« L'humain, acteur de la cybersécurité sur terre et sur mer ».

Synthèse du Colloque « Charente-maritime Cyber sécurité » (CMCS)

La Rochelle - 15, 16 & 17 octobre 2019

Pierre Berthelet

Docteur en droit, chercheur associé auprès de la Gendarmerie nationale (CREOGN) et de l'Université Grenoble-Alpes (CESICE)

L'être humain, objet de ce colloque CMCS 2019, apparaît comme vulnérable. Alors qu'Internet est censé connecter chacun d'eux, celui-ci semble se trouver isolé plus que jamais. Tandis que les nouvelles technologies étaient censées lui offrir de nouvelles opportunités, celles-ci paraissent désormais se retourner contre lui. Il se retrouve en effet dépouillé (ou menacé de l'être) de ses moyens financiers et de ses données personnelles. En parallèle, l'édition 2019 met en exergue une forte mobilisation des acteurs du monde économique et maritime (puisque le thème portait également sur ce sujet), le déploiement significatif de politiques publiques et de stratégies d'entreprise, ainsi que le recours accru à l'innovation. Ce colloque met en évidence une cybersécurité pourvoyeur de lien social. Il s'agit, en d'autres termes, d'un projet au service de l'homme. C'est à cet égard l'expression d'un humanisme entendu comme une doctrine morale reconnaissant à l'homme la valeur suprême.

En 1963, l'historien Richard Hofstadter avait dépeint, dans un essai célèbre *The Paranoid Style in American Politics*[1], la manière dont le discours McCartyste sur l'infiltration de Washington par les communistes s'était diffusé parmi l'opinion publique. Ce « style paranoïaque » dans la façon de gouverner la Cité au regard duquel le complotisme constitue un ressort central du narratif politique n'a jamais eu autant de succès qu'à l'époque contemporaine. L'essayiste Susan Jacoby, dans son

[1] R. Hofstadter, « The Paranoid Style in American Politics », *Harper's Magazine*, 2012 [1963].
Article disponible à l'adresse suivante : https://harpers.org/archive/1964/11/the-paranoid-style-in-american-politics/

ouvrage *The Age of American Unreason in a Culture of Lies*[2] déclare à ce sujet qu'Internet s'apparente à une autoroute en direction des contrées lointaines de la pensée moisie ("a highway to the far-flung regions of junk thought"). Force est de constater à cet égard que l'essor des réseaux sociaux contribue largement à la propagation de fausses nouvelles (*fake news*). Qui plus est, ce phénomène n'est pas isolé. Il a colonisé le monde numérique et il constitue désormais un levier puissant d'influence, à la fois dans la compétition pour le pouvoir et dans son exercice[3] (aux États-Unis, le Président Trump n'hésitant pas diffuser des fake news pour disqualifier ses adversaires politiques, ou à colporter des théories complotistes), ainsi que dans l'usage du *soft power* tel que théorisé par le politologue Joseph Nye : grâce aux *fake news*, les puissances étrangères sont à même d'influer sur le cours des démocraties occidentales (en écho aux « fermes à trolls » russes ayant été mentionnées lors du colloque « Charente-maritime Cyber sécurité » 2018).
Au cours du colloque CMCS pour l'année 2019, plusieurs intervenants ont mis en exergue le fait qu'Internet était devenu à cet égard un terrain de confrontation, les fake news devenant une arme. Un intervenant avait évoqué les opérations de guerre psychologique (« PsyOp ») réalisées au moyen des outils numériques. Un autre avait souligné le fait que désormais, la tendance était à la concentration des forces. Les pirates se professionnalisent et s'organisent. Il s'agit avant tout de spécialistes chevronnés, formés et travaillant le cas échéant sous la responsabilité des États.

Cette concentration des forces s'accompagne d'une aggravation des dangers : multiplication des cyberattaques, pertes toujours plus importantes pour l'économie, altération généralisée de processus électoraux, et émergence de nouvelles menaces liées au développement de la 5G ainsi que l'intelligence artificielle.

