne peut pas empêcher l'utilisation anonyme de réseaux ouverts tels qu'Inter-

[30] Jean-François Thery et Isabelle Falque-Pierrotin. *Internet et les réseaux numériques*. fr. rapport public. Conseil d'État, juin 1998. Disponible à l'adresse : http://www.ladocumentationfrancaise.fr/rapports-publics/984001519/index.shtml (visité le 29/05/2013), p. 131.

[31] Ce principe de responsabilité limité fait toutefois l'objet d'importantes remises en causes. Voy. s'agissant du droit d'auteur Etienne Montero et Quentin Van Enis. «Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries : Squaring the circle ?» In : *Computer Law & Security Review* 27.1 (fév. 2011), p. 21–35.

net » (considérant 14), ni être interprétée d'une manière qui remettrait en cause le « secret des communications », lequel est protégé dans le droit de l'Union européenne depuis 1997[32].

En France, ces règles sont transposées par la Loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004, laquelle garantit le droit à un anonymat limité, uniquement pour les éditeurs non-professionnels. Ils ne sont certes pas tenus de diffuser leur identité sur les sites qu'ils éditent, mais doivent toutefois avoir donné leurs noms, prénoms et adresse à leur hébergeur (article 6-III-2). Ce dernier est quant à lui soumis au secret professionnel, et ne peut en principe divulguer ces informations en dehors d'une procédure judiciaire. La loi précise en outre qu'hébergeurs et FAI sont tenus de conserver « les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires », et ce pendant une durée d'un an. Il s'agit notamment des informations d'identification renseignées dans les formulaires de souscription aux services en question ou, au minimum, des adresses IP correspondant à leur connexion.

Un droit à l'anonymat relatif est donc reconnu, celui-ci pouvant toutefois être contourné au travers de réquisitions de données permettant l'identification du titulaire de l'accès Internet utilisé pour commettre une infraction. En 2008, la CEDH va même consacrer à cet égard une obligation positive pour les États parties à la Convention. L'affaire en question, *K.U. c. Finlande*, concernait une fausse petite annonce publiée en ligne et contenant des propos diffamatoires relatifs à la sexualité d'un mineur. La police avait relevé l'adresse IP correspondant à l'accès Internet utilisé pour publier cette annonce, mais le fournisseur d'accès refusait de communiquer l'identité du détenteur de l'abonné correspondant, s'estimant lié par la confidentialité des télécommunications, ce en quoi les juridictions nationales lui avaient donné raison. Dans sa décision, la Cour a ainsi condamné la Finlande pour ne pas avoir prévu dans son droit interne des moyens de recours permettant d'identifier le titulaire de l'accès Internet et, partant, l'auteur des infractions, afin de le traduire en justice. Selon la Cour :

> « Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit

[32] Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

> parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui » (§49)[33].

La CEDH consacrait ainsi le principe selon lequel l'anonymat et la confidentialité des communications Internet – « préoccupations primordiales » associées aux article 8 et 10 de la Convention –, devaient être mis en balance avec d'autres droits et intérêts.

On retrouve cette même logique déclinée dans le droit de l'Union européenne, notamment dans le domaine spécifique de la lutte contre les infractions au droit d'auteur. En 2004, la directive 2004/48/CE relative au respect des droits de propriété intellectuelle (IPRED, de son acronyme anglais), a ainsi harmonisé les procédures d'identification des internautes. Elle permet aux ayants droit d'obtenir, par voie d'injonction judiciaire, l'identification des abonnés dont l'adresse IP a été relevée sur les réseaux peer-to-peer où s'échangent sans autorisation des œuvres artistiques protégées par le droit d'auteur[34]. En 2008, dans l'arrêt *Promusicae*, la CJUE a explicitement reconnu la possibilité de faire valoir cette faculté non seulement devant les juridictions pénales, mais également civiles[35]. De même en France, la loi HADOPI adoptée en 2009 a mis en place un mécanisme similaire pour la lutte contre les infractions au droit d'auteur sur Internet, mais cette fois sous l'égide d'une autorité administrative indépendante

2.3. Les solutions créatives mais problématiques des juges et législateurs

Dans le domaine du droit d'auteur notamment, ce renforcement de l'arsenal juridique a logiquement encouragé certains internautes à utiliser des outils d'anonymisation[36]. Une évolution qui illustre bien les obstacles techniques auxquels se heurtent les procédures d'identification. En effet, quand bien même les hébergeurs et fournisseurs d'accès seraient tenus de conserver pendant une durée déterminée l'adresse IP des personnes ayant contribué

[33]CEDH, 2 décembre 2008, *K.U. c. Finlande*, n° 2872/02.

[34]Directive 2004/49CE du 29 avril 2004 relative au respect des droits de propriété intellectuelle, article 8.

[35]CJUE, 29 janvier 2008, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, C-275/06 et CJUE, 19 avril 2012, *Bonnier Audio et al. c. Perfect Communication Sweden AB*, C-461/10.

