01 janvier 2020



L'EUROPE DE LA CYBERSÉCURITÉ, POUR UNE LIBERTÉ SÉCURISÉE

TRANS • EUROPE EXPERTS



UNIVERSITÉ BRETAGNE SUD

"L'Université Cyber"

Premier centre de formation
d'entraînement et de recherche
en gestion de crise cyber

Cyber Security Center

ubs : Université Bretagne Sud

L'Europe de la cybersécurité

www-cybersecuritycenter.univ-ubs.fr

EDITO

L'Europe de la cybersécurité, pour une liberté sécurisée





Par Célia Zolynski et Michel Séjean

Quel meilleur endroit que le FIC pour réunir le savoir-faire français sur l'Europe de la cybersécurité ? Avec le sens de la formule qu'on lui connaît, le fondateur de cet événement incontournable a résumé les stratégies qui animent la cybersécurité à l'échelle mondiale : alors que les États-Unis instaurent une liberté surveillée, que les régimes autoritaires mettent en place une sécurité surveillée, l'Europe a l'occasion de se démarquer en œuvrant pour une liberté sécurisée (Général M. Watin-Augouard).

Une telle stratégie doit mobiliser toutes les énergies, toutes les compétences. Alors que le FIC était créé depuis peu, plusieurs universitaires français décidaient en 2009 d'agir pour que l'expertise française soit plus visible et accessible sur les sujets européens, en créant le réseau TEE (Trans Europe Experts).

En phase avec le thème de cette année 2020 qui porte sur l'Humain, trois dimensions ont mobilisé les membres du groupe TEE autour de l'Europe de la cybersécurité : la première est individuelle, qui suppose de sécuriser l'identité numérique de l'Humain ; la deuxième est relationnelle, qui impose de protéger la confidentialité numérique des Humains en chiffrant leurs échanges ; et la troisième dimension est collective, qui vise à penser une autonomie numérique pour l'Europe – plus connue sous le nom d'autonomie stratégique – distincte de la souveraineté dont le concept est inadapté à l'Union européenne.

Identité, Confidentialité, Autonomie, telles pourraient être trois composantes essentielles d'une liberté sécurisée dans un réseau cybernétique européen pensé pour l'Humain. La régulation y jouerait un rôle structurant, l'Union européenne ayant été fondée par le droit et héritière d'une tradition humaniste dans laquelle la réglementation libère l'Humain au lieu de l'opprimer. C'est en assumant son savoir-faire régulateur que l'Union européenne a pu inspirer les législations de pays étrangers virtuoses en matière de cybersécurité – songeons à l'entrée en vigueur en janvier 2020 d'une réglementation californienne directement inspirée par le RGPD, tout comme le sont d'ailleurs les nouveaux textes japonais et brésiliens sur la protection des données personnelles.

Il y a urgence à transformer l'Union européenne en un puissant réseau qui protège et promeuve la liberté grâce à la cybersécurité. *« Les nouveaux réseaux de services numériques deviennent des États et les États traditionnels tardent à devenir des réseaux »* écrit Pierre Bellanger (Comment gagner une guerre perdue ? in Cahiers de la Sécurité et de la Justice 2019, n° 45, p. 27 s., spéc. p. 28).

Mais il n'y a pas de fatalité : pour reprendre en mains notre sort, il faut encore des femmes et des hommes qui connaissent l'Europe et qui pensent la cybersécurité. En Allemagne, toute cette expertise est immédiatement disponible dans des instituts de type Max Planck. Mais où la trouver en France ? Le réseau TEE fut créé il y a dix ans pour rassembler nos savoir-faire et contribuer aux politiques de l'Union européenne.

Ce livret a pour ambition d'unir dans la diversité les regards de nos juristes, politistes et géographes pour que l'Humain soit au centre d'une Europe de la cybersécurité au service de la liberté.



SOMMAIRE

05 Enjeux d'une Europe de la cybersécurité

06 L'Europe de la cybersécurité : l'action du Conseil de l'Union européenne **– Par Michel Séjean**

08 De la 5G aux débats sur le hack-back, des initiatives européennes aux négociations au sein de l'ONU : quels enjeux pour la régulation de la cyber-sécurité en 2020 ? – **Par Karine Bannelier**

10 Convention de Budapest et cybercriminalité **Par Nadir Ouchene**

12 Un cyberespace européen éthique et résilient **Par Anne Cammilleri**

14 Approches culturelles de la cybersécurité **Par Anne-Thida Norodom**

16 Acteurs d'une Europe de la cybersécurité

17 La Fondation Women4Cyber – **Par Anne Le Hénanff**

19 AI-REGULATION.COM : Une Chaire sur la régulation de l'Intelligence Artificielle **Par Théodore Christakis et Karine Bannelier**

21 Zoom sur le FIC 2020 : l'Humain au cœur de l'Europe de la cybersécurité

22 Technologies de reconnaissance faciale : encore trop de méconnaissance du sujet dans l'UE **Par Michel Séjean**

24 Identité numérique et cybersécurité **Par Chloé Hervochon et Thibault Douville**

26 Confidentialité numérique : pour un chiffrement sans porte dérobée des données traitées par les confidents **Par Émilie Pouffier-Thompson et Michel Séjean**

28 Chiffrement et confiance en ligne **Par Emmanuel Netter**

30 De Magritte au CLOUD Act et à E-Evidence : Quels régimes juridiques pour l'accès à la preuve numérique ? – **Par Théodore Christakis**

32 Souveraineté, cybersécurité et Union européenne – **Par Anne-Thida Norodom**

34 Souveraineté numérique et autonomie stratégique : la nécessaire clarification pour une ambition européenne – **Par Alix Desforges**

36 L'extraterritorialité en questions : CLOUD Act et RGPD – **Par Fabienne Jault-Seseke**

38 La lutte contre la prolifération des programmes informatiques malveillants et le droit international – **Par Aude Géry**

40 Le droit international applicable aux opérations dans le cyberespace – **Par François Delerue**

UNE PUBLICATION DU RÉSEAU TRANS EUROPE EXPERTS

SIEGE : 12 PLACE DU PANTHÉON
75005 PARIS – FRANCE
0033 (0) 6 62 84 47 45

FABIENNE JAULT-SESEKE, PROFESSEUR DE DROIT PRIVÉ, CO-PRÉSIDENTE DE TEE
SOPHIE ROBIN-OLIVIER, PROFESSEUR DE DROIT PRIVÉ, CO-PRÉSIDENTE DE TEE
ZOÉ JACQUEMIN, MAÎTRE DE CONFÉRENCES EN DROIT PRIVÉ, SECRÉTAIRE GÉNÉRALE DE TEE
JULIEN BOISSON, MAÎTRE DE CONFÉRENCES EN DROIT PRIVÉ, TRÉSORIER DE TEE

CONTACT
CONTACT@TRANSEUROPEXPERTS.EU

© 2020 – TRANS EUROPE EXPERTS / ESPRIT COM'
Les opinions émises dans cette publication n'engagent que les auteurs. Les publicités et rédactionnels insérés le sont sous la responsabilité des annonceurs. L'éditeur se réserve le droit de refuser toute demande d'insertion sans avoir à motiver son refus. Reproduction intégrale ou partielle interdite sans autorisation de Trans Europe Experts.



01

ENJEUX D'UNE EUROPE DE LA CYBERSÉCURITÉ

L'EUROPE DE LA CYBERSÉCURITÉ : L'ACTION DU CONSEIL DE L'UNION EUROPÉENNE

Michel SÉJEAN

Qu'il semble loin, le temps où l'on pouvait reprocher à l'Union européenne (UE) de ne s'occuper que de la courbure des concombres ! En quatre dates, l'année 2019 aura démontré l'engagement de l'UE pour une cybersécurité qui nous protège des tragédies. Du plus ancien au plus récent, les actes de ce *« tournant 2019 »* méritent un rappel et une appréciation.

Acte I : le 13 mars, le Conseil de l'Union européenne a entamé des négociations avec le Parlement européen qui doivent aboutir à la création, à partir du 1er janvier 2021, et au plus tard le 31 décembre 2029, d'un Centre de compétences industrielles, technologiques et de recherche en matière de cybersécurité. Ce Centre serait soutenu par un Réseau de compétences en cybersécurité reposant sur des centres nationaux de coordination désignés par les États membres. L'ensemble ainsi constitué doit compléter les activités de la nouvelle Agence de l'UE pour la cybersécurité, ce qui nous mène à l'Acte II.

Acte II : le 9 avril, le Conseil a adopté le règlement sur la cybersécurité – également appelé *« Cybersecurity Act »* ou *« Acte législatif sur la cybersécurité »*. Ce texte d'application directe crée un système européen de certification des produits en matière de cybersécurité, et transforme l'actuelle Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) en un organe permanent rebaptisé

1. *« L'avenir de la cybersécurité européenne, Entretien avec M. le député E. Bothorel »*, sd-magazine.com, 27 nov. 2019
2. Voir article page 5
3. www.consilium.europa.eu
4. H. Ferrebœuf et J.-M. Jancovici, *« La 5G est-elle vraiment utile ? »*, Le Monde, 9 janv. 2020

Agence de l'Union européenne pour la cybersécurité. Les questions relatives à l'étendue des compétences de ce nouvel organe permanent sont nombreuses. Il s'agira par exemple de décider comment animer la coopération européenne sans empiéter sur la souveraineté nationale de chaque État membre[1]. En d'autres termes, la nouvelle agence doit-elle devenir un organe supranational, ou faut-il limiter strictement son périmètre à la coordination des efforts des États membres[2] ?

Acte III : le 14 mai 2019, le Conseil de l'Union européenne a adopté une décision *« concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres »* (Décision PESC 7299/19). Cet instrument est la suite logique des conclusions que le Conseil avait adoptées le 19 juin 2017 pour une réponse diplomatique conjointe face aux actes de cybermalveillance (décision également appelée *« boîte à outils cyberdiplomatique »*). Par cette décision, l'UE se donne les moyens d'imposer des sanctions à des entités qui mènent des cyberattaques portant atteinte aux intérêts de l'UE ou de ses États membres. Sont également sanctionnés la tentative d'attaque, le soutien financier et l'implication directe ou indirecte dans de telles attaques.

Acte IV : Enfin, le 3 décembre 2019, le Conseil a adopté des conclusions relatives aux dangers que représente la 5G pour la sécurité européenne. Certes, le Conseil reconnaît que *« les réseaux 5G prendront place parmi les infrastructures essentielles pour le maintien de fonctions sociétales et économiques vitales »*[3]. Il souligne toutefois le risque de dépendance à la 5G pour les opérateurs d'importance vitale (OIV) ou les opérateurs de services essentiels (OSE) : le point n° 15 des conclusions souligne la nécessité pour les États membres d'évaluer ces risques de dépendance avec attention. Le point n°17 insiste sur le fait que la 5G devra respecter les valeurs fondamentales de l'UE (droits humains et libertés fondamentales, État de droit, protection de la vie privée, les données personnelles et de la propriété intellectuelle, l'engagement à la transparence, à la fiabilité et à l'inclusion de tous les citoyens et de toutes les parties prenantes, ainsi que la coopération internationale renforcée). Toutefois, aucune réserve n'est émise quant à l'impact écologique de cette course au haut débit dont personne n'a pu prouver qu'elle était indispensable à la survie de l'Humanité sur une planète dont les technologies numériques bouleversent le climat. S'est-on même demandé si la 5G était utile[4] ? Sur ces réflexions fondamentales, il y a une faille, une vulnérabilité qui doit faire l'objet d'une mise à jour politique et citoyenne.