Dans ce cybermonde toujours plus dangereux, l'être humain, objet de ce colloque CMCS 2019, apparaît comme vulnérable. Alors qu'Internet est censé connecter chacun d'eux, celui-ci paraît se trouver isolé plus que jamais. Tandis que les nouvelles technologies étaient censées lui offrir de nouvelles opportunités, celles-ci semblent désormais se retourner contre lui. Il se retrouve en effet dépouillé, ou menacé de l'être, de ses moyens financiers et de ses données personnelles.

En conséquence, le cybermonde constitue un problème (1). Toutefois, et le colloque l'a clairement fait ressortir, il apparait aussi comme un espace sécurisé et le numérique une solution, vecteur de croissance et créateur de lien social (2). En effet, l'édition 2019 a mis en exergue une forte mobilisation des acteurs du monde économique et maritime (puisque le thème portait également sur ce sujet), le déploiement significatif de politiques publiques et de stratégies d'entreprise, ainsi que le recours accru à l'innovation. Ces différents outils visent à rendre le cybermonde plus sûr et davantage engobant. En effet, ce colloque comprend une dimension « inclusion numérique ». Il s'agit de venir en aide aux populations fragiles (personnes en situation de précarité sociale, mais également personnes âgées, personnes en situation de handicap ainsi que personnes vivant en zone rurales, plus exactement au sein de zones dites « blanches »).

À ce propos, CMCS 2019 met en exergue une cybersécurité pourvoyeur de lien social. Il s'agit, en d'autres termes, d'un projet au service de l'homme. C'est l'expression d'un humanisme entendu comme une doctrine morale reconnaissant à l'homme la valeur suprême. Le juriste Lawrence Lessing, dans un article remarqué, intitulé « Code is law, On Liberty in Cyberspace »[4], avait insisté sur

[2] S. Jacoby, *The Age of American Unreason*, New York, Vintage Books.
[3] Pour une confirmation actuelle de cette approche, voir les travaux de J. Eric Oliver Thomas J. Wood, « Conspiracy Theories and the Paranoid Style(s) of Mass Opinion », *American Journal of Political Science*, vol. 58, n° 4, 2014, p. 952-966.
[4] L. Lessing, « Code and Other Laws of Cyberspace », *Harvard Magazine*, janvier 2000.
Article disponible à l'adresse suivante : https://harvardmagazine.com/2000/01/code-is-law-html

l'importance politique du code, c'est-dire l'absence de neutralité de l'architecture technique du monde numérique. La table ronde sur l'intelligence artificielle, qui s'est tenue en marge de ce colloque, a souligné la dimension non seulement politique mais aussi morale de la cybersécurité et de l'IA[5]. « Code is ethical » au sens où les nouvelles technologies tendent à être gouvernées, c'est du moins le vœu des intervenants de cette table ronde, par un ensemble des règles conduites fondées sur un humanisme pratique instaurant un ensemble de devoirs et d'interdits éthiques.

1. Le cybermonde, forme d'anomie ou d'anarchie numérique ?

Deux tendances complémentaires se dégagent. La première est semblable à l'anomie décrite par le père de la sociologie, Emile Durkheim : l'espace numérique s'apparente à une société sans règles au sein de laquelle l'individu est abandonné, livré aux cyberpirates (1.1).

La deuxième rappelle l'anarchie dépeinte par le philosophe Thomas Hobbes, en vertu de la célèbre maxime « l'homme est un loup pour l'homme ». Dans un cybermonde périlleux où chacun est en proie à ses pulsions et poursuit son intérêt, l'être humain menacé apparaît comme vulnérable (2.2).