[36]Stefan Larsson et Måns Svensson. «Compliance or Obscurity ? Online Anonymity as a Consequence of Fighting Unauthorised File-sharing». In : *Policy & Internet* 2.4 (déc. 2010), p. 77–105 ; Raphaël Suire, Sylvain Dejean et Thierry Pénard. *Une première évaluation des effets de la loi Hadopi sur les pratiques des internautes français*. Rapp. tech. Rennes : Université de Rennes 1, mar. 2010. Disponible à l'adresse : https://www.marsouin.org/article345.html (visité le 30/06/2017).

à la publication ou à la diffusion d'un contenu, il est possible que ce dernier ait utilisé un serveur intermédiaire (ou « proxy ») masquant son adresse d'origine – par exemple un VPN ou le réseau d'anonymisation TOR, des outils d'anonymisation qui sont parfaitement licites et bénéficient du régime d'exemption de responsabilité prévu par la directive 2000/31/CE sur la société de l'information[37]. Il est également possible que l'adresse IP collectée corresponde à un point d'accès Internet partagé entre plusieurs individus. Autant d'obstacles techniques qui, s'ils ne sont pas nécessairement insurmontables[38], peuvent compliquer les investigations et, parfois, faire échec aux poursuites.

Face à ces difficultés pratiques, les juges et les législateurs ont donc fait preuve d'une certaine « créativité », qui n'est pas toujours sans poser problème. Dans le cas de la loi HADOPI, le législateur français a ainsi fait le choix de créer une infraction pénale spécifique contre le titulaire de l'accès Internet repéré sur les réseaux de partage peer-to-peer. Lorsque celui-ci est condamné, ce n'est pas pour avoir lui-même enfreint le droit d'auteur – ce qui est, faute d'aveux ou de saisie du matériel informatique, généralement difficile à démontrer. Le juge ne cherchera pas non plus à le reconnaître comme responsable du fait d'autrui. C'est en fait la « négligence caractérisée » dans la surveillance de l'accès Internet – et donc le fait de ne pas avoir su empêcher la commission d'une infraction – qui est reproché, et passible d'une amende de 1500 euros[39].

Un autre exemple de ce type de « bricolage juridique » est fourni par une décision récente de la CJUE dans l'affaire *McFadden*. En l'espèce, un disquaire allemand avait ouvert son accès WiFi au public. Celui-ci était donc librement accessible à toute personne située dans un périmètre de plusieurs

[37]En effet, tant que les personnes qui opèrent ces serveurs proxy endossent un rôle à « caractère purement technique, automatique et passif », et qu'elles n'ont « pas la connaissance ni le contrôle des informations transmises ou stockées » (articles 12 et 15 de la directive 2000/31/CE), elles bénéficient du statut du « simple transporteur » d'informations (« *mere conduit* ») et ne peuvent être tenues pour responsables des agissements de leurs utilisateurs. Cela étant, les autorités nationales, et en particulier les autorités judiciaires, pourront exiger de ces intermédiaires techniques « qu'il soit mis un terme à toute violation ou que l'on prévienne toute violation » (voir le considérant 45 de la directive et son article 18). À noter également qu'en France, la LCEN exclut ces simples « transporteurs d'information » (dont le statut est prévu à l'article L32-3-3 du code des postes et télécommunications) des obligations d'identification des utilisateurs imposées aux fournisseurs d'accès et aux hébergeurs (aux articles 6-I-1 et 6-I-2 respectivement).

[38]Voy. par exemple les enquêtes récentes du FBI contre des groupes criminels utilisant la cryptographie pour tenter d'échapper à la répression : Jérôme Hourdeaux. «Comment le FBI a eu raison de l'« eBay de la drogue »». In : *Mediapart* (oct. 2013) ; Lily Hay Newman. *The Feds Would Rather Drop a Child Porn Case Than Give Up a Tor Exploit*. Mar. 2017. Disponible à l'adresse : https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/.

[39]Article L335-7-1 du code de la propriété intellectuelle.

dizaines de mètres autour de son magasin. Or, l'entreprise Sony avait repéré que l'une des œuvres de son catalogue avait été diffusée sans autorisation sur Internet depuis l'adresse IP du disquaire. L'ayant-droit avait demandé à la justice allemande de prononcer des mesures préventives capables de dissuader les utilisateurs du réseau ouvert de diffuser des œuvres sans autorisation. Saisie de cette question au détour d'une question préjudicielle, la CJUE a estimé que le droit de l'Union européenne ne s'opposait pas à ce qu'un juge enjoigne au gestionnaire d'un réseau ouvert de procéder à l'identification préalable de tous les utilisateurs d'un réseau WiFi ouvert. Allant à l'encontre des conclusions de l'avocat général, elle a en effet estimé que « sécuriser la connexion à Internet au moyen d'un mot de passe peut dissuader les utilisateurs de cette connexion de violer un droit d'auteur ou des droits voisins, pour autant que ces utilisateurs soient obligés de révéler leur identité afin d'obtenir le mot de passe requis et ne puissent donc pas agir anonymement »[40].