DE LA 5G AUX DÉBATS SUR LE HACK-BACK, DES INITIATIVES EUROPÉENNES AUX NÉGOCIATIONS AU SEIN DE L'ONU : QUELS ENJEUX POUR LA RÉGULATION DE LA CYBERSÉCURITÉ EN 2020 ?

Karine BANNELIER



La loi du 1er août 2020 sur l'exploitation des réseaux radioélectriques mobiles comme les récentes conclusions du Conseil de l'UE du 3 décembre (significance of 5G to the European Economy and the need to mitigate security risks linked to 5G) montrent la nécessité d'une adaptation du cadre légal pour répondre aux défis sécuritaires de la 5G. Ces évolutions technologiques combinées au contexte international pourraient préfigurer un changement de paradigme dans la gouvernance de la cyber-sécurité, la prévention et la réaction aux cyber-attaques, domaines auxquels je consacre mes recherches au sein du Grenoble Cybersecurity Institute[1].

Gouvernance de la cybersécurité

L'échec des négociations sur la cyber-sécurité au sein de l'ONU en 2017 a créé un grand vide et montré les limites d'une approche exclusivement interétatique. Dans plusieurs articles[2], nous avançons l'idée de créer un organe multi-acteur de coopération réunissant les Etats, le secteur privé et la société civile. Cet organe, le Global Forum on Digital Security for Prosperity a vu le jour au sein de l'OCDE en 2018 et l'Appel de Paris confirme la nécessité d'une telle approche et le rôle majeur des acteurs privés en matière de cyber-sécurité. La récente reprise des négociations à l'ONU est certes une bonne nouvelle mais elle présente aussi des risques de

fragmentation. C'est en effet désormais au sein de deux instances distinctes que ces négociations sont menées : un groupe restreint soutenu par les pays occidentaux et un groupe à composition non limitée soutenu par la Russie et la Chine. Cette dualité qui s'explique par les désaccords entre les Etats sur l'application et l'interprétation dans le cyberespace des grands principes du droit international (contre-mesures ; légitime défense ; souveraineté ; droit des conflits armés, etc.)[3] pourrait rapidement bloquer toute évolution juridique voire affaiblir les règles existantes. La récente décision de l'ONU (initiative russe) d'engager des négociations sur une convention internationale sur la cybercriminalité concurrente de la convention de Budapest est à cet égard un motif de préoccupation. Comme je le montre par ailleurs[4], le Manuel de Tallinn 2.0 qui *« codifie »* 154 règles du droit international applicables aux cyber-opérations contribue lui aussi à cette fragmentation en faisant prévaloir une lecture anglo-saxonne du droit qui n'est pas nécessairement toujours en phase avec le droit positif ni avec les conceptions et intérêts français.

Prévention des cyberattaques et cyber-diligence

Le développement de cyber-attaques relevant d'acteurs privés est souvent associé à l'idée selon laquelle les Etats n'assument à leur égard aucune responsabilité. Dans plusieurs articles j'ai démontré que cette idée est fausse. En vertu du principe de due diligence/cyber-diligence[5], les Etats ont une obligation (de moyens) de prévenir et faire cesser les cyber-attaques lancées depuis leurs infrastructures. J'ai aussi essayé d'analyser les obligations des Etats dans ce domaine, notamment en termes de protection des infrastructures critiques, de certification, de divulgation des vulnérabilités ou encore de lutte contre la prolifération d'outils malveillants. Récemment, j'ai ainsi montré comment la gendarmerie nationale dans l'affaire *« Retadup »* a assumé ses responsabilités en neutralisant un centre de contrôle et commande qui était à la tête d'un gigantesque botnet[6].

Réactions aux cyberattaques et attributions

Dans l'ouvrage *« Cyber-attaques »*[7], nous proposons une classification des réactions admissibles aux cyber-attaques allant des mesures de rétorsion à la légitime défense en passant par les contre-mesures et les mesures de self-help. Cette analyse m'a aussi conduit à travailler sur les enjeux de l'attribution et plus récemment sur les 'cyber-sanctions' que l'UE souhaite adopter[8].

Hack-Back

Plusieurs de nos publications[9] analysent les mesures de cyberdéfense active et de hack-back *(« fait pour un acteur privé de mener des actions cyber offensives en réponse à une attaque dont il serait victime »)* développées par le secteur privé. Nous montrons notamment les risques du hack-back *« sauvage »* (à savoir des ripostes unilatérales du secteur privé sans l'accord ou le contrôle d'un Etat) tout en proposant des pistes pour le développement d'un hack-back *« sage »* mené en concertation avec les pouvoirs publics.

1. https://cybersecurity.univ-grenoble-alpes.fr
2. https://www.ejiltalk.org/reinventing-multilateral-cybersecurity-negotiation-after-the-failure-of-the-un-gge-and-wannacry-the-oecd-solution/
3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2656226
4. http://hal.univ-grenoble-alpes.fr/hal-02055582
5. http://rbdi.bruylant.be/public/modele/rbdi/content/TAP-KarineBANNELIER.PDF
6. A paraître : https://cyberlaw.ccdcoe.org/wiki/Main_Page
7. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941988
8. https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf
9. https://www.cairn.info/revue-strategique-2017-4-page-99.htm#

CONVENTION DE BUDAPEST ET CYBER-CRIMINALITÉ

Nadir OUCHENE

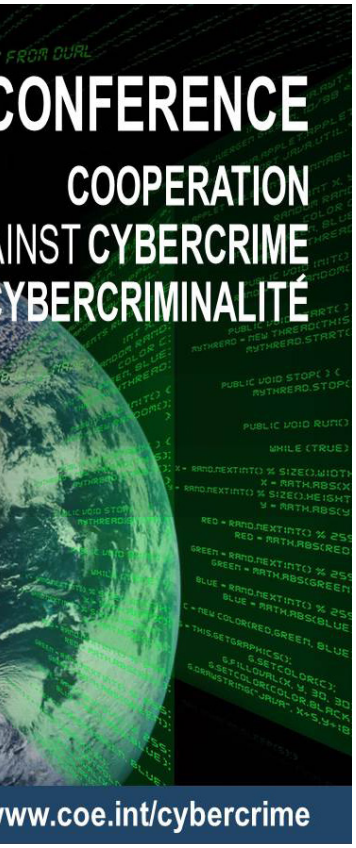


Si la cybercriminalité est un concept difficile à cerner, qu'en est-il, dès lors, de l'harmonisation des lois l'encadrant ? En la matière, la Convention de Budapest, entérinant une véritable coopération internationale, a entrepris de relever ce défi des plus ardus. À travers 48 articles, elle vise en effet *« à harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes, à fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction (...), et à mettre en place un régime rapide et efficace de coopération internationale ».*

Œuvre du Conseil de l'Europe et signée à Budapest en novembre 2001, transposée en France par la loi n°2005-493 du 19 mai 2005 parue au JO n°116 du 20 mai 2005, il s'agit de la première convention pénale destinée à lutter contre le cybercrime. En ce sens, elle aborde les infractions informatiques afin de coordonner certaines lois nationales, d'améliorer les techniques d'enquêtes et d'augmenter la coopération entre les nations. Ainsi, dans un souci de conciliation et de modernisation des règles relatives à la cybercriminalité, cette convention rallie vingt-six membres du Conseil de l'Europe sur quarante-trois ainsi que l'Afrique du Sud, le Canada, le Japon et les États-Unis ; soit trente pays au total.

La cybercriminalité relève du droit pénal des nations de sorte qu'il en existe autant de définitions que de pays. Certes, le droit interne français l'évoque mais sans en offrir toutefois de définition arrêtée.

En réalité, le concept de cybercriminalité est cerné de manière indirecte par le contenu de conventions internationales qui sont dans l'incapacité d'avoir une portée générale. Dès lors, l'objectif de la Convention de Budapest est de définir les notions techniques fondamentales pouvant faire l'objet de plusieurs approches.



À titre d'exemple, le substantif *« informatique »* est devenu un terme polysémique visant aussi bien le domaine industriel, en rapport avec l'ordinateur, que la science du traitement des informations par des algorithmes. Or, selon la convention, l'expression de *« système informatique »* désigne *« tout dispositif interconnecté ou apparenté, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données »*. Ainsi, c'est la partie informatique du système d'information qui est visée. Elle est constituée de matériels, logiciels, réseaux et procédures d'utilisation qui permettent le traitement automatique de l'information. Agréées par les États membres, ces définitions facilitent la mise en place d'un cadre juridique minimal nécessaire en matière de cybercriminalité afin d'éviter les zones de non droit.

S'agissant de la coopération policière, la Convention de Budapest préconise une coopération entre les États signataires qui pourront être amenés à utiliser des moyens coercitifs sur leur propre territoire, pour les besoins d'un autre État, s'ils concernent une infraction visée dans la Convention. Elle aspire à une meilleure efficacité pour les enquêtes et procédures pénales d'infractions en lien avec les données et systèmes informatiques en *« tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclu entre les États membres du Conseil de l'Europe et d'autres États »*. En outre, l'article 35 de la Convention de Budapest prévoit la mise en place d'un *« point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept »*, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme electronique d'une infraction pénale. Les échanges d'informations entre représentants des différentes polices ont ainsi été développés par Interpol tandis qu'Europol traite les différentes bases d'informations pour assurer une meilleure coordination des actions policières. En France, ce point de contact joignable en permanence est l'Office central de lutte contre la criminalité liée aux techniques de l'information et de la communication, créé le 15 mai 2000. Il est chargé d'apporter des conseils techniques, de conserver des données, de recueillir des preuves et de localiser les suspects.

À ce jour, la Convention de Budapest est donc la principale arme employée par l'Europe pour lutter contre la cybercriminalité. Bien qu'il s'agisse indéniablement d'une progression notable dans le traitement de la cybercriminalité, les limites de cette lutte sont encore trop nombreuses, comme en atteste notamment l'absence de prise en compte du Darknet.



UN CYBERSPACE EUROPÉEN ÉTHIQUE ET RESILIENT

Anne CAMMILLERI

L'avenir du cyberespace résilient sera celui qui s'appuiera sur les nouvelles technologies et notamment l'intelligence artificielle (IA). Il sera au service des valeurs portées par les Etats membres de l'Union européenne, à savoir valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'état de droit, ainsi que le respect des droits de l'Homme.

L'Union européenne ambitionne le développement d'une IA de confiance au sein du cyberespace : elle sera licite et éthique. L'université d'Harvard promeut le maintien du contrôle humain sur la technologie, mais aussi l'émergence de règles de responsabilité, de transparence et d'explicabilité, de justice et de non-discrimination. Les chartes éthiques ont le mérite de donner un code de conduite souple à tous les utilisateurs industriels ou chercheurs qui travaillent à améliorer notre société, tout en inscrivant l'ensemble des usages de l'IA dans le plein respect des droits fondamen-

taux. Le cyberersespace doit être porté par des valeurs humanistes. L'OCDE y promeut l'intelligence artificielle portée par *« des principes complémentaires fondés sur des valeurs : la croissance inclusive, le développement durable et le bien-être ; les valeurs centrées sur l'humain et équité ; la transparence et l'explicabilité ; la robustesse, la sûreté et la sécurité et la responsabilité »*. Le recours au codesign, la promotion de l'éthique dès la conception (ethics by design), la sécurité dès la conception (Security by design) sont indispensables pour forger un cyberespace sécurisé. De plus, l'Union européenne promeut le calcul de haute performance et tente de se placer *« à l'avant-garde du développement des technologies quantiques, en particulier l'informatique et les communications quantiques »*. Ce soutien au développement mathématique doit s'accompagner d'une politique d'éducation large afin de pouvoir susciter la confiance à l'égard de l'intelligence artificielle et de lutter contre l'illectronisme.