1.1 L'espace numérique, une expression nouvelle d'anomie

Dans ce monde dérégulé, l'individu semble être cerné par les dangers : multitude de fausses nouvelles qui abondent sur Internet, prises USB hackées dans les gares et les aéroports, pédopornagraphie sur les réseaux sociaux et, tendance nouvelle, vente en ligne de drogue sur la célèbre application Snapshat. Un intervenant avait donné l'exemple d'un serveur destiné à servir d'appât (« honeypot »). Une fois connecté sur le net, celui-ci avait fait l'objet d'une dizaine d'attaques en quelques minutes seulement. Quant à la nature de celles-ci, elles se caractérisent par les virus, rançonlogiciels et divers malwares « à la mode », selon le terme employé par cet intervenant.

L'exemple des produits contrefaits donné par un autre intervenant est édifiante : la contrefaçon n'a jamais été aussi présente sur Internet. Elle se banalise et se professionnalise. Internet regorge de produits de contrefaçon, partagés par des particuliers, à huis clos au sein de groupes Facebook, ou vendus par des professionnels ayant développé des stratégies marketing de haut niveau. Ceux-ci utilisent des techniques telles que le système d'évaluations positives des acheteurs, les promotions éphémères et les ristournes accordées aux clients fidèles.

« Le problème est que sur le net comme dans la vie, il y a plus de cons que de méchants ». Cette formule quelque peu provoquante d'un intervenant illustre néanmoins un constat simple : la criminalité est constituée pour une grande partie, de criminels opportunistes, ayant peu de compétences en informatique. La dangerosité du monde numérique est aggravée par l'attitude des utilisateurs du web, peu conscients des menaces qui pèsent sur eux. Au cours de ce colloque, les exemples de comportements peu responsables étaient particulièrement abondants : utilisation par le collaborateur curieux d'une clé USB « abandonnée » ayant permis la captation de secrets d'affaires d'un célèbre cabinet d'avocat, mails de phishing cliqués par des internautes appâtés par la promesse de loterie, d'un téléphone gracieusement offert, ou de billets de concerts à prix sacrifié, non actualisation de systèmes d'exploitation, usage récurrent de mots de passe simples ou non mis à jour, téléchargement d'une application de jeu corrompue, connexion non sécurisée au réseau wifii, partage

La deuxième version, intitulée *Code v2* (New, York, Basic Book, 2006), est disponible en pdf à l'adresse suivante : http://codev2.cc/

[5] Voir ce sur ce thème : N. Bostrom, E. Yudkowsky, « The ethics of artificial intelligence », *in* K. Frankish, W. M. Ramsey, *The Cambridge Handbook of Artificial Intelligence*, Cambridge, Cambridge University Press, 2014, p. 316-334.

d'informations sur la vie familiale donnant au cambrioleurs des renseignements sur les projets de vacances, etc.

Les mésaventures de la « famille Padbol » sont une illustration archétypique des mauvais comportements dans le monde numérique. Elles illustrent la négligence des individus dépeintes par « Olivier », officier de la Direction générale de la sécurité intérieure (DGSI), montrant à quel point il est aisé de s'approprier des données personnelles et d'affaires : codes confidentiels notés sur un post-it laissé sur le bureau (cet officier des services de renseignement ayant expliqué que des données relatives à l'utilisation de l'ordinateur se trouvaient toujours à proximité, généralement à moins d'un mètre du poste concerné), outils informatiques laissés sans surveillance dans le train, réunion de travail dans des lieux publics et possibilité d'appropriation de projets R&D sensibles par une simple capture d'écran d'ordinateur d'un collaborateur travaillant dans une gare. Toutes ces formes négligence se rapportent au « PFH » (« putain de facteur humain ») mentionné par un autre intervenant.