Cette décision, qui pouvait sembler de portée relativement restreinte en ce qu'elle subordonnait l'imposition d'un système d'identification à une procédure judiciaire préalable, semble d'ores-et-déjà faire l'objet d'interprétations qui mettent en cause l'existence même de ces réseaux ouverts[41]. Elle pourrait ainsi indirectement menacer le développement de réseaux Internet citoyens fondés sur le partage de points d'accès WiFi[42].

Du côté de la CEDH, l'affaire *Delfi AS c. Estonie* procède d'une logique similaire, et conduit à une solution jurisprudentielle qui va à l'encontre des équilibres traditionnels entourant la responsabilité des intermédiaires techniques[43]. Delfi, un site d'actualité estonien, avait été poursuivie pour diffamation par les juridictions de son pays en raison de commentaires jugés diffamatoires et insultants tenus par ses utilisateurs. Ces derniers réagissaient à un article de 2006 au sujet d'un opérateur de ferries qui avait décidé de changer ses liaisons maritimes :le cela le conduisait à briser les routes de glace qui se forment sur la mer gelée dans les pays nordiques, contribuant en retour à l'isolement de petites îles au large des côtes. Les conditions d'utilisation indiquaient que les propos tenus dans la section du site ouverte à commentaires – lesquels pouvaient être publiés anonymement – ne

[40] CJUE, 15 septembre 2016, *Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH*, C-484/14.

[41] Eleonora Rosati. *Higher Regional Court of Düsseldorf applies CJEU Mc Fadden decision*. Avr. 2017. Disponible à l'adresse : http://the1709blog.blogspot.com/2017/04/higher-regional-court-of-dusseldorf.html.

[42] Federica Giovanella et Mélanie Dulong de Rosnay. «Community wireless networks, intermediary liability and the McFadden CJEU case». In : *Communications Law* 22.1 (fév. 2017), p. 11–20.

[43] CEDH [GC], 16 juin 2015, *Delfi AS c. Estonie*, n° 64569/09.

reflétaient pas ceux des responsables du site. En outre, une fois informé des commentaires litigieux, Delfi avait promptement procédé à leur retrait, le jour même de la notification. En tant qu'éditeur d'un site comportant des espaces participatifs, l'entreprise faisait valoir son exemption de responsabilité tirée du statut d'hébergeur prévu dans la directive 2000/31/CE.

En dépit de ces précautions, la Grande chambre de la Cour a estimé dans sa décision que, puisque Delfi autorisait des commentaires anonymes et qu'elle trouvait un intérêt commercial à l'existence de ces espaces contributifs, il était « raisonnable » que l'entreprise soit déclarée responsable en lieu et place des auteurs des propos litigieux. Pour la CEDH :

> « L'anonymat est de longue date un moyen d'éviter les représailles ou l'attention non voulue. En tant que tel, il est de nature à favoriser grandement la libre circulation des informations et des idées, notamment sur Internet. Pour autant, la Cour ne perd pas de vue la facilité, l'ampleur et la vitesse avec lesquelles les informations sont diffusées sur Internet, et leur caractère persistant après leur publication sur ce média, toutes choses qui peuvent considérablement aggraver les effets des propos illicites circulant sur Internet par rapport à ceux diffusés dans les médias classiques » (§147).

Dans cette jurisprudence – précisée dans une décision rendue l'année suivante[44] –, les juges de Strasbourg confirment en fait la casuistique « exceptionnaliste » d'Internet qui se dégage de leur jurisprudence, et qui consiste à faire d'Internet un moyen de communication dont les caractéristiques créent des risques spécifiques pour les intérêts concurrents de la liberté d'expression, justifiant par là-même de plus grandes restrictions de libertés que celles admises pour les médias traditionnels[45]. En l'espèce, il y a l'idée – implicite dans la décision de la Cour mais soulignée à la fois par le gouvernement estonien et le juge Boštjan Zupančič dans une opinion concordante – que l'anonymat, par le sentiment d'impunité qu'il procure, encourage des expressions immodérées, voire violentes. Cela conduit la Cour à une solution en rupture avec le droit de l'Union européenne, créant une telle insécurité juridique pour les intermédiaires techniques qu'elle risque, comme l'expliquent les juges Nona Tsotsoria et András Sajó dans leur opinion dissidente, de

[44] CEDH, 2 mai 2016, *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, n° 22947/13. Cet arrêt semble confirmer la portée relativement limitée de l'arrêt Delfi aux propos qui relèveraient clairement du discours de haine ou d'incitation à la violence. Sur cette question, voy. la contribution de C. Ruet dans le présent ouvrage.