Depuis l'entrée en vigueur de l'Acte européen sur la Cybersécurité du 17 avril 2019, la cybersécurité au sein du marché intérieur est renforcée par l'émergence de nouvelles règles de certification et de normalisation qui restent des enjeux essentiels dans le cadre de la libre concurrence. Ces règles juridiques viennent consolider les règles éthiques promues au sein du cyberespace. L'acte européen sur la cybersécurité constitue un renfort au service de la sécurité juridique, car il permet de créer un climat de confiance technologique ! Sur le plan formel, l'acte européen est un règlement, ce qui le rend applicable directement dans le chef des particuliers et permet une uniformisation européenne bienvenue du droit de la cybersécurité. Mais l'effectivité de l'application des règles éthiques au sein du cyberespace n'a de sens que si cet espace est sécurisé. L'éthique promue par l'humain sans la sécurité dans le cyberespace est anéantie ! Les Britanniques l'ont très bien compris en promouvant une stratégie nationale tournée vers la sécurité, en invoquant le principe de *"SECURE by design"* dans leur programme *« Active cyber defence »* tout à fait en phase avec les ambitions européennes, malgré le lancinant BREXIT. Le pragmatisme britannique l'emporte avec un affichage clair d'anticipation technologique dès la conception. Les Américains ancrent la cybersécurité au cœur de leur politique de sécurité nationale.

Le comportement éthique dans l'usage des formes variées d'intelligence artificielle au sein du cyberespace n'est pas étranger à l'art de faire la guerre. Si l'art de la guerre est celui de la tactique, cette dernière n'interdit pas une éthique de la guerre dans les mesures appropriées prises par l'organisation internationale. Mais il est vrai qu'en cet endroit, l'art de faire la guerre face *"au danger d'escalade"* est en soi une éthique de la guerre... qui repose sur le droit des conflits armés, qui lui-même est soumis aux règles internationales de protection des droits de l'Homme ! L'éthique et le droit, même dans le cadre d'une stratégie internationale dans le cyberespace, sont unis de manière aussi définies que les frontières des Etats.

En fêtant ses 70 ans, l'Alliance atlantique prouvait son adaptabilité en réaffirmant que le cyberespace est *« le cinquième milieu d'opérations »,* au sein duquel l'organisation confirme sa volonté de mettre en œuvre la clause de défense collective, s'il y a lieu... ou en d'autres termes.... comment le droit l'emporte sur l'éthique.

APPROCHES CULTURELLES DE LA CYBERSÉCURITÉ

Anne-Thida NORODOM



L'observation des différents fora internationaux de négociation sur la cybersécurité montre que les parties en présence n'ont pas la même appréhension de la cybersécurité, ce qui constitue un obstacle majeur pour que les discussions puissent aboutir. Face aux deux approches opposées, l'Union européenne pourrait faire valoir une autre voie.

L'existence parallèle de deux fora sur la cybersécurité au sein de l'ONU illustre parfaitement l'opposition culturelle dans la conception qu'ont les Etats du cyberespace et de la cybersécurité. Alors que le GGE souhaite limiter les discussions à la sécurité dans la cyberespace et n'envisage pas de créer de nouvelles normes, partant du principe que le droit international existant s'applique (Résolution A/RES/73/266), l'OEWG adopte une vision plus large de ces questions en y incluant la manipulation de l'information et considère que si le droit international s'applique, il n'est sans doute pas suffisant et d'autres normes doivent être adoptées (Résolution A/RES/73/27). Les discussions sont rendues impossibles par l'existence de conceptions différentes de leur objet.

Si l'on simplifie, les Etats-Unis, et plus largement le bloc occidental, prônent un Internet libre et ouvert, tout en cherchant à assurer la sécurité dans le cyberespace. Ils bénéficient, à l'échelle mondiale, d'une supériorité technologique, économique et institutionnelle dans le cadre la gouvernance de l'internet, qui a été contestée lors des négociations du nouveau Règlement des télécommunications internationales au sein de l'Union internationale des télécommunications à Dubaï en 2012, puis s'est amplifiée avec l'affaire Snowden en 2013 et notamment dans le cadre du NetMundial de São Paulo de 2014.

Parallèlement la Russie a construit un Internet, qui se caractérise notamment par des opérateurs nationaux, une zone d'influence russophone et un espace de contrôle du contenu plus que de gestion des systèmes



d'échange des données (K. Limonier, Ru.net. Géopolitique du cyberespace russophone, 2018). La Chine, quant à elle, a élaboré son propre intranet et, tout comme la Russie, possède des opérateurs numériques nationaux. Aux yeux de ces deux Etats, le principe de souveraineté est par ailleurs primordial : pour la Chine parce qu'il autorise l'exercice d'une compétence pleine et exclusive de l'Etat sur son territoire, dont sa dimension numérique ; pour la Russie parce qu'il interdit toute ingérence extérieure. Ces deux Etats considèrent ainsi, pour des raisons différentes, qu'ils doivent pouvoir contrôler pleinement le cyberespace ou plutôt *« l'espace informationnel »* les concernant.

Face à ces approches diamétralement opposées, quelle peut-être la place de l'Union européenne et y a-t-il une approche européenne à défendre ? Un rapport d'information du Sénat français évoquait, en 2013, le risque que l'Union européenne devienne *« une colonie du monde numérique, à la fois parce qu'elle devient dépendante des puissances étrangères et parce qu[e] (...) le sous-développement la guette ».*

L'UE est pourtant en train de développer des éléments d'une politique numérique, par l'instauration de son marché unique numérique mais également par l'élaboration d'un droit ambitieux de protection des données à caractère personnel. Les questions de cybersécurité sont certes encore insuffisamment développées et les Etats membres de l'UE n'ont pas nécessairement tous la même conception de la cybersécurité. Pourtant il existe un début d'approche européenne de la cybersécurité.

L'UE a cependant une approche éparse et non homogène du numérique : développée dans le domaine économique interne et la protection des données, insuffisante en matière de recherche, balbutiante dans celui de la cybersécurité, ou en cours s'agissant de la manipulation de l'information pour ne prendre que ces quelques exemples. Son approche de la cybersécurité se fait par l'élaboration d'une politique de risques et plus particulièrement de risques industriels alors qu'elle devrait être conçue de manière plus globale pour être plus efficace. Même si l'UE doit encourager le développement d'une industrie du numérique, il lui appartient de convevoir une véritable politique transversale du numérique et non pas seulement de promouvoir le volet numérique des différentes politiques européennes existantes. Tout en continuant de développer les secteurs pauvres du numérique européen, elle doit s'appuyer sur ses atouts : sa dimension économique et sa vision protectrice des données. Pour ce faire le droit constitue un instrument incontournable, le RGPD en est un parfait exemple : il promeut un modèle européen de protection des données et conduit les acteurs étrangers à adapter leur législation en conséquence. Il faudrait maintenant que l'UE puisse adopter cette démarche, cohérente en interne et innovante vis-à-vis de l'extérieur, dans l'ensemble des domaines du numérique.



02

ACTEURS D'UNE EUROPE DE LA CYBERSÉCURITÉ

Anne LE HÉNANFF

LA FONDATION WOMEN4CYBER



Face à l'inquiétant constat que les ressources humaines et le nombre d'experts sont déjà aujourd'hui insuffisants dans le secteur de la cybersécurité et, prenant en compte la sous-représentation des femmes dans la filière en Europe, ECSO (European Cyber Security Organisation) a lancé le 22 janvier 2019 l'initiative Women4Cyber à Bruxelles, fortement soutenue par Mariya Gabriel, alors commissaire européenne en charge de la société et l'économie digitales. ECSO, ayant à son origine un contrat de partenariat public-privé sur la cybersécurité avec la Commission européenne, a pour mission de structurer un écosystème européen de cybersécurité en rassemblant en son sein différents types d'acteurs, y compris les administrations publiques nationales et régionales, les grosses entreprises, les PME, les universités et centres de recherche, etc. C'est dans la lignée de cette mission holistique qu'ECSO a créé Women4Cyber.

Membres fondatrices de l'initiative, 30 femmes d'Europe de haut niveau des secteurs public, privé, académique ou associatif, ont été invitées à accompagner la structure avec l'ambition de proposer plusieurs actions communes ou individuelles au niveau européen, ainsi que et surtout dans leur propres pays :

- rassembler et fédérer les énergies dans chaque pays mais également au niveau du territoire européen pour valoriser la filière cybersécurité

Toutes les informations sont disponibles sur le site d'ECSO https://ecs-org.eu/working-groups/news/women4cyber. Women4Cyber est également présente sur les médias sociaux.

- trouver les actions pertinentes pour donner l'envie aux jeunes filles et aux femmes de s'engager professionnellement dans la filière trop souvent perçue comme masculine et peu attractive
- adapter des actions dans chaque pays membre en complémentarité des mesures déjà engagées par les écosystèmes nationaux
- relayer les actions de Women4Cyber dans chaque pays par des opérations de communication et de participation à des événements dédiés (FIC, etc.)
- nouer des partenariats avec les universités, les écoles, les cabinets de recrutement et tous acteurs du secteur pour faire évoluer les pratiques et adapter les techniques
- faire des recommandations et des propositions stratégiques à la structure de gestion de la fondation pour mener des actions pertinentes et agiles
- valoriser dans chaque État et en Europe les *« success stories »* professionnelles de femmes ayant réussi dans le domaine de la cybersécurité

Aujourd'hui, Women4Cyber est portée par une structure légale officielle, la fondation Women4Cyber Mari Kert-Saint Aubyn qui est régie par un plan d'actions et une charte comprenant des objectifs stratégiques tels que l'accompagnement de l'environnement éducatif, la bonne connaissance du marché de l'emploi mais également l'intégration dans les réseaux et les communautés existantes.
La fondation comprend en son sein le Women4Cyber Council, un organe ad hoc de discussion qui fournit les recommandations stratégiques nécessaires à la fondation. Toutes les membres fondatrices de l'initiative ont été invitées à faire partie du Conseil qui a été lancé le 23 septembre dernier à Rome à l'occasion de sa première réunion. Luigi Rebuffi, secrétaire général d'ECSO, se voit également faire partie de l'organe d'administration de la fondation et est membre du Conseil.

La fondation Women4Cyber Mari Kert-Saint Aubyn est prête à mener toutes les actions opérationnelles lui permettant d'atteindre son objectif et faire de l'Europe un espace motivant et ambitieux pour les femmes de la cyber. A cet effet, il lui est impératif de profiter du soutien de la communauté, que ce soit au niveau de la promotion ou au travers de donations qui permettront la mise en place d'actions concrètes.

Pour ses efforts, Women4Cyber s'est récemment vue décerner le *« 2019 Cyber Security Nordic Award »*, un prix destiné à augmenter la visibilité et l'importance de la cybersécurité au niveau international à travers la promotion de la cyber expertise et de cyber experts.

AI-REGULATION.COM UNE CHAIRE SUR LA RÉGULATION DE L'INTELLIGENCE ARTIFICIELLE

Théodore CHRISTAKIS

Karine BANNELIER



Cent jours pour réguler l'intelligence artificielle (IA). Rien de moins ! C'est pourtant l'objectif que s'est fixée la nouvelle Présidente de la Commission Européenne Ursula von der Leyen : *« Au cours de mes 100 premiers jours au pouvoir, je proposerai une législation pour une approche sur les implications humaines et éthiques de l'intelligence artificielle »* a-t-elle déclarée. Le compte à rebours a commencé le 2 décembre 2019. Tic-tac, tic-tac... l'horloge tourne et à Bruxelles c'est un peu la panique.