Ces multiples négligences corrélées aux actes de malveillance volontaires semblent attester que le numérique est un espace sans loi, ou du moins, au sein duquel le droit, celui émanant des États démocratiques, s'applique de manière théorique. Le sentiment qui ressort de multiples interventions est qu'Internet parait être dérégulé ou, plus précisément, il est soumis à des régulations qui échappent aux États, car imposées par les grandes entreprises du numérique, les GAFAM (Google, Apple, Facebook, Amazon et Microsoft). « On a tout balancé sur le web » avait déclaré un intervenant. L'appropriation des données, l'intrusion dans la vie privée et le déploiement de technologies de traçage de l'individu sont d'autant plus aisés que ceux-ci consentent, à des degrés divers, au dévoilement de la vie privée. L'existence ou non de cette vie privée a constitué un réel clivage entre les intervenants de ce colloque. Pour certains, celle-ci existe et doit être préservée (évoquant l'intérêt du règlement général sur la protection des données - RGPD), alors que pour d'autres, elle est désormais une vue de l'esprit (notamment au regard de la puissance des GAFAM). Sans entrer davantage dans ce débat, un aspect a été relevé par eux : les individus, qu'ils soient soucieux ou non de la préservation de leur vie privée, libèrent un ensemble de données les concernant, de nature à permettre de cerner certains aspects les plus intimes de leur vie.

Ce processus de dévoilement volontaire a été remarquablement mis en évidence à travers la vidéo belge du faux mage : celui-ci, guidé par des complices cachés en coulisse, divulguait des informations données à des quidams volontaires, ignorant tout de la supercherie. Disposant de données trouvées sur Internet par ses complices chargés de parcourir les réseaux sociaux, ce mage, « devinait » sous une tente créée à cet effet, la situation financière, familiale et professionnelle des cobayes stupéfaits par les informations révélées par ce mage doté de capacités présupposées hors du commun.

La question du consentement est un aspect sous-jacent des discussions de ce colloque. Elle interroge en effet, et ce, particulièrement à un double titre :

- il s'agit de la situation de l'internaute qui ne sait pas ce qu'il télécharge. Le cas de grand-mère de la famille Padbol illustre cette méconnaissance des dispositifs intrusifs de la vie privée,

- il s'agit de la situation de données divulguées par des tiers. Le problème relatif à la vie privée de l'application Faceapp a été mentionnée, surtout lorsque ces données concernent des visages transmis par un proche désireux de découvrir l'évolution morphologique de son entourage.

L'individu est alors soumis à des régulations qui lui échappent. Ces dernières sont parfois délibérément ignorées par certains opérateurs économiques, voire purement et simplement contournées par des

individus peu scrupuleux. Dans un tel monde dérégulé, l'homme est menacé par ses pairs. Internet apparaît alors comme l'illustration d'une forme contemporaine d'anarchie dite « hobbesienne ».

1.2 L'espace numérique, une forme contemporaine d'anarchie

« Personne n'accepterait un gâteau offert par un inconnu dans la rue, pourtant, nous acceptons tous les cookies sur le net ». C'est par ces propos qu'un intervenant a souligné les dangers sur Internet. Force est de constater que ceux-ci sont nombreux. Ce colloque a d'ailleurs été l'occasion de dresser un panorama pour le moins inquiétant : développement des rançonlogiciels, prolifération des mails de phishing, multiplication des supports de stockage infectés. Cet essor des cyberdangers est accentué par le description faite par les hackers, dépeints par certains intervenants comme des êtres sans scrupules, appâtés par le gain facile et ne reculant devant rien.

Ce phénomène est renforcé par la disponibilité des biens et des services sur le Darknet, mais aussi parfois sur l'Internet officiel : données bancaires et personnelles proposées à vil prix, ransomewares et autres malwares vendus au plus offrant, sans compter les services de hacking mis à disposition par certains pirates désireux de mettre à disposition leurs services contre rémunération.