[45] Félix Tréguer. «Internet dans la jurisprudence de la Cour européenne des droits de l'Homme». In : *Revue des droits et libertés fondamentaux* (mai 2013).

conduire à la « censure collatérale » d'expressions légitimes. Quant au rapporteur des Nations Unies pour la liberté d'opinion et d'expression, il estime pour sa part que cette jurisprudence « risque d'aboutir soit à la mise en place de politiques d'enregistrement des utilisateurs sous leur nom véritable, ce qui nuirait à l'anonymat, soit à l'élimination pure et simple des commentaires sur les sites Web qui n'ont pas les moyens d'appliquer des procédures de modération, au détriment des petits médias indépendants »[46].

On mesure en tout cas au terme de ce survol que, plutôt qu'un droit à part entière, l'anonymat et la confidentialité des communications sont directement subordonnées à la liberté d'expression et à la vie privée auxquels ils se rattachent. S'ils sont, selon l'expression de la CEDH, des « préoccupations primordiales » étroitement associées à ces droits – ce qui peut par exemple légitimer le fait d'imposer à un acteur oligopolistique comme Facebook de permettre à ses utilisateurs de s'exprimer sous pseudonyme[47] –, ils n'ont évidemment rien d'absolu. Les efforts des législateurs et des juges ces vingt dernières années ont donc consisté à instaurer des règles procédurales permettant soit de procéder à l'identification des auteurs des propos litigieux soit, lorsque cela s'avérait trop complexe en pratique, de prévenir ou de remédier aux abus occasionnés par la communication anonyme. Au final, ces débats traduisent la recherche d'un équilibre complexe et toujours précaire entre d'un côté, la liberté d'expression et la vie privée et, de l'autre, des intérêts concurrents. Un équilibre désormais radicalement menacé par les formes contemporaines de la surveillance d'Internet.

3. Le droit à l'anonymat et au chiffrement, rempart indispensable à la surveillance

À la fin du XVIII^{e} siècle, sous le sceau de l'état d'exception provoqué par les guerres révolutionnaires, le Comité de Salut public avait pu, pendant un temps, prononcer l'ouverture de toutes les lettres en provenance de l'étranger (voy. *supra*). Cette remise en cause radicale du droit au secret des correspondances – pourtant reconnu quelques mois plus tôt par le législateur – restait toutefois limitée aux seuls courriers de l'infime partie de la population qui entretenait alors des correspondances avec l'étranger. En dépit de tentations bien réelles qu'illustre par exemple la réactivation du contrôle postal et de la censure pendant la Première Guerre mondiale, « tout surveiller » était tout simplement impossible. Bien sûr, la police pou-

[46] Kaye, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression sur le chiffrement et l'anonymat*.

[47] Julia Fioretti. «German regulator orders Facebook to allow pseudonyms». In : *Reuters* (juin 2015).

vait tourner ses espions et autres informateurs contre les groupes suspects, les régimes totalitaires organiser l'auto-surveillance des citoyens et tenter ainsi de se prémunir de toute dissidence. Mais la surveillance des communications de l'ensemble de la population est demeurée pendant longtemps une mesure impraticable, trop coûteuse en ressources pour être réellement envisagée.

Certes, une surveillance totale des communications reste aujourd'hui encore impossible en pratique. L'ère numérique marque cependant une rupture historique en ce que le principe même d'une telle surveillance n'apparaît plus totalement chimérique. Non seulement la notion de communication sort radicalement transformée des évolutions socio-techniques associées au numérique, absorbant non seulement l'expression publique et les correspondances privées, mais également toutes sortes de comportements et d'activités individuelles ou collectives. Mais en outre, les outils techniques dédiés à la collecte et à l'analyse de l'ensemble de ces données, de même que le droit qui encadre l'usage de ces technologies, n'excluent plus, dans leur principe même, l'idée d'une surveillance sinon totale du moins massive. Dans ce contexte transformé, le droit à l'anonymat et la confidentialité des communications apparaissent donc à la fois extrêmement fragilisés, et plus importants que jamais.

3.1. La conservation généralisée des données de connexion : émergence d'un nouveau régime de surveillance

Cette rupture historique trouve en partie son origine dans le régime de justification illibéral qui s'accentue au lendemain des attentats du 11 septembre 2001[48]. Dans les jours qui suivent ces attaques, le Royaume-Uni, la France et l'Italie vont ainsi imposer aux opérateurs télécoms une conservation généralisée des données techniques, ou « métadonnées », associées aux communications téléphoniques et Internet. À l'époque, il ne s'agit plus seulement d'identifier les internautes, et en particulier ceux qui se seraient exprimés dans l'espace public numérique, mais de retracer l'origine et la destination de l'ensemble des communications traitées et acheminées par les opérateurs télécoms (adresse IP d'origine et de destination, numéro appelé ou appelant). Alors présentée comme une mesure exceptionnelle et donc limitée dans le temps, cette forme nouvelle de surveillance sera élargie à l'ensemble des États-membres de l'Union européenne après les attentats de Madrid et de Londres, avec l'adoption en moins de six mois de la directive 2006/24/CE sur la conservation des données.