Réguler l'IA en 100 jours ? Pourquoi ne pas réguler l'électricité ? L'IA n'est pas un bloc monolithique à réguler de façon isolée et rapide. Elle connait des champs d'applications variés et des utilisations diverses par des acteurs bien différents. Personne à Bruxelles ne croit d'ailleurs pouvoir trouver d'ici le 11 mars 2020 la formule magique qui permettra de *« tout réguler »* d'un coup de baguette.

Il est plus probable que la Commission ne propose que quelques grands principes pour *« prendre date »*. L'Europe n'a-t-elle pas déjà montré le chemin dans d'autres domaines, surtout en matière de protection des données et de vie privée ? Le 11 mars 2020 pourrait en réalité n'être que le début d'un gigantesque chantier qui permettra de développer progressivement des règles et apporter les protections nécessaires sans pour autant freiner l'innovation.

Inutile de le dire, la régulation de l'IA est le sujet du moment. Au-delà même de l'Europe, de nombreuses voix appellent à l'adoption de règles juridiques contraignantes.

C'est pour accompagner ces évolutions que nous avons créé la Chaire sur la Régulation de l'IA, au sein de l'Institut MIAI Grenoble Alpes (Multidisciplinary Institute in Artificial Intelligence) sélectionné par un jury international dans le cadre du programme national pour l'intelligence artificielle lancé par le Président de la République. La Chaire est heureuse de bénéficier de plusieurs partenariats, dont surtout Microsoft et Skopai.

La Chaire trouvera son incarnation dans son site internet : <*ai-regulation.com*> qui sera lancé dans le courant du mois de janvier. Ce site publiera des articles, études et dépêches sur : l'in-

terprétation des règles existantes dans le domaine de l'intelligence artificielle ; les initiatives politiques, législatives et réglementaires en matière de IA ; les décisions de justice... et ceci dans une perspective nationale, comparée, européenne et internationale organisée autour de 8 thèmes.

Gouvernance et réglementation de l'IA
Cet axe transversal permet d'analyser la pertinence du droit existant en matière d'IA (par ex. le RGPD) et à quoi ressemblera la gouvernance de l'IA demain. Les questions vont de la protection des données, de la vie privée et d'autres droits humains à celles de transparence, d'auditabilité des systèmes d'IA, de responsabilité/accountability/liability et de contrôle, en passant par la lutte contre les biais et les discriminations.

Reconnaissance faciale
Les techniques de reconnaissance faciale peuvent être déployées tant dans la sphère privée que publique pour y assurer des fonctions multiples : authentification, identification, surveillance, reconnaissance émotionnelle... Elles impliquent des traitements de données biométriques particulièrement sensibles. Comment interpréter les règles existantes pour atténuer les risques pour nos libertés ? Quelles nouvelles règles mettre en place ?

Agents conversationnels et chatbots
Alexa, Siri, Cortana, chatbots... La montée en puissance des assistants numériques transforme profondément notre environnement. Cet axe propose d'étudier ces technologies qui s'introduisent dans notre intimité afin d'en identifier les enjeux juridiques : biais technologiques, cybersécurité, libertés publiques, contrats etc.

Villes intelligentes, maisons intelligentes, objets connectés
Le développement des objets connectés pousse d'aucuns à parler de maisons ou villes *« intelligentes »*. Si ces objets permettent d'envisager une gestion plus raisonnable et adaptée de nos ressources et infrastructures, les enjeux en matière de vie privée, de protection des données, de propriété intellectuelle ou encore de sécurité sont cruciaux. Comment favoriser une utilisation responsable des IoT ?

Manipulation des données, IA et démocratie
Des deepfakes aux ingérences dans les processus électoraux cet axe vise à analyser comment l'IA peut manipuler l'humain et à développer le concept de *« sécurité cognitive »*.

Santé, humains et IA
Demain l'IA nous soignera et arrivera peut-être même à assouvir nos désirs les plus intimes. Mais nos données de santé sont particulièrement sensibles.... La protection de ces données et la façon dont l'IA les utilise devient un enjeu vital de société tout comme le transhumanisme.

Véhicules connectés et autonomes
Bientôt nous ne serons que les hôtes de nos véhicules. Ils seront en capacité de gérer mieux que nous conduite, trajet et...trajectoires. Alors qui dit voiture connectée dit aussi nouveaux enjeux de responsabilité, données personnelles collectées et quid d'une voiture hackée ?

IA, sécurité nationale et internationale
L'IA est désormais au cœur des enjeux de sécurité nationale. Conscients des implications révolutionnaires de l'IA pour leur sécurité et leur défense, certains pays cherchent activement à développer et améliorer l'usage de l'IA pour une gamme très étendue d'applications allant du renseignement aux armes létales autonomes (*« robots-tueurs »*). Ces activités agitent le spectre d'une course aux armements IA et soulèvent de redoutables questions juridiques.





03

ZOOM SUR LE FIC 2020 : L'HUMAIN AU CŒUR DE L'EUROPE DE LA CYBERSÉCURITÉ

TECHNOLOGIES DE RECONNAISSANCE FACIALE : ENCORE TROP DE MÉCONNAISSANCE DU SUJET DANS L'UE

Michel SÉJEAN

« ***Ensemble, on protège mieux »***, écrit l'Union européenne (UE) sur son site[1]. L'on y trouve des vidéos promotionnelles fort bien réalisées sur la sécurité aérienne, la lutte contre la radicalisation, le rôle de l'UE dans le démantèlement de trafic d'êtres humains ou encore l'importance des patrouilles maritimes aux frontières de l'UE : autant de sujets dont le traitement pourrait changer avec les technologies de reconnaissance faciale. Mais l'opinion publique n'est pas encore suffisamment informée sur ces technologies pour que l'UE valorise les protections qu'elle a mises en place : il y a encore trop de méconnaissance sur les enjeux européens de la reconnaissance faciale.

Un excellent rapport rédigé par l'Agence des droits fondamentaux de l'Union européenne pourrait dissiper les fantasmes sur cette question déterminante de l'avenir de nos démocraties. Intitulé *« Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le cadre du maintien de l'ordre »* (disponible en langue anglaise seulement) et publié à la fin du mois de novembre 2019, ce rapport dresse un tableau exhaustif des dispositions du droit de l'UE qui protègent les données biométriques, ainsi que les enjeux de protection des droits fondamentaux.

Ce texte doit être rapproché de celui que la CNIL française a publié quelques semaines auparavant, et dont la qualité est, là encore, remarquable de pédagogie, de précision et de lucidité[2].

Dès 2012, un groupe de travail sur la protection des données proposait une définition des technologies de reconnaissance faciale émettant l'Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles sous le titre : *« la reconnaissance faciale est le traitement automatique d'images numériques qui contiennent le visage de personnes à des fins d'identification, d'authentification / de vérification ou de catégorisation de ces personnes »*[3]. Si le rapport de la



CNIL reprend les deux premières fonctions de la reconnaissance faciale, celui de l'agence des droits fondamentaux analyse les trois finalités possibles de ces technologies pour les distinguer les unes des autres.

S'authentifier par reconnaissance faciale, c'est démontrer que l'on est la personne que l'on prétend être. Cette démonstration s'opère par la comparaison d'une image avec une seule autre image. La première image est un gabarit préconstitué, stocké par exemple dans la puce de son passeport. La seconde est un gabarit tiré d'une photographie prise au cours du processus d'authentification. C'est ainsi que l'on déverrouille son téléphone, ou que l'on franchit les portiques frontaliers du système PARAFE. Ici, l'utilisateur est acteur de sa propre reconnaissance faciale : il y consent, et c'est ce qui atténue grandement la dangerosité des technologies d'authentification.

Identifier un individu par la reconnaissance faciale, c'est retrouver son identité par la comparaison entre une image et plusieurs autres images stockées sur une banque d'images préexistante. La vidéosurveillance dans des lieux publics illustre cette fonction d'identification. Or, à cette occasion, les personnes identifiées ne sont pas informées qu'elles font l'objet d'un traitement, car la technologie de reconnaissance est *« sans contact »*. L'absence de consentement, mais aussi la mauvaise qualité des images obtenues à la volée dans des conditions techniques et graphiques défavorables à la fiabilité, imposent un encadrement très strict – voire une interdiction de principe.

Enfin, catégoriser les individus ne consiste pas à les identifier, mais à extraire des informations permettant de les classer, d'établir leurs profils en fonction de leur genre, de leur âge ou de leurs origines ethniques. De manière plus subtile, il s'agit de détecter les émotions que trahissent les visages, notamment afin de déterminer si une personne dit la vérité. Ce dispositif a été utilisé en Grèce, en Hongrie et en Lettonie, dans le cadre du projet iBorderCtrl[4].
L'Union européenne et ses États-Membres sont confrontés à un choix : veulent-ils d'une liberté surveillée à l'américaine, d'une sécurité surveillée à la chinoise ou à la russe, ou sont-ils désireux de promouvoir une liberté sécurisée, selon la distinction opérée par le Général Watin-Augouard ? Il n'y aura pas de liberté sécurisée sans discernement : il nous faut continuer d'affiner nos connaissances sur la reconnaissance faciale.

1. https://europa.eu/euprotects/content/homepage_fr
2. Reconnaissance faciale : pour un débat à la hauteur des enjeux, en libre accès sur le site de la CNIL, oct. 2019
3. 00727/12/FR WP 192, 22 mars 2012, p. 2
4. (v. J. Grelier, *« Aux portes de l'Europe, on filtre les mensonges »*, Libération, 21 août 2019