La gravité des dangers est accentuée par deux autres phénomènes. Le premier est lié à l'usage actuel des téléphones intelligents. Un intervenant avait qualifié ceux-ci de véritable « plaie », tant ils regorgent de données personnelles susceptibles d'être collectées par des cyberpirates. L'évolution tend actuellement d'ailleurs vers l'appropriation de ce type de données. Un intervenant avait souligné le fait que leur valeur avait gagné en importance à un point tel qu'elles présentaient davantage d'intérêt que les données bancaires (par exemple dans la perspective d'une usurpation d'identité). Ce risque est aggravé par l'absence de méfiance des utilisateurs conjuguée au fait que certains malwares sont désormais dormants. En effet, ces nouvelles générations de logiciels malveillants ne causent aucune perturbation dans le téléphone. Ils sont alors indétectables rappellent un intervenant. Ils peuvent alors être activés au bout de certains mois seulement. Une fois le téléphone infecté, le cyberpirate peut observer le trafic de données, captant au passage celles de nature à revêtir un intérêt, ceci sans que l'utilisateur ne soit conscient de ce mouvement de « syphonnage » qui s'opère des mois durant.

Le deuxième phénomène est lié à la tendance actuelle des objets connectés. L'interconnectivité est décrite par un intervenant comme la « bombe atomique ». Peu sécurisés, ces objets, avant tout conçus pour leurs fonctionnalités, se révèlent vulnérables. Un autre intervenant avait expliqué que les stratégies d'intrusion dans un système s'orientaient désormais vers la prise de contrôle d'un objet connecté. Un autre encore avait précisé que les nouvelles rançonlogiciels visaient à paralyser l'activité d'entreprises en bloquant ces objets connnectés, les rendant ainsi inopérant.

Les dangers sont importants au regard du développement des objets autonomes. Le risque de la prise de contrôle de bateaux autonomes représente à ce propos un danger non négligeable du point de la sécurité maritime. Les intervenants de cette édition 2019 de CMCS, dont l'un des points d'orgue portait sur la cybersécurité dans ce domaine, ont d'ailleurs souligné la vulnérabilité des entreprises et des systèmes. Ainsi, l'un d'eux, évoquant les cybermenaces pesant sur la numérisation de la pêche à la criée, avait indiqué, à juste titre, « nous sommes des pêcheurs et des négociants, nous ne sommes pas des geeks ». Avec le perfectionnement des attaques et la faiblesse des moyens pour les contrer, les intervenants de la dernière table ronde du colloque ont mis en relief une forme actualisée d'anarchie dépeinte par le philosophe Thomas Hobbes : faute de puissance publique forte, les individus craignent pour leur sécurité et sont à la merci d'individus malveillants. Elle rappelle ainsi l'état de nature décrit par l'éminent penseur anglais où chacun craint pour sa sécurité, où l'Autre constitue une menace et

où la confiance cède le pas à la méfiance (au cours de de ce colloque, un intervenant avait d'ailleurs vivement suggéré de ne jamais se fier à ses collaborateurs).

En écho à cette situation d'anarchie, un autre intervenant souligne qu'avec le phénomène du big data (renforcé par l'essor de l'internet des objets), le problème ne porte plus sur la disponibilité des données. Celles-ci sont désormais partout. Redondantes, car stockées sur de multiples serveurs, l'enjeu les concernant porte désormais sur leur intégrité. Illustré par le problématique des fake news, le problème a trait à leur authenticité, ceci d'autant plus que les outils d'altération (tels que le deepfake) sont toujours plus accessibles et plus perfectionnés. Le développement de ces nouvelles technologies sont, non seulement de nature à altérer la qualité des données, mais aussi à renforcer la méfiance entre individus et à aggraver les tensions entre communautés (l'usage d'un logiciel de deepfake destiné à créer de toutes pièces des images de soldats américains brûlant le Coran est susceptible d'aggraver les tensions au Moyen-Orient). Ils peuvent nuire à un candidat à une élection, à la réputation d'une entreprise et même au particulier (les outils de Revenge Porn permettant dorénavant d'apposer de manière réaliste, le visage d'une personne, dont une autre cherche à se venger, sur le corps d'un acteur ou d'une actrice de film X).