[48] Mireille Delmas-Marty. *Libertés et sûretés dans un monde dangereux*. Seuil, 2010.

Ce régime de conservation généralisée a depuis fait l'objet de nombreuses décisions de la part de juges nationaux. En Roumanie (2009), en Allemagne (2010), en Bulgarie (2010), à Chypre (2011) et en République Tchèque (2011), des juges nationaux ont ainsi estimé que de telles dispositions emportaient une ingérence disproportionnée dans la vie privée et la liberté de communication de leurs citoyens. Saisie à son tour, la CJUE a rendu en avril 2014 un arrêt historique invalidant l'ensemble de la directive de 2006[49]. Dans cet arrêt, *Digital Rights Ireland c. Irlande*, elle a rejeté le principe d'une conservation des données de personnes pour lesquelles il n'existe, dit-elle, « aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves ». Selon la Cour, « ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci » (§27).

L'avocat général de la Cour, Pedro Cruz Villalón, avait au préalable souligné « l'importance acquise par les moyens de communications électroniques dans les sociétés modernes, qu'il s'agisse des réseaux mobiles numériques ou d'Internet, et leur utilisation massive et intensive par une fraction très importante des citoyens européens dans tous les champs de leurs activités privées ou professionnelles »[50]. Ce sont des considérations similaires sur l'évolution des technologies numériques et de leurs usages qui, l'année suivante, conduiront un conseiller d'État français à plaider que « la *summa divisio* entre accès de données et accès de contenus n'a probablement plus la même portée qu'il y a quelques années ». Il ajoute alors : « sans doute l'ingérence dans la vie privée que constitue l'accès aux données de connexion doit être réévalué »[51].

Derrière le langage mesuré de ces éminents juristes, on comprend que le numérique a fait voler en éclat la distinction traditionnelle entre métadonnées et contenu, et donc les équilibres attachés au secret des communications. Après deux arrêts significatifs mais à certains égards contradictoires

[49] CJUE [GC], 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, affaires jointes C-293/12 & C-594/12.

[50] Conclusions de l'avocat général dans l'affaire *Digital Rights*, présentées le 12 décembre 2013, § 73-74.

[51] Cité dans : Marc Rees. *Données de connexion : la QPC de la Quadrature, FDN et FFDN transmise au Conseil constitutionnel !* Mai 2015. Disponible à l'adresse : https://www.nextinpact.com/news/95334-donnees-connexion-qpc-quadrature-fdn-et-ffdn-transmise-au-conseil-constitutionnel.htm.

en matière de surveillance[52], la CEDH pourrait à son tour avoir à se prononcer sur ces questions, notamment pour renforcer les garanties procédurales associées à la surveillance des métadonnées. Les recours formés contre les activités de surveillance des agences de renseignement françaises et britanniques ces derniers mois devraient bientôt lui en donner l'occasion.

3.2. De la surveillance ciblée à la surveillance massive et exploratoire

La conservation généralisée des données de connexion illustre en fait le changement de paradigme dans les pratiques policières contemporaines. À la surveillance détaillée de quelques cibles bien identifiées illustrée par la pratique des « écoutes judiciaires », les agences de renseignement et les services de police ont repris à leur compte des doctrines issues du monde militaire et fondées sur la détection de « signaux faibles », de traces associées à des comportements suspects, tels que la consultation de certains contenus sur Internet[53]. Il s'agit, dans l'océan de données numériques qui circulent le long des réseaux transnationaux, de déceler au sein du trafic, à la volée et en temps réel, des mots-clés, des identifiants, des signatures numériques... Et ainsi, comme l'affirmait un ministre français en 2015 à l'occasion du débat parlementaire de la loi relative au renseignement, de repérer « des connexions à certaines heures, depuis certains lieux, sur certains sites », « de repérer ainsi un trafic caractéristique »[54].

Comme le montrent les récentes réformes des cadres juridiques associés au renseignement en Europe, ce sont les métadonnées qui apparaissent comme les plus stratégiques pour les systèmes contemporains de surveillance.

[52]CEDH [GC] , 4 décembre 2015, *Zakharov c. Russie*, n° 47143/06 ; CEDH [4ème section] , 6 juin 2016, *Szabó et Vissy c. Hongrie*, n° 37138/14. Voy. notamment le commentaire suivant : *Arrêt ambiguë de la Cour européenne des droits de l'Homme sur les questions de surveillance - Association Européenne pour la Défense des Droits de l'Homme*. Jan. 2016. Disponible à l'adresse : http://www.aedh.eu/Arret-ambigue-de-la-Cour.html.