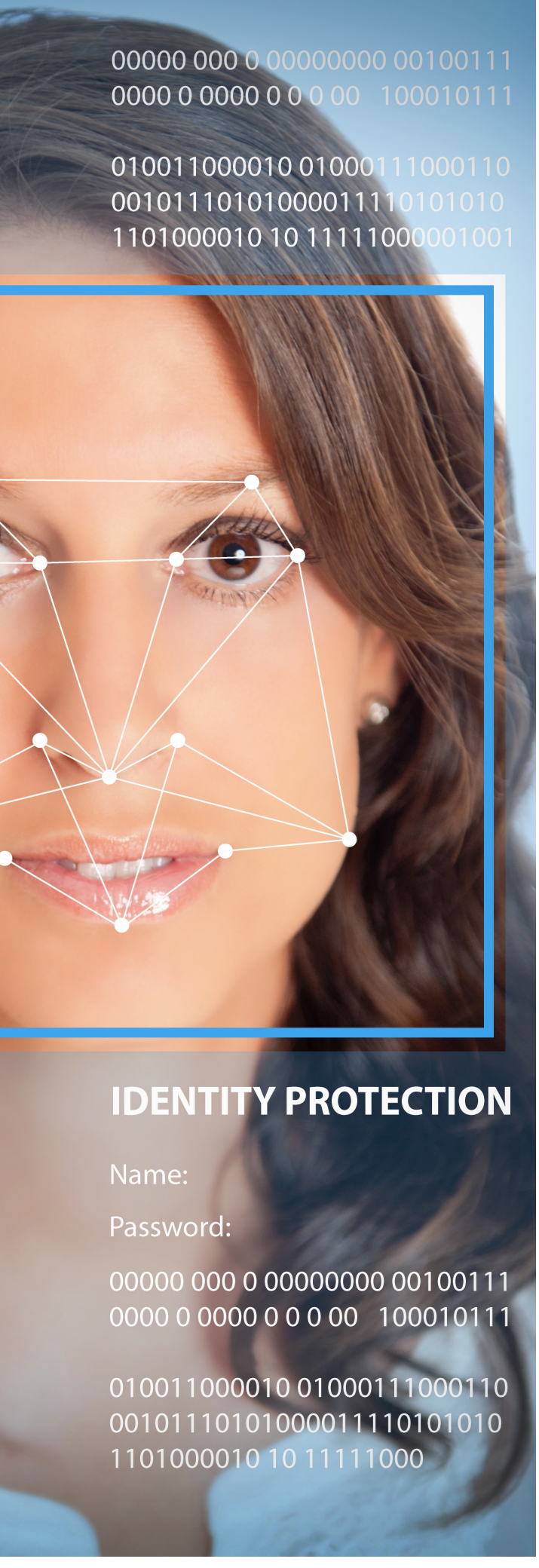
IDENTITÉ NUMÉRIQUE ET CYBERSÉCURITÉ





Par Chloé HERVOCHON et Thibault DOUVILLE

L'identité d'une personne physique est ce qui la distingue d'une autre et regroupe l'ensemble des éléments permettant de l'identifier. Dans l'univers numérique, elle peut être envisagée à travers deux fonctions. Une fonction probatoire, à travers l'identification (processus consistant pour une personne à dire qui elle est) et l'authentification (processus permettant de confirmer l'identité déclarée) et une fonction de protection, à travers le régime applicable au traitement des données à caractère personnel. Dans les deux cas, les enjeux de cybersécurité sont importants car les risques sont protéiformes dans leur objet (usurpation d'identité, fraudes, soustraction, divulgation ou destruction de données à caractère personnel...), dans leur nature (intentionnelle ou non) et dans leurs conséquences : psychologiques (confiance), juridiques (sécurité des transactions), économiques (dommages) ou techniques (types d'attaques, mesures de prévention...). La réponse du législateur européen (pour l'essentiel) repose sur une logique de précaution. Cette logique se retrouve notamment en matière d'identification électronique et de services de confiance (signature électronique ou cachet électronique) dont le règlement eIDAS constitue la colonne vertebrale (Règlement (UE) n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur) ou en matière de données à caractère personnel (Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel). Ainsi, les responsable du traitement, les sous-traitants mais aussi les prestataires de services de confiance doivent prendre les mesures techniques et organisationnelles adéquates afin de garantir un niveau de sécurité adapté au risque. Une identi-



fication des risques doit donc intervenir afin de procéder à leur évaluation et à la mise en place de mesures pour les détecter, les gérer et assurer la résilience des systèmes d'information et des données. La responsabilité des différents acteurs de l'identité numérique en dépend. S'ajoute à cela, en cas d'atteinte de sécurité, des exigences de notification auprès des autorités de contrôle compétentes (CNIL et ANSSI en France) et, le cas échéant, d'information des personnes intéressées.

À l'échelle européenne, la question de la cybersécurité se pose avec acuité à propos des schémas d'identification électronique que les États européens sont incités à mettre en place à la suite du règlement eIDAS. Ils peuvent en effet, à certaines conditions, notifier à la Commission européenne un schéma d'identification électronique. Ces schémas, et les moyens d'identification électronique qui leurs sont associés, ont pour but de permettre aux citoyens européens de s'identifier et de s'authentifier en ligne. Les niveaux de garantie substantiels et élevés entraînent la reconnaissance mutuelle des moyens d'identification électronique entre les États membres pour les services en ligne proposés par les organismes du secteur public. Pour cela, les schémas sont intéropérables. Les défis posés par un tel système en matière de cybersécurité sont nombreux. Si la fiabilité de l'authentification transfrontalière est remise en cause, le schéma doit être suspendu (un délai de trois mois est laissé) ou révoqué. Non sans paradoxe, l'importance des risques sécuritaires dépend des solutions retenues pour l'identification électronique (reconnaissance faciale par exemple), la recherche de confiance peut à certains égards être source de cyber-risques...

CONFIDENTIALITÉ NUMÉRIQUE : POUR UN CHIFFREMENT SANS PORTE DÉROBÉE DES DONNÉES TRAITÉES PAR LES CONFIDENTS

Émilie POUFFIER-THOMPSON et
Michel SÉJEAN





L'Union Européenne au soutien du chiffrement

Le RGPD a instauré des dispositions qui encouragent le chiffrement de bout en bout au lieu d'en réprimer l'utilisation[1]. Souhaitons que cet élan aille jusqu'à interdire aux États membres de forcer les fournisseurs de solutions de chiffrement à l'insertion de portes dérobées au sein de ces outils. La jurisprudence de la Cour de Justice de l'Union Européenne laisse espérer cette évolution, si l'on considère que la CJUE est défavorable aux moyens de contrôle des conversations privées des individus. Bien que la Cour ne se soit pas exprimée sur le chiffrement, elle s'est prononcée de manière remarquée sur les échanges privés, en invalidant la directive 2006/24/CE du 15 mars 2006 sur la conservation des données des services de communications électroniques[2]. Dans cette affaire, la Cour avait jugé que ce texte contrevenait tant au droit à la vie privée qu'au droit à la protection des données personnelles. En effet, la directive invalidée permettait aux États membres de contraindre les fournisseurs de services de communications électroniques à conserver systématiquement certaines données relatives aux échanges de leurs clients et surtout, à permettre aux autorités d'y accéder. Ce genre de mesure n'est-il pas assimilable à une disposition qui autoriserait les autorités à contraindre les fournisseurs de solutions de chiffrement à y introduire des portes dérobées ? L'analogie est permise : à moins

qu'elle ne modifie radicalement sa position, la Cour devrait continuer à préserver et sécuriser la liberté de ses ressortissants. S'en réjouiront les responsables de traitement qui traitent des données confidentielles, et en particulier les professionnels qui détiennent des informations confidentielles que leur confient un client ou un patient, en un mot : les confidents. Débarrassé des portes dérobées, le chiffrement de bout en bout demeure à ce jour la solution idoine qui protège les échanges d'informations intimes entre un client ou un patient et le professionnel à qui ils se confient.

Au-delà de la vie privée : l'intimité

Qu'ils soient avocats ou médecins, les professionnels tenus au secret sont les confidents des individus dont ils traitent les données intimes. Parce que ce secret touche à l'intimité de la personne et à ses droits fondamentaux, il mérite une protection absolue, qui dépasse encore celle du secret des affaires. Mais qu'est-ce que l'intimité ? Cette notion est un concept qui va au-delà de celui de la vie privée. En témoigne le législateur français lorsqu'il emploie l'expression *« intimité de la vie privée »*[3]. dont on comprend que l'intimité est une abstraction qui se loge au sein de la vie privée, mais qui est plus sacrée que son hôte. Est-il pour autant utile de rechercher les signes de cette dissociation entre intimité et vie privée ? Certainement, car à notre avis elle justifie le recours au chiffrement de bout en bout pour les échanges d'informations intimes, et permet d'écarter la suspicion dont le chiffrement fait l'objet. En d'autres termes, le recours à des moyens techniques permettant d'assurer la confidentialité dans la relation particulière unissant le confié et le confident est essentiel et ne saurait être bridé.

1. articles 6, 32 et 34, et considérant 83 du préambule
2. CJUE, gr. ch., 8 avr. 2014, aff. C-293/12 et aff. C-594/12, Digital Rights Ireland
3. V. entre autres C. civ., art. 9 ; C. pén., art. 226-1

Le chiffrement, allié de la confidentialité

Les portes dérobées qui s'ouvrent sur les conversations chiffrées sont particulièrement néfastes pour les individus. En ce sens, le considérant 75 en préambule du RGPD attire l'attention sur les *« risques pour les droits et libertés des personnes physiques »* qu'entraînerait une *« perte de confidentialité des données protégées par le secret professionnel »*. Toute autant cruciale que les droits et libertés des individus, c'est l'efficacité de la médecine et de la justice qui serait affectée par une trop faible sécurisation des données traitées par les professionnels tenus au secret. Comment, en effet, soigner un patient lorsqu'on ne peut être certain que la confidentialité de ses données est assurée par son médecin ? Et comment un justiciable peut-il se croire défendu s'il ne peut se confier sans crainte à son avocat ? Pour ces raisons, les professionnels tenus au secret doivent recourir à un contrefort technique au moins aussi infaillible que leur devoir, une muraille sans porte dérobée.



CHIFFREMENT ET CONFIANCE EN LIGNE

Emmanuel NETTER



À l'occasion d'un discours le 10 avril 2019, M. Emmanuel Macron, alors candidat à la Présidence de la République, déclarait : *« les organisations qui nous menacent abusent des facilités offertes par la cryptologie moderne pour dissimuler leur projet. Ils utilisent des messageries instantanées fortement cryptées pour prendre des contacts, donner des ordres. Une grande partie de ce trafic Internet, parce qu'il est crypté, échappe ainsi aux services de sécurité »*[1]. Il rejoignait ainsi les positions exprimées par M. Cazeneuve[2], alors ministre de l'Intérieur, ou M. Molins, alors procureur de la République de Paris[3].

Il est ainsi donné un large écho aux usages nuisibles du chiffrement. La place réservée, dans les médias destinés au grand public, aux utilisations légitimes de ces techniques paraît bien plus discrète, alors même qu'elles sont bien plus significatives, tant du point de vue quantitatif que qualitatif.

Une des fonctions de la cryptographie est de soustraire des informations à la curiosité humaine. Elle est très ancienne, comme en témoigne la dénomination de la plus fruste des techniques, *« le chiffre de César »,* qui consiste simplement à décaler les lettres constitutives d'un message d'un certain nombre de rangs dans l'alphabet. Ainsi l'ordre envoyé par le général à son armée, s'il était intercepté, restait-il inintelligible à l'ennemi. Cette fonction de préservation du secret persiste évidemment de nos jours, qu'il s'agisse de protéger les informations stockées sur un support ou un flux de communication (voix sur IP, emails, messagerie instantanée, etc.). Elle est particulièrement cruciale s'agissant de professions



astreintes par nature à la confidentialité[4], et bien au-delà : il est notoire que le président de la République, en dépit de ses réserves précédemment rappelées, utilise des messageries chiffrées de bout-en-bout pour communiquer avec son entourage politique et privé. Au vrai, n'importe quel citoyen, quel que soit son statut ou son importance supposée, a le droit au secret des correspondances et au respect de sa vie privée, dont le droit au chiffrement n'est qu'un simple corollaire, s'agissant des activités en ligne.

Mais toutes les données chiffrées qui transitent sur internet, une fois mises au clair, ne dévoileraient pas une information destinée à l'intelligence humaine : un ordre de mouvoir les troupes, un secret industriel, une lettre anodine ou un mot d'amour. La cryptographie vient également au secours des machines qui parlent aux machines. Sur internet, il est impossible de savoir à qui vous avez affaire sans recourir au chiffrement dans sa fonction d'authentification. Soit un internaute qui souhaite connaître le solde de son compte courant grâce au service en ligne proposé par sa banque. Il tape, par exemple, l'URL https://particuliers.societegenerale.fr dans la barre d'adresse de son navigateur. Aussitôt, un serveur DNS est interrogé. Ce système a notamment vocation à faire correspondre aux URL en toutes lettres l'adresse IP du serveur qu'il convient d'interroger. Comment s'assurer qu'un attaquant n'a pas pris le contrôle du serveur DNS, comment vérifier que l'information est légitime ? Les serveurs DNS *« racines »*, sous le contrôle de l'ICANN, attestent de l'intégrité des centaines de serveurs DNS locaux grâce au chiffrement. Une fois l'IP contactée, comment savoir s'il s'agit bien du site internet de la banque, et non d'une imitation qui aurait été placée sur le serveur après qu'on en a pris le contrôle ? Grâce à un certificat, chiffré. Comment permettre ensuite au client d'entrer ses identifiants et mots de passe sans qu'il soit interceptés par un attaquant qui écoute l'échange d'informations tout en le relayant (l'attaque *« de l'homme du milieu »*) ? Encore par le chiffrement.