La maitrise par l'individu de ses données personnelles (et authentiques) est donc devenue un véritable enjeu mis en exergue par les intervenants de ce colloque. L'un d'entre eux avait d'ailleurs évoqué le perfectionnement des techniques de captation. En dépit du fait qu'il soit professionnel de la cybersécurité, il avait expliqué la manière dont il s'était fait berné par des escrocs ayant eu recours à une forme d'hameçonnage sophistiquée. D'après plusieurs intervenants, les mails de phishing sont de moins en moins grossiers. De surcroît, les pirates prennent le temps d'observer la vie privée des victimes. En outre, ils possèdent des outils de collecte plus perfectionnés. Plus généralement, tous s'accordent à dire que les techniques dites « d'ingénierie sociale » se développent. La fraude dite « au président » a ainsi été largement mentionnée à côté du cyber-hameçonnage.

L'être humain est alors vulnérable car sans défense. Ceci est dû non seulement au perfectionnement des techniques d'attaques et par cette « concentration des forces » mentionnée en introduction, mais aussi par l'absence de sensibilisation des dangers qui l'environnent. L'atelier sur l'inclusion numérique a souligné ce type de vulnérabilité. L'exclusion numérique concerne à l'heure actuelle cinq millions de Français. Cette fragilité est largement abordée : fragilité sociale et difficultés cognitives (obstacles à la mémorisation des mots de passe par exemple) rendent toute une population particulièrement vulnérable. Or, un intervenant avait mis en exergue le fait que les pirates visaient de préférence un public vulnérable. « Les fragiles, c'est comme les pauvres. Ils n'ont pas grand-chose, mais ils sont tellement nombreux qu'une attaque à grande échelle est rentable ».

Reste que différents outils sont déployés pour aider ce public. Le cyber se révèle en effet à maints égards, être désormais à la solution.

2. Du cyber comme problème au cyber solution : les remèdes apportés par la cybersécurité et l'intelligence artificielle

« La cybersécurité n'est pas affaire de gros sous, mais de bons sens ». Ces propos de cet officier de la DGSI rappellent que la cybersécurité est affaire de comportements individuels. Chacun est acteur de sa propre sécurité, bien que les comportements adoptés soient ceux de personnes sensibilisées aux dangers d'Internet. La sensibilisation figure, à cet égard, parmi la gamme des mesures préconisées. La cybersécurité correspond en effet à une panoplie de moyens techniques, de stratégies économiques et de leviers sociaux visant à protéger l'individu. Elle est au service de l'homme, c'est d'ailleurs le thème du colloque (2.1).

Il est même possible d'aller plus loin en considérant que l'homme constitue non seulement la finalité de la cybersécurité, mais aussi sa mesure. Celle-ci est en effet modelée par une morale humaniste, au sens où l'homme s'impose, au nom d'un principe de l'autonomie propre à cette doctrine, une série de devoirs et d'interdits éthiques (2.2).

2.1 L'individu protégé, la cybersécurité au service de l'homme

« Soyez acteurs de votre vie numérique ». C'est le message d'un intervenant soulignant l'importance de l'attitude à avoir sur Internet. D'après lui, il faut apprendre aux 90% des internautes à se méfier, et aux 10% des personnes non connectées (ou qui rechignent à le faire) à faire confiance.

Cette mesure du risque constitue un élément central des différentes interventions. Il s'agit d'apprendre non seulement aux internautes à adopter un comportement avisé dans le cybermonde, mais aussi à avoir une attitude suffisamment confiante, tout en se montrant raisonnablement méfiant. Il est en de même pour les entreprises vis-à-vis de leurs partenaires économiques. Celles-ci doivent faire confiance à ceux qui se protègent correctement et qui en apportent les gages. Il s'agit, à l'inverse, de se méfier de celles qui ne respectent pas les règles de cybersécurité et ne remplissent les standards de conformité.