[53]En matière de remise en cause de l'anonymat dans la consultation d'informations en ligne en rapport avec la surveillance d'État, voir par exemple la création en France du délit de consultation habituelle de sites terroristes : Pierre Alonso. *Première condamnation pour consultation de sites terroristes*. Août 2016. Disponible à l'adresse : http://www.liberation.fr/france/2016/08/10/premiere-condamnation-pour-consultation-de-sites-terroristes_1471320, Voy. également le recours du groupe inter-associatif d'action contentieuse Les Exégètes amateurs contre le système français de blocage administratif de sites Web, où est contestée la légalité du choix d'une technique de blocage qui conduit à ce que le ministère de l'Intérieur recueille les adresses IP des personnes ayant tenté de se connecter aux sites ainsi censurés : https://exegetes.eu.org/dossiers/filtragecazeneuve/index.html#orangefail. Voy. enfin la surveillance du lectorat du site WikiLeaks par les services britanniques : *NSA and GCHQ spying on WikiLeaks*. Fév. 2014. Disponible à l'adresse : https://wikileaks.org/NSA-and-GCHQ-spying-on-WikiLeaks.html.

[54]Propos de Jean-Yves Le Drian, alors ministre français de la Défense. Assemblée nationale, deuxième séance du mercredi 15 avril 2015.

En effet, elles sont non seulement extrêmement signifiantes et peuvent suffire à décrire l'identité et les activités des personnes surveillées. Mais elles se prêtent en outre à un stockage massif et un traitement automatique à travers des outils Big Data, qui permettant des mises en relation et des recoupements statistiques à grande échelle pour tenter de décrire et d'anticiper des phénomènes sociaux[55].

Pour capter ces données, on sait par exemple que les services de renseignement britanniques ou français ont déployé au cœur des réseaux des opérateurs télécoms nationaux des sondes DPI (pour « *Deep Packet Inspection* ») permettant de scanner en temps réel une grande partie du trafic à la recherches de métadonnées de toutes sortes, telles que l'utilisation de protocoles de chiffrement, des pseudonymes, des adresses IP, dans le but de de repérer des comportements suspects[56]. Aux Pays-Bas, la police semble vouloir s'approprier ces mêmes techniques d'enquête. Souhaitant retrouver l'identité des responsables d'une fraude bancaire sur Internet, elle a ainsi fait installer une de ces sondes dans le data-center d'un grand hébergeur situé sur le territoire national. L'engin était paramétré pour ausculter l'ensemble du trafic à la recherche de 400 pseudonymes utilisés sur un service de messagerie instantanée par des hackers russes déjà connus des services de police[57]. Lorsque les paquets de données scannés comportaient ces identifiants, ils étaient collectées et soumis à une analyse détaillée.

Ces pratiques, identifiées dès la fin des années 1990[58], étaient jusque–là mal documentées. Les informations internes de la *National Security Agency* (NSA), révélées par le lanceur d'alerte Edward Snowden, ont permis de mieux les comprendre. Depuis 2013, ces révélations ont permis de détailler la manière dont les services de renseignement pouvaient exploiter des failles du droit existant dans l'ombre du secret d'État afin de s'engager dans des formes de surveillance exploratoire, passant au crible les communications de segments entiers de la population et captant à grande échelle non seulement les métadonnées – données les plus stratégiques –, mais également le contenu des communications[59]. Ce sont ces pratiques que les réformes du

[55] David Lyon. *Surveillance After Snowden*. Polity Press, 2015, p. 78 et suiv.

[56] Jérôme Hourdeaux. *Comment les services de renseignement ont mis en place une surveillance générale du Net dès 2009*. Juin 2016. Disponible à l'adresse : https://www.mediapart.fr/journal/france/060616/comment-les-services-de-renseignement-ont-mis-en-place-une-surveillance-generale-du-net-des-2009.

[57] Geplaatst door P/K. *Dutch-Russian cyber crime case reveals how the police taps the internet*. Juin 2017. Disponible à l'adresse : http://electrospaces.blogspot.com/2017/06/dutch-russian-cyber-crime-case-reveals.html.

[58] Steve Wright. *An appraisal of technologies for political control*. Rapp. tech. European Parliament, jan. 1998. Disponible à l'adresse : https://cryptome.org/stoa-atpc.htm (visité le 30/01/2015).

[59] Glenn Greenwald. *No Place to Hide : Edward Snowden, the NSA, and the U.S. Surveillance State*. [S.l.] : Metropolitan Books, 2014.

renseignement adoptées en France, au Royaume-Uni, en Allemagne ou aux Pays-Bas depuis 2015 sont venues légaliser, et dont la CEDH sera là encore prochainement amenée à juger[60].