Interdire ou affaiblir le chiffrement, c'est aussi compromettre tous ces usages : cet élément crucial du débat est parfois occulté. Il reste que le progrès technique, comme c'est souvent le cas, peut être placé au service de funestes projets. Mais la cryptographie rend-elle radicalement impossible la surveillance ou l'enquête pénale ? Une prochaine note abordera cette question.

1. M. Rees, *« Emmanuel Macron en Marche contre le terrorisme (et le chiffrement) »*, article nextinpact.com du 10 avril 2019

2. M. Untersinger, *« Terrorisme : pour contourner le chiffrement des messages, Bernard Cazeneuve en appelle à l'Europe »*, article lemonde.fr du 23 août 2016

3.Cyrus R. Vance Jr., François Molins, Adrian Leppard et Javier Zaragoza, *"When Phone Encryption Blocks Justice, tribune nytimes.com du 11 août 2015"*

4. Voir article page 26

DE MAGRITTE AU CLOUD ACT ET À E-EVIDENCE : QUELS RÉGIMES JURIDIQUES POUR L'ACCÈS À LA PREUVE NUMÉRIQUE ?



Théodore CHRISTAKIS

Vous souvenez-vous du tableau de Magritte *« L'Assassin menacé »* ? Un homme écoute de la musique dans une pièce où gît une femme nue décapitée. Tandis que deux policiers armés l'attendent dans l'entrée, trois autres à l'extérieur le guettent à travers une fenêtre. C'était le *« vieux monde »*, celui où les enquêtes criminelles étaient une affaire d'hommes et de femmes, celui où il suffisait aux hommes de loi de se déplacer sur les lieux pour trouver les preuves nécessaires à la résolution du crime.

Dans le monde digital d'aujourd'hui, se rendre sur les lieux pour confondre le criminel ne suffit souvent plus. Encore faut-il accéder à ses emails, réunir ses données de géolocalisation et autres métadonnées, dépouiller les messages postés sur les réseaux sociaux, vérifier les photos et les fichiers stockés sur le Cloud... Un rapport de la Commission Européenne de 2018 indique ainsi que les preuves électroniques sont essentielles dans 85% des enquêtes criminelles. Le problème est que souvent ces preuves sont stockées dans une juridiction différente : plus de la moitié des enquêtes criminelles implique une demande internationale d'accès à des preuves électroniques. La mondialisation des preuves criminelles représente un défi majeur pour les autorités policières et judiciaires. Les mécanismes transfrontaliers traditionnels comme les traités d'entraide judiciaire sont considérés comme trop lents et trop fastidieux. Les Etats essayent donc désormais de mettre en place des régimes juridiques pour obtenir les preuves électroniques directement par les fournisseurs de services Cloud.

L'adoption du CLOUD Act en mars 2018 ainsi que le projet *« E-Evidence »* présenté par la Commission Européenne en avril 2018 ont constitué le point de départ d'un gigantesque chantier juridique qui occupera sans doute les Etats pour les années à venir. Depuis 2017 une partie importante de mes recherches dans le cadre du Grenoble Alpes Data Institute et du

Cross Border Data Forum consiste à examiner les problèmes juridiques qui se posent dans ce domaine et à envisager des solutions pour les résoudre.

Une première série de mes articles concerne la question cruciale de l'extra-territorialité de certaines lois organisant l'accès direct à la preuve numérique. J'ai d'abord publié une étude[1] dans la fameuse affaire Microsoft Ireland qui a opposé Microsoft au gouvernement américain devant la Cour Suprême américaine. J'ai ensuite consacré plusieurs études à la question de la compatibilité du CLOUD Act avec le RGPD[2].

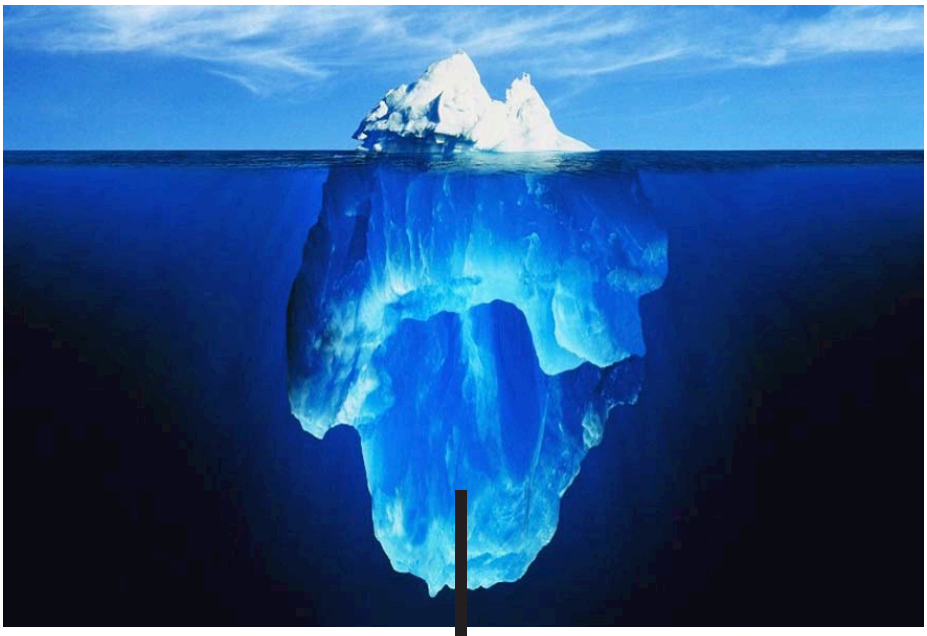
Une deuxième série de mes articles concerne le projet « E-Evidence » qui est un peu l'équivalent européen du CLOUD Act. J'ai avancé plusieurs propositions sur ce qui me semble être le juste équilibre entre les besoins des autorités de police et de justice d'accéder rapidement aux preuves numériques et les garanties nécessaires à la protection des droits de l'homme et des prérogatives souveraines des Etats. Si, j'ai critiqué la version de E-Evidence proposée par le Conseil de l'UE[3], je considère dans un article qui vient de paraître que la Rapporteur du Parlement Européen Birgit Sippel propose une approche plus satisfaisante dans son Rapport rendu en Novembre 2019[4].



Une troisième série de mes articles concerne les négociations internationales en cours pour conclure des accords internationaux dans ce domaine. J'ai publié, par exemple, une analyse du premier *« accord CLOUD Act »* conclu entre les Etats-Unis et le Royaume-Uni en octobre 2019, qui me semble problématique de plusieurs points de vue[5]. Je suis, par ailleurs, de très près les négociations entre l'Union Européenne et les États-Unis en essayant d'imaginer, avec mes collègues du Cross Border Data Forum, des solutions constructives pour pouvoir aboutir à un accord satisfaisant pour les deux parties. D'autres négociations internationales importantes sont en cours, y compris celles concernant l'adoption d'un Protocole additionnel à la Convention de Budapest sur la cybercriminalité qui portera précisément sur la question de l'accès à la preuve numérique.

Nous vivons des temps passionnants pour le développement de régimes internationaux d'accès à la preuve numérique. En maître, Magritte domptait les nuages ; dompter les preuves dans les nuages demandera sans doute encore plus de maestria, mais il faudra y parvenir d'une façon satisfaisante pour les droits de l'homme.

1. https://ssrn.com/abstract=3086820
2. https://ssrn.com/abstract=3397047 ou ici : https://www.dalloz-revues.fr/Revue_critique_de_droit_international_prive-cover-85228.htm
3. https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead
4. https://www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/.
5. https://ssrn.com/abstract=3469704



SOUVERAINETÉ, CYBERSÉCURITÉ ET UNION EUROPÉENNE

Anne-Thida NORODOM



La notion de *« souveraineté numérique »* a été popularisée par Pierre Bellanger avec la publication en 2014 de son ouvrage portant ce titre. Depuis, l'expression est utilisée partout, attribuée à n'importe quelle entité, pour désigner à peu près tout et n'importe quoi. Il importe de clarifier la notion de souveraineté si l'on veut que la notion soit opérationnelle, et justifier pour quelle raison il n'est juridiquement pas possible de parler de souveraineté numérique pour l'Union européenne.

En droit, la souveraineté est l'attribut exclusif de l'Etat. Il ne peut donc y avoir de souveraineté numérique des utilisateurs[1], ni des opérateurs de plateforme en ligne[2] ou encore de l'Union européenne[3]. L'utilisation d'autres termes pour désigner l'idée sous-jacente à celle de souveraineté devrait donc être favorisée lorsqu'il s'agit d'entités autres qu'étatiques.
Il y a plusieurs manières de définir la souveraineté en droit.

Il peut s'agir du *« plus haut degré de puissance et de liberté légales »*[4] ; la souveraineté peut désigner *« des compétences, des droits et des attributs juridiques au profit de son titulaire (...) un noyau dur de prérogatives qui seraient celles de l'Etat »*[5] ; on peut encore distinguer la souveraineté interne, qui s'apparenterait à l'exercice d'un pouvoir exclusif sur son territoire, de la souveraineté externe (ou s'exerçant dans l'ordre international), qui serait synonyme d'indépendance et de non subordination à une autre autorité.

Lorsque l'on parle de souveraineté de l'UE, l'expression est juridiquement erronée parce que l'UE n'est en aucun cas un Etat. Utiliser cette expression, c'est donc s'inscrire dans un débat sur la nature de l'UE qui dépasse de loin la question numérique. Pourtant l'idée sous-jacente d'autonomie stratégique de l'UE doit être défendue et elle peut l'être par le droit. Trois domaines permettraient d'assurer cette autonomie de l'UE dans le domaine du numérique et de la cybersécurité.

La protection des données des citoyens européens constitue un premier domaine d'autonomie stratégique. Le RGPD et sa portée extraterritoriale[6] ont conduit les autres Etats à adapter leur propre législation. La protection des données, conçues non pas dans une perception patrimoniale mais comme un attribut de l'individu, propose un véritable modèle européen voire un standard international.

1. Avis du Conseil économique, social et environnemental, Pour une politique de souveraineté européenne du numérique, 2019, p. 17

2. A. Blandin, « Les entreprises souveraines de l'Internet : un défi pour l'Europe », Droits et souveraineté numérique en Europe, 2016

3. Rapport de la mission d'information du Sénat, L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne, 2014, p. 26

4. J. Combacau et S. Sur, Droit international public, 2019

5. R. Rivier, Droit international public, 2017

6. voir article page 36

Le développement de la puissance technologique de l'UE apparaît comme le deuxième volet de cette autonomie. La protection de l'industrie et du consommateur européens ainsi que le soutien apporté au développement des entreprises et de la recherche dans le domaine numérique sont indispensables. Cet aspect économique de l'autonomie stratégique de l'UE est aujourd'hui le plus développé ; il permet à l'UE de protéger son indépendance économique vis-à-vis des actuelles puissances numériques. Il doit continuer à être développé mais dans une perspective plus transversale en établissant une véritable politique européenne du numérique.

Des efforts restent cependant à produire en matière de cyberdéfense, troisième domaine de l'autonomie numérique stratégique. L'UE a surtout développé des mesures de cybersécurité dans la perspective du e-commerce. Quelques éléments de cybersécurité en dehors de ce champ ont toutefois vu le jour : l'adoption de la directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS (UE) 2016/1148), la création en 2004 d'une agence ENISA dont le mandat prendra fin en juin 2020 pour se voir attribuer un mandat permanent au centre du dispositif de certification prévu par le projet de règlement sur la cybersécurité de 2018, enfin la mise en place d'une équipe CERT-UE pour réagir aux cyberattaques visant les institutions et agences de l'UE. La cyberdéfense reste toutefois essentiellement l'apanage des Etats alors qu'une réponse aux cyberattaques ne peut être uniquement nationale et devrait être a minima coordonnée à l'échelle européenne.