Une tendance se dégage en effet de la part des intervenants. Face aux cyberpirates, il existe toute une série de parades visant à restaurer la confiance dans ce monde numérique perçu comme dangereux. De nombreux exposés techniques ont mis en évidence les solutions technologiques pour contrer les attaques. Plusieurs acteurs ont mis en avant une palette de solutions, qu'elles soient technologiques ou sociales. La présentation d'un « serious game » par un des intervenants, permet aux utilisateurs des outils du monde numérique, de se mettre dans la peau d'un cyberpirate. L'objectif est de favoriser la prise de conscience de la vulnérabilité des systèmes de même que les comportements fautifs. Il s'agit d'un exemple des bonnes pratiques visant à sensibiliser et à former le public, qu'il soit collaborateur d'une entreprise ou fonctionnaire d'un organisme public. Cette nouveauté illustre les efforts menés en matière innovation.

Il est fait appel également à l'innovation comme parade aux cyberattaques. À cet égard, plusieurs intervenants ont souligné l'importance d'une défense dite « en profondeur ». Il s'agit concrètement de multiplier les lignes de défense, l'objectif étant de rendre aux assaillants la tâche plus complexe. Cette stratégie en termes de structuration de systèmes se double d'une meilleure formation des personnels : comportements vertueux, dispersion des données, choix de mots de passe uniques et forts, sauvegarde selon la technique dite du « 3-2-1-0 ». Les conseils divulgués, parfois redondants au cours du colloque, rappellent néanmoins la vertu d'adopter des règles d'hygiène pour éviter toute forme d'intrusion, décrite au moyen d'une sémantique médicale comme une contamination (la métaphore de la gastro-numérique » avait été donnée).

De telles règles d'hygiène élémentaire se doublent d'un changement de posture des victimes. Même si l'idée selon laquelle les attaques numériques ne concernent « que les autres » prédomine encore, l'activité du site cybermalveillance.fr reflète malgré tout un changement de comportement. Les individus dénoncent plus facilement les faits et les victimes rapportent plus aisément les actes malveillants.

Ce changement est relatif à un phénomène dit d'« acculturation » (ce thème ayant été employé à de multiples reprises par divers intervenants) de la part des citoyens certes, mais aussi du monde de l'entreprise. Les acteurs de celui-ci adoptaient classiquement deux attitudes :

- Le déni du risque : un chef d'entreprise prenant par définition des risques, le cyber-risque est perçu comme un risque quelconque pesant sur l'activité économique (deux intervenants différents avaient déploré que, suite à une attaque par ransomware, les rançons étaient payées par les chefs d'entreprises victimes désireux de reprendre au plus vite cette activité, ceux-ci ayant intégré les coûts de telles attaques dans leur comptabilité). Cette perception limitée du risque est renforcée par le fait que les dommages sont purement matériels et les attaques de nature virtuelle au sens où elles sont issues du monde numérique par opposition au monde réel (les dommages causés à un serveur étant moins traumatisants qu'un cambriolage). Enfin, la cybersécurité est une variable d'ajustement en cas de processus de réduction des coûts (à l'avantage, le cas échéant, selon un autre intervenant, de secteurs jugés prioritaires, le marketing ou la communication par exemple),
- Le recours au « minimum syndical » : de manière à répondre aux prescriptions du RGPD ou aux demandes des clients (par exemple dans le cadre d'un contrat de sous-traitance), une société se contentera d'effectuer des efforts minima de manière à répondre aux exigences imposées, sans percevoir la cybersécurité comme un enjeu en tant que telle. Celle-ci se limite à un ensemble de prescriptions réglementaires ou figurant dans un cahier des charges. La cybersécurité se révèle à ce sujet, lourde à mettre en œuvre. Un intervenant avait souligné la paperasserie générée par le RGPD, perçu comme un fardeau supplémentaire pour les entreprises.