Or, ces pratiques ne vont pas seulement à l'encontre de principes fondateurs de l'État de droit, comme la présomption d'innocence ou le droit à un procès équitable. Elles sont d'autant plus délétères pour la liberté de communication qu'elles visent ceux qui jouent un rôle clé dans le fonctionnement démocratique : les journalistes, avocats et militants. Un document de l'archive Snowden en date de 2008 montre ainsi que, durant un exercice conduit par le *Government Communication Headquarters* (GCHQ) britannique, plus de 70 000 courriels échangés entre des journalistes et rédacteurs en chef du *Guardian*, de la BBC, de *Reuters*, du *New York Times*, du *Washington Post*, du *Monde*, du *Sun* et de la NBC avaient été collectés en moins de 10 minutes, puis sauvegardés et partagés au sein de l'agence[61]. D'après le document en question, « les journalistes et reporters des différents médias d'actualité représentent une menace pour la sécurité », en particulier « les "journalistes d'investigation" qui se spécialisent dans des enquêtes relatives aux questions de défense, soit dans un but commercial soit en fonction de ce qu'ils estiment être d'intérêt public ».

En février 2017, le *Spiegel* rapportait également que le *Bundesnachrichtendienst* (BND), l'agence allemande de renseignement extérieur, avait depuis 1999 procédé à la surveillance des numéros de téléphone, de fax et d'e-mails de nombreux journalistes du *New York Times*, de la BBC ou de *Reuters*, mais aussi de nombreux autres organismes de presse de par le monde[62]. Dans ces conditions, la protection des sources ne peut tout simplement pas être assurée.

Les avocats et organisations de défense des droits semblent également être des cibles de choix pour les agences de renseignement, comme l'illustrent des affaires récentes jugées par l'*Investigatory Powers Tribunal* britannique, qui examine les recours formés au niveau national contre les agences de renseignement du pays. Dans une affaire récente, ce dernier a indiqué que le GCHQ avait pu, sans contrevenir au droit applicable, surveiller les communications de plusieurs ONG dont Amnesty International[63]. Une autre

[60] Voy. section 3.1. Voy. aussi : Félix Tréguer. «Intelligence Reform and the Snowden Paradox : The Case of France». In : *Media and Communication* 5.1 (mar. 2017), p. 17–28.

[61] James Ball. *GCHQ captured emails of journalists from top international media.* Jan. 2015. Disponible à l'adresse : https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post.

[62] Alison Smale. *Germany's Intelligence Service Spied on Journalists, Report Says.* Fév. 2017. Disponible à l'adresse : https://www.nytimes.com/2017/02/25/world/europe/germany-bnd-surveillance-der-spiegel.html.

[63] *UK surveillance Tribunal reveals the government spied on Amnesty International.* Juil.

affaire a permis de confirmer que non seulement la surveillance des communications entre un avocat et son client était autorisée par les codes de procédures internes employés par les services, mais que de manière plus générale, différentes catégories de communications sensibles pourtant censées bénéficier d'un degré de protection renforcé constituaient en fait des cibles prioritaires pour les services[64].

3.3. Le droit au chiffrement, clé de voûte de l'anonymat et du secret des correspondances ?

Depuis 2013, la prise de conscience provoquée par les révélations d'Edward Snowden a conduit à d'importants progrès pour la reconnaissance d'un droit au chiffrement, qui apparaît désormais comme l'un des seuls moyens effectifs de rétablir un peu de l'équilibre perdu entre, d'un côté, l'anonymat et la confidentialité des communications et, de l'autre, la sécurité nationale et la protection des droits d'autrui.

Dans un rapport paru en 2015, l'Assemblée parlementaire du Conseil de l'Europe indique ainsi que, « jusqu'à ce que les États acceptent de fixer des limites aux programmes de surveillance massive menés par leurs agences de renseignement, le chiffrement généralisé visant à renforcer la vie privée constitue la solution de repli la plus efficace pour permettre aux gens de protéger leurs données »[65]. Au même moment, dans son rapport au Conseil des droits de l'Homme des Nations Unies, David Kaye affirmait notamment que « le chiffrement et l'anonymat, ainsi que les notions de sécurité qui les sous-tendent, offrent la confidentialité et la sécurité nécessaires à l'exercice

2015. Disponible à l'adresse : https://www.amnesty.org/en/latest/news/2015/07/uk-surveillance-tribunal-reveals-the-government-spied-on-amnesty-international/.

[64]Ryan Gallagher. *British Spies Are Free to Target Lawyers and Journalists*. Nov. 2014. Disponible à l'adresse : https://theintercept.com/2014/11/06/uk-surveillance-of-lawyers-journalists-gchq/.

[65]Pieter Omtzigt. *Les opérations de surveillance massive*. Rapp. tech. 12734. Strasbourg : Assemblée parlementaire du Conseil de l'Europe, mar. 2015. Disponible à l'adresse : http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-fr.asp?fileid=21583&lang=fr (visité le 26/01/2015) ; Avant cela, un rapport du Parlement européen de février 2014 sur le scandale de la NSA avait déjà appelé les autorités européennes à soutenir les outils de chiffrement. Celui-ci invitait en effet « l'ensemble des États membres, la Commission, le Conseil et le Conseil européen à soutenir sans réserve, y compris au moyen de financements dans le domaine de la recherche et du développement, le développement des capacités innovatrices et technologiques européennes en matière d'outils, de sociétés et de fournisseurs dans le secteur de l'informatique (matériel, logiciels, services et réseau), notamment aux fins de la cybersécurité et des capacités de cryptage et cryptographiques » : Claude Moraes. *Rapport d'initiative sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures*. Rapp. tech. 2013/2188(INI). Bruxelles : Parlement européen, fév. 2014. Disponible à l'adresse : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN.

du droit à la liberté d'opinion et d'expression à l'ère du numérique »[66].