L'autonomie stratégique de l'UE en matière numérique ne sera pleinement opérationnelle que si elle est complète dans ces différents domaines. L'élaboration d'un cadre normatif est en cours mais doit encore être développé.

SOUVERAINETÉ NUMÉRIQUE ET AUTONOMIE STRATÉGIQUE : LA NÉCESSAIRE CLARIFICATION POUR UNE AMBITION EUROPÉENNE

Alix DESFORGES



En décembre 2019, comme Angela Merkel quelques jours plus tôt, Jean-Yves le Drian appelait à *« construire une souveraineté numérique européenne »*. L'expression qui a connu un intérêt croissant depuis la fin des années 2000, est le plus souvent mobilisée pour évoquer une volonté d'émancipation à l'égard des plates-formes et entreprises du numérique américaines ultra dominantes sur le marché européen. Plus récemment, l'expression est également employée à l'égard de la montée en puissance d'entreprises chinoises en matière d'intelligence artificielle et de technologie 5G.

Très populaire chez les industriels de défense et dans les discours politiques français et européens, les documents officiels de stratégie ne reprennent pas ces termes et lui préfèrent le concept voisin d' *« autonomie stratégique numérique »*. Depuis 2017, le concept d'autonomie stratégique a en effet fait son entrée dans la politique européenne y compris dans les documents d'orientation stratégique de l'UE en matière de sécurité et d'affaires étrangères. Cet intérêt récent se fait à la faveur de l'évolution du contexte géopolitique de l'Europe ces dernières années : élection de D. Trump et désengagement américains des processus multilatéraux, Brexit, déstabilisation des frontières est de l'Europe par la Russie etc. Dans le do-



maine numérique, les enjeux géopolitiques contribuent également à l'émergence de ces discours par la représentation d'un espace numérique comme une menace géopolitique issues d'autres États à l'encontre de l'UE et de ses États-membres : soupçons d'influence dans les processus démocratiques, utilisations abusives des données personnelles avec Cambridge Analytica, régulation difficile des contenus des plates-formes ou encore extraterritorialité de la législation américaine avec le Cloud Act.

Historiquement, l'autonomie stratégique est l'un des piliers de la politique de défense française depuis la Seconde Guerre Mondiale. Dans la littérature stratégique française, l'autonomie stratégique vise à détenir la *« capacité autonome d'appréciation, de décision et d'action »* de la France. A ce titre, elle est aux fondements mêmes des politiques françaises en faveur d'une base industrielle et technologique de défense. En France, la stratégie de cyberdéfense reprend largement les bases de l'autonomie stratégique : émancipation de la domination d'acteurs américains et développement d'une base industrielle et technologique.

Le concept fait référence à l' *« autonomie de décision »* telle que définie par Lucien Poirier, théoricien de la dissuasion nucléaire française, à savoir la *« faculté pour un peuple de choisir librement, à l'abri de toute pression étrangère, le projet politique qu'il juge conforme à ses intérêts et à ses ressources »* (Poirier, 1982). L'autonomie de décision n'exclue pas les alliances, elle les encourage mais ces alliances doivent être explicitement désirées et surtout éclairées. C'est dans le choix *« des modalités de l'interdépendance »* (Poirier, 1982) que réside l'autonomie de décision.

Souveraineté et autonomie stratégique sont fortement liés. Ils renvoient pourtant à deux dimensions du même problème. Tout d'abord, l'expression *« souveraineté numérique »* peut être trompeuse car elle est basée sur la représentation d'une perte de souveraineté de l'État dans le cyberespace. En réalité le numérique vient plutôt bouleverser les modalités de l'exercice de cette souveraineté notamment par sa dimension transfrontalière. En outre, la *« souveraineté numérique »* peut renvoyer à une multitude d'enjeux d'ordre très différents (stratégiques, économiques, culturels, politiques), celui d'autonomie stratégique s'ancre lui dans une dimension sécurité et défense. Mais les discours identifient la domination d'entreprises américaines et son corolaire (le manque d'entreprises européennes) sur le marché du numérique comme une vulnérabilité au regard des potentialités de renseignement, d'espionnage et de déstabilisation permis par les outils numériques qui peuvent menacer l'exercice de la souveraineté des États. Ainsi, en 2017, la stratégie de cybersécurité de l'Union Européenne est présentée comme un élément concourant à l'autonomie stratégique de l'Europe dans le cyberespace. Le développement d'une autonomie stratégique européenne devient donc le moyen pour l'UE et ses États-membres de garantir l'exercice de leur souveraineté.

Toutefois, la prolifération des publications en Europe sur le sujet montre que l'autonomie stratégique ne fait l'unanimité ni dans ce qu'il recouvre ni dans ce qu'il implique. Quelles capacités européennes sont à développer et avec quel niveau d'ambition ? Il est pourtant crucial d'avoir cette discussion si l'UE veut parvenir à gagner en autonomie stratégique.

Fabienne JAULT-SESEKE

L'EXTRATERRITORIALITÉ EN QUESTIONS : CLOUD ACT ET RGPD



Une loi est extraterritoriale lorsqu'elle entend s'appliquer hors du territoire national. Les législations récentes en matière de données revêtent de façon évidente cette caractéristique.

Le Cloud Act, adopté en 2018, permet à l'administration américaine, dans le cadre de procédures pénales et c'est important de le préciser sur décision judiciaire, d'obtenir les données en possession des prestataires de services électroniques immatriculés aux Etats-Unis quel que soit le lieu de stockage de ces données, quel que soit le lieu de résidence ou la nationalité du data subject. Les GAFAM, immatriculés aux Etats-Unis, contrôlant soit directement, soit par l'intermédiaire de leurs filiales étrangères, elles aussi soumises au Cloud Act, l'essentiel du cloud mondial, cette législation peut être perçue comme offrant un accès à l'ensemble des données mondiales.

L'extraterritorialité est tempérée de deux façons. D'abord, le Cloud Act ménage une place au principe de courtoisie internationale pour respecter les intérêts des pays tiers. Ensuite, il encourage la conclusion d'accords bilatéraux pour organiser l'échange des données. Concrètement, en cas d'accord, l'accès aux données localisées dans l'Etat contractant, dont il est exigé qu'il respecte les standards minimaux de protection des droits de l'homme, reste possible mais cet Etat aura réciproquement accès aux données localisées aux US. Le système est proche de celui que souhaite mettre en place l'Union européenne avec le futur règlement e-evidence destiné à permettre aux autorités de poursuite d'obtenir directement des prestataires de services électroniques la divulgation des données. Seul l'avenir dira si ces deux mécanismes sont utilisés.

La loi de blocage française de 1968 susceptible d'interdire la communication à l'étranger d'informations sensibles et le règlement européen de blocage de 1996 destiné à contrer les décisions d'embargos n'ont pas prouvé leur efficacité pour s'opposer aux règles extrate-



rritoriales américaines. La nouvelle directive sur le secret des affaires adoptée en 2016 changera-t-elle la donne ? Tout dépendra de la conception de la courtoisie internationale que retiendront les juridictions américaines.

L'arme la plus efficace pourrait être le RGPD qui est clairement empreint d'extraterritorialité : les données pourraient être immunisées contre les demandes de communication américaines. Il interdit en principe les transferts internationaux et si les exceptions sont nombreuses dès lors qu'à l'étranger une protection équivalente à celle que prévoit le RGPD est garantie, le Cloud Act ne correspond à aucune d'elles. Or la violation du RGPD est sévèrement sanctionnée et on peut imaginer que le juge américain hésitera à exposer les entreprises américaines à de lourdes amendes.

La réglementation des transferts internationaux de données n'est pas la seule marque de l'extraterritorialité du RGPD, qui doit être entendue de façon générale (à la différence de celle du Cloud Act, limitée à l'efficacité des procédures pénales). Le RGPD soumet les sociétés établies dans les États tiers mais actives sur le marché européen aux mêmes règles que les sociétés européennes. En effet si le RGPD s'applique d'abord aux responsables de traitement et aux sous-traitants ayant un établissement dans l'Union, quel que soit l'endroit où a lieu le traitement, il s'applique aussi aux prestataires qui ne sont pas établis dans l'Union, dès lors que les traitements visent des personnes dans l'Union et sont liés à des offres de biens ou de services dans l'Union, ou au profilage du comportement de ces personnes sur le territoire de l'Union. Par exemple, l'utilisation de cookies pour suivre des internautes se trouvant dans l'UE déclenche l'application des règles européennes et le responsable de traitement ou le sous-traitant ne pourront pas arguer de leur extranéité pour y échapper.

On remarquera enfin que les injonctions prises en application de la législation européenne sont susceptibles d'avoir une portée mondiale. Ainsi en matière de droit au déréférencement, la Cour de justice a affirmé le principe leur dimension européenne mais elle laisse les autorités nationales libres, en fonction des intérêts à mettre en balance, de leur donner une dimension mondiale[1]. Cette dimension mondiale est de principe pour l'obligation d'effacer les contenus illicites[2].

L'extraterritorialité semble nécessaire pour que soit garanti le haut niveau de protection fixé par les règles européennes.

1. CJUE 24 sept. 2018, C-507/17

2. CJUE, 3 oct. 2019, aff. C-18/18



LA LUTTE CONTRE LA PROLIFÉRATION DES PROGRAMMES INFORMATIQUES MALVEILLANTS ET LE DROIT INTERNATIONAL

Aude GÉRY

La multiplication des attaques informatiques et la course au développement de capacités offensives interrogent nécessairement sur la capacité du droit international à se saisir d'un sujet par nature transnational : la lutte contre la prolifération des programmes informatiques malveillants. Les caractéristiques de l'espace numérique, des biens considérés (immatérialité, capacité à être volés, réutilisés, etc.) et de l'environnement de leur prolifération (diversité des acteurs impliqués, de leurs motivations, etc.)

Les Etats membres du cinquième Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (GEG) se sont saisis de cette question en 2015 et ont adopté une norme recommandant aux Etats prévenir la prolifération des techniques et outils informatiques malveillants et l'utilisation des fonctionnalités cachées malveillantes[1]. Le caractère déclaratoire de cette disposition nécessite qu'elle soit mise en œuvre de façon concrète par les Etats.
A cette question on oppose souvent une réponse technique : les spécificités techniques empêcheraient toute application des obligations de l'entreprise du désarmement. La confrontation du droit et de la technique rend indéniablement limitée toute approche fondée sur un contrôle du bien lui-même, soulevant principalement des difficultés

de définition du champ matériel et d'application de ces obligations. Cependant, il doit être pensé en lien avec le contrôle de l'usage dans le cadre d'une approche globale fondée sur la *« création d'une culture mondiale de la cybersécurité »*[2]. Dans ce domaine, l'Europe a certainement un rôle à jouer et peut même faire figure de modèle.

En matière de contrôle du bien, la reprise des discussions sur le projet européen de réforme du régime de contrôle aux exportations des biens à double usage constitue une étape importante en raison des risques, notamment pour les droits de l'homme, associés à l'utilisation des technologies de cyber-surveillance (Commission européenne, Proposition de règlement, 28 sept. 2016). Quelles que soient leurs limites, ces contrôles participent au renforcement de la stabilité de l'espace numérique. La préservation des usages légitimes doit cependant être placée au cœur de la réflexion sur les contrôles aux exportations, menant ainsi à une réflexion plus large sur le contrôle de l'usage.