Au plan technique, de nombreux projets ont connu un véritable regain d'intérêt, avec le déploiement de logiciels et applications intégrant des solutions cryptographiques robustes, protégeant les communications « bout-à-bout » (c'est-à-dire depuis l'émetteur jusqu'au destinataire et non seulement entre l'utilisateur et l'intermédiaire technique), tout en tâchant de les rendre plus faciles d'utilisation. Chez les groupes militants ou dans les organes institutionnels comme l'*Internet Engineering Task Force* (IETF), chargée de la standardisation des protocoles Internet au niveau mondial, l'affaire Snowden a en effet provoqué une prise de conscience quant à l'importance du chiffrement. Même chez les grandes entreprises de la Silicon Valley, pointées du doigt pour leur participation aux programmes de surveillance de la NSA, des déploiements similaires sont intervenus afin de rassurer les utilisateurs.

Bien évidemment, les forces de police, et, plus encore, les agences de renseignement disposent de moyens pour contourner le chiffrement et conduire à bien leurs missions. De nombreuses « métadonnées » circulent en clair sur les infrastructures des intermédiaires techniques et constituent autant de traces qui, on l'a vu, peuvent fournir de nombreux renseignements aux enquêteurs. Même lorsque les informations sont chiffrées, les services peuvent contourner ces systèmes, par exemple en retrouvant le mot de passe associé aux clés de déchiffrement, en exploitant des failles de sécurité, ou en pénétrant directement dans les équipements informatiques des cibles où les données s'affichent en clair (via des méthodes de hacking). Pour les agences les mieux dotées, des super-calculateurs dédiés à la cryptanalyse peuvent également permettre de « casser » les codes secrets. Les documents Snowden ont d'ailleurs confirmé que l'ensemble du trafic chiffré constituait une cible de choix pour la NSA, et que celle-ci disposait de plusieurs moyens techniques et juridiques pour contourner des systèmes d'anonymisation comme le réseau TOR[67].

En dépit de ces limites, le chiffrement n'en demeure pas moins un outil essentiel pour restaurer un équilibre perdu. Il rend en effet de nombreuses données illisibles pour les dispositifs de surveillance massive et automatisée développés ces dernières années, sans entraver réellement les techniques de surveillance ciblée[68]. Et c'est justement cette efficacité relative qui conduit,

[66] Kaye, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression sur le chiffrement et l'anonymat*.

[67] Jacob Appelbaum, A. Gibson et J Goetz. *NSA targets the privacy-conscious*. Juil. 2014. Disponible à l'adresse : http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html.

[68] Évidemment, le chiffrement peut compliquer la mise en œuvre de certaines techniques de surveillance. Certains magistrats ont ainsi fait part d'une plus grande difficulté à accéder à des informations stockées sur des disques durs chiffrés. Voy. Cyrus R. Jr Vance

depuis 2015, à une offensive concertée de deux côtés de l'Atlantique pour contraindre les entreprises du numérique à affaiblir leurs systèmes cryptographiques. L'argument de la lutte antiterroriste est bien sûr mis en avant pour justifier de nouvelles restrictions à l'usage de ces techniques. Mais outre les défenseurs des libertés publiques qui s'opposent à ces propositions, nombre d'experts soulignent que tout affaiblissement du chiffrement menacerait à terme la sécurité de l'ensemble de l'infrastructure numérique, exposant les communications non seulement à la surveillance des États mais également à toutes sortes d'acteurs criminels[69].

Dans les années à venir, les juridictions européennes auront sans doute à intervenir à leur tour dans ces débats. Il est donc à espérer que, dans ce contexte, la CJUE et la CEDH voudront bien renforcer leur jurisprudence pour faire du droit à l'anonymat et à la confidentialité des communications une composante essentielle de la liberté d'expression et de la vie privée, toute en reconnaissant le rôle du chiffrement dans la mise en œuvre effective de ce droit. Cela ne suffira certes pas à rompre la logique multi-séculaire qui fait que ceux qui font usage de leurs libertés pour défendre la démocratie sont suspectés par l'État au même titre que les criminels les plus violents. Mais au moins auront-ils la certitude d'avoir les droits humains de leur côté.

et al. «When Phone Encryption Blocks Justice». In : *The New York Times* (août 2015).

[69]Wolfgang Schulz et Joris van Hoboken. *Human rights and encryption*. Rapp. tech. Paris : UNESCO, 2016. Disponible à l'adresse : http://unesdoc.unesco.org/images/0024/002465/246527E.pdf, p. 24.