Selon que l'on s'intéresse à leur usage par les Etats ou les acteurs non-étatiques, le contrôle de l'usage permet de prendre en compte la double dualité de ces biens. Pour les premiers, l'application du droit international général fait face à de profondes divergences d'interprétation qui pour certaines sont intrinsèquement liées aux spécificités de l'espace numérique et à la prédominance de la perception du risque géopolitique sur le risque systémique[3]. Pour les seconds, les outils de la lutte contre la cybercriminalité s'imposent comme un instrument majeur. Ils partagent avec l'application du droit international général des problématiques communes posées en des termes différents notamment en matière d'extraterritorialité et d'attribution.

Pour être mis en œuvre, ces contrôles du bien et de l'usage nécessitent enfin d'importantes capacités et un haut niveau de coopération internationale, piliers de la *« création d'une culture mondiale de la cybersécurité »* à laquelle l'Assemblée générale a appelée. C'est ici que cette approche globale prend tout son sens. Là encore, l'Europe peut servir de modèle à travers la directive NIS (Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union) et le Cybersecurity Act[4]. Disposant d'un important pouvoir d'influence normatif, l'Europe fait figure de référence dans la mise en œuvre des recommandations de l'ONU et pourrait, dans le cadre d'une stratégie diplomatique européenne coordonnée, être force de propositions dans la mise en oeuvre des recommandations de l'Assemblée générale et des précédents rapports des GEG.

L'étude du recours au droit international pour lutter contre la prolifération de ces biens amène donc à dépasser l'analyse de l'application des obligations de l'entreprise du désarmement pour s'intéresser aux différents instruments adoptés au sein d'organisations internationales ou régionales. Elle soulève des questions fondamentales qui vont au-delà du simple cadre de la lutte contre la prolifération des programmes informatiques malveillants, conduisant ainsi à mener une réflexion sur ce qui serait un droit international du cyberespace en formation.

1. AGNU, Résolution 73/27 « Progrès de l'informatique et des télécommunications et sécurité internationale », adoptée le 5 déc. 2018, A/RES/73/27, para. 1.10

2. AGNU, Résolution 57/239 « Création d'une culture mondiale de la cybersécurité », adoptée le 20 déc. 2002, A/RES/57/239

3. Frédérick Douzet, « Premier anniversaire de l'Appel de Paris », Paris Peace Forum, 12 nov. 2019

4. Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°426/2013 (règlement sur la cybersécurité)

LE DROIT INTERNATIONAL APPLICABLE AUX OPERATIONS DANS LE CYBERESPACE

François DELERUE



Le droit international est au cœur des relations internationales et est essentiel au maintien de la paix et de la sécurité internationales. Ceci est encore plus vrai dans l'espace numérique et en ce qui concerne les actions numériques des États et des autres acteurs.

Il est aujourd'hui unanimement admis par les États et la littérature académique que le droit international est applicable dans le cyberespace et aux opérations qui s'y déroulent. À l'inverse, l'application concrète des normes de droit international est au cœur des discussions internationales sur la paix et la stabilité dans le cyberespace et fait l'objet de désaccords voire d'oppositions importantes entre les États.

Les travaux des différents Groupes d'experts gouvernementaux chargés d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (GEG) des Nations Unies illustrent particulièrement cette situation. Les rapports des GEG de 2013 et 2015 ont reconnu que *« [l]e droit international et, en particulier la Charte des Nations unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible »*[1]. Néanmoins, le cinquième GEG a échoué en juin 2017 à cause de désaccords importants sur le droit international, plusieurs États s'opposant à ce que l'applicabilité du droit de légitime défense, des contre-mesures et du droit des conflits armés soit mentionnée et développée dans le rapport du GEG. Il y a actuellement deux processus en cours aux Nations Unies sur ces questions, un nouveau GEG[2] et un Groupe de travail à composition non limitée[3].

Le droit international définit les droits et obligations des États dans le cyberespace. Ainsi, il détermine le cadre juridique pour l'attribution des cyber opérations à un État, leur qualification juridique (violation

de souveraineté, intervention illicite, violation des droits de l'homme, recours à la force ou encore agression armée), les obligations qui incombent à l'État responsable (obligation de cessation et de réparation) et les modalités de réaction de l'État victime (mesures de rétorsion, contre-mesures ou légitime défense). Le droit international encadre également le recours aux cyber opérations dans le cadre de conflits armés.

L'Union européenne et ses États membres ont affirmé avec force leur attachement au respect du droit international, notamment dans le cyberspace. En ce sens, la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité rappelait le 12 Avril 2019 que *« [l]'Union européenne et ses États membres sont des ardents avocats d'un cyberespace ouvert, stable et sûr, respectueux des droits de l'homme, des libertés fondamentales et de l'État de droit »*. De plus en plus d'États exposent publiquement leur approche du cadre juridique international applicable dans le cyberspace. La France, par exemple, a ainsi rendu public en septembre 2019 un rapport sur le 'Droit international appliqué aux opérations dans le cyberespace' qui expose la position française et a vocation à servir de base dans les négociations onusiennes. Plus largement, au niveau multilatéral, les États discutent de l'interprétation et de l'application du cadre juridique international et sur la définition des comportements responsables à adopter dans le cyberespace. Une littérature académique fournie s'est développée sur le droit international applicable aux opérations dans le cyberespace au cours de la dernière décennie, notamment dans le monde anglo-saxon, mais aussi en France.

Tout d'abord, il convient de mentionner les deux éditions du Manuel de Tallinn parue en 2013 et 2017 aux Presses universitaires de Cambridge. Le Manuel de Tallinn est le résultat de la demande du Centre d'excellence de cyberdéfense coopérative de l'OTAN (NATO CCD COE) à un groupe d'experts internationaux de préparer un manuel sur le droit international applicable à la cyberguerre. Bien que financés par le NATO CCD COE, les deux éditions du Manuel de Tallinn ne sont pas des documents officiels ou l'expression de la position du NATO CCD COE, de l'OTAN ou de leurs États membres ou partenaires.

Le monde universitaire français est aussi particulièrement actif sur ces questions. Au sein du centre de recherche et de formation sur la géopolitique de la datasphère (Géode) Aude Géry et le Professeur Anne-Thida Norodom développent des recherches originales sur le droit international applicable aux activités numériques. Le Professeur Anne-Thida Norodom avait co-organisé avec le Professeur Philippe Lagrange le colloque de la Société française pour le Droit international sur *« Internet et le droit international »* en 2013. Plus récemment, elle a réuni avec Maryline Grange un groupe d'internationalistes pour réfléchir à ces questions, conduisant à la publication d'un ouvrage collectif en 2019. La thèse de doctorat d'Aude Géry se concentre sur la réglementation internationale de la prolifération des cyber armes et elle développe aujourd'hui ses recherches sur la diversité des approches des États sur le droit international applicable au cyberespace. À l'Université de Grenoble Alpes, Karinne Bannelier-Christakis et le Professeur Théodore Christakis sont particulièrement actifs sur ces questions et sont à l'origine de la création du Cyber Security Institute et du Grenoble Alpes Data Institute. À l'Institut de Recherche stratégique de l'École militaire (IRSEM), François Delerue (l'auteur de la présente note) travaille sur l'application du droit international aux cyber opérations et l'analyse des différentes approches des États, son livre paraîtra prochainement. Dans le cadre du projet EU Cyber Direct dont il est rapporteur, il développe ses recherches sur la diplomatie numérique européenne.

1. documents des Nations Unies A/68/98 et A/70/174

2. Résolution A/RES/ 73/266

3. GTCNL – Résolution A/RES/73/27

Les auteurs

Karine BANNELIER-CHRISTAKIS, MCF-HDR en droit international, Directrice adjointe du Grenoble Alpes CyberSecurity Institute et de la Chaire *Legal and Regulatory Implications of Artificial Intelligence* du MIAI Grenoble Alpes. – **Anne CAMMILLERI,** Professeure de droit public et droit de la cybersécurité à l'Université Sorbonne Paris Nord, co-directrice de l'Institut de Droit public, sciences Politiques et Sociales- IDPS – **Théodore CHRISTAKIS,** Université Grenoble Alpes, Directeur de la Chaire *Legal and Regulatory Implications of Artificial Intelligence* (MIAI) ; Membre de l'IUF, du Conseil National du Numérique, du *Cross Border Data Forum* et du Comité National Pilote sur l'Ethique du Numérique et de l'Intelligence Artificielle – **François DELERUE,** Chercheur en cyberdéfense et en droit international, IRSEM ; Rapporteur pour le droit international, EU Cyber Direct ; Enseignant, Sciences Po Paris – **Alix DESFORGES,** Post-doctorante au centre Géopolitique de la Datasphère (GEODE), Université Paris 8 – **Thibault DOUVILLE,** Professeur des Universités en droit privé, Université de Caen Normandie – **Aude GÉRY,** Chercheuse au centre Géopolitique de la Datasphère (GEODE), Université Paris 8 ; doctorante en droit international public – **Chloé HERVOCHON,** Doctorante contractuelle en droit privé avec mission d'enseignement, Université de Caen Normandie – **Fabienne JAULT-SESEKE,** Professeur des Universités en droit privé, Université de Versailles Saint-Quentin-en-Yvelines, co-présidente du réseau Trans Europe Experts – **Anne LE HÉNANFF,** Titulaire de la Chaire de Cybersécurité des Grands Événements publics, Université Bretagne Sud, membre fondatrice de la fondation Women4Cyber – **Emmanuel NETTER,** Maître de conférences HDR en droit privé, Université d'Avignon **– Anne-Thida NORODOM,** Professeur de droit public, Université de Paris – **Nadir OUCHENE,** Docteur en droit, Université Paris 2, Panthéon-Assas, et Attaché Temporaire à l'Enseignement et à la Recherche à l'Université Sorbonne Paris Nord – **Émilie POUFFIER-THOMPSON,** Doctorante en droit, Cabinet Alema Avocats et Université Bretagne-Sud (laboratoire Lab-LEX) – **Michel SÉJEAN,** Professeur de droit privé et sciences criminelles, Membre du Bureau du *Cyber Security Center* de l'Université Bretagne Sud – **Célia ZOLYNSKI,** Professeur des Universités, Ecole de Droit de la Sorbonne, Université Paris 1, Panthéon-Sorbonne, co-directrice du pôle numérique du réseau Trans Europe Experts

Sponsors

Partenaires

S&D MAGAZINE

VOTRE MAGAZINE RÉFÉRENCE **EN SÉCURITÉ & DÉFENSE**



JE M'ABONNE
sur sd-magazine.com

Smart & Safe JO 2024
Export & Economie
Lutte contre le terrorisme
Diplomatie & coopération internationale
Cybersécurité & Confiance numérique
Smart & Safe Cities
Risques majeurs - Sécurité privée
Techno & innovation
Défense - **Politique & stratégie,** etc.

Contact : S&D Magazine
Rédaction en chef : Mélanie BENARD-CROZAT
6 numéros par an / redaction@sd-magazine.com / +33 6 84 75 32 32

Cybersecurity Institute
Univ. Grenoble Alpes

Reshaping Technologies and Social Sciences



Cost Effective IoT / Hardware Protection

Social Impact, Law & Governance

Prevention & Reactions to Attacks

Quantum-Safe Security & Privacy

Cybersecurity & AI

Resilient Critical Infrastructure

Cybersecurity & Policy Challenges

- Undertaking ground-breaking interdisciplinary research in order to address cybersecurity and privacy challenges
- Holistic approach, encompassing technical, legal, law-enforcement, economic, social, diplomatic, military and intelligence-related aspects
- Strong partnerships with the private sector and robust national and international cooperations with leading institutions in France and abroad

More information on
cybersecurity.univ-grenoble-alpes.fr

UGA Université Grenoble Alpes

financed by
IDEX Université Grenoble Alpes