Or progressivement, plusieurs intervenants ont noté, une fois encore, un changement de posture :

- La perception de la cybersécurité comme une opportunité économique : le respect strict du droit numérique, la mise aux normes et le caractère « RGPD-comptatible » d'une entreprise sont garants d'une confiance accordée par les partenaires, de même qu'un moyen de gagner des appels d'offre publics,
- La sensibilisation au risque progresse. Non seulement la règlementation impose parfois de déclarer les risques, mais de surcroît, la répétition des attaques est de nature à nuire à l'image de l'entreprise désormais jugée non fiable par ses partenaires. Par conséquent, les investissements réalisés en matière de cybersécurité (achat de matériels certifiés et souscription d'un contrat d'assurance spécifique) sont de nature à la fois à rassurer ces partenaires et préserver la réputation de l'entreprise.

Selon un intervenant, ce changement est observable dans le monde de l'assurance. Des produits spécifiques se développent (les mécanismes de quantification des risques s'affinant) et se vulgarisent (les assureurs prenant eux-mêmes conscience de l'intérêt de proposer ces produits aux entreprise).

De surcroît, un tel changement est observable parmi les autorités publiques qui travaillent :

- davantage entre elles (par exemple Cybermalveillance avec la police judiciaire) aux fins de transmission de l'information sur les attaques,
- étroitement avec les entreprises de manière à ce que, à l'issue d'une attaque (par exemple un cyberrançonnage), une enquête menée, et qui amène à figer la scène de crime, n'entrave pas pour autant la reprise d'activité.

De manière plus générale, un mouvement de fond de collaboration, visant apporter un niveau de confiance indispensable en matière économique, s'instaure entre les acteurs du monde numérique, et entre eux et les autres (par exemple les entreprises, les acteurs du monde de la mer, puisqu'un aspect de ce colloque porte sur ce thème). La « co-construction de la sécurité » a été rappelée par un intervenant. Cette collaboration à tous les niveaux se traduit par une intervention des autorités publiques et des acteurs privés toujours plus structurée :

- L'édiction de normes techniques par l'AFNOR (sur la Blockchain, la cybersécurité, les avis clients en ligne et la protection des données personnelles) ainsi que par l'ANSSI (qui délivre ainsi une certification et une qualification de sécurité des équipements industriels),
- L'édiction de normes législatives par l'État et l'Union européenne (telles que la directive sur la sécurité des réseaux et des systèmes d'information (directive dite « SIR » ou « NIS »), ou le RGPD).

Cette co-construction déborde largement le champ économique pour aller sur le terrain social. Les investissements en matière d'inclusion numérique, en particulier pour lutter contre l'« illectronisme » et faire en sorte que les populations les plus fragiles soient elles aussi protégées. L'objectif est que ce public soit, à travers une action partenariale, en mesure d'assurer toute opération sur internet en toute sécurité (transactions financières par exemple), mais aussi que les rapports avec les organismes de différente nature (administrations d'État ou structures privées, telles que les banques) se déroulent en toute confiance à l'heure où de tels rapports se dématérialisent toujours plus.

Cette action menée contre l'« illectronisme » rappelle, dans cette perspective de lutte contre l'exclusion numérique, que l'être humain est la finalité de la cybersécurité. Il est possible d'aller plus loin en considérant qu'elle est modelée par une morale humaniste.

2.2 L'individu valorisé, la cybersécurité modelée par une morale humaniste

« Le problème n'est pas de savoir si oui nous voulons du numérique ou non, mais de quel type de numérique nous désirons ». Par ces propos, un intervenant rappelle que la cybersécurité implique des choix moraux en matière de protection. Un autre avait souligné le vœu des individus d'une sécurité « ici et maintenant ». Cette soif de sécurité s'illustre tout particulièrement en matière terroriste. La moindre attaque se traduit par une « panique morale » définie par Stanley Cohen comme une forme d'hystérie collective découlant d'un évènement médiatique et générant une onde de choc intense parmi l'opinion publique, dont l'interprétation est effectuée sous un angle moral[6]. Ce phénomène s'exprime, en écho aux travaux du criminologue Davis Garland, par un désir de vengeance à l'égard des auteurs des attentats, ceux-ci devant être rapidement et durement châtiés, ainsi que par une pression intense exercée sur les autorités publiques : l'État, garant de la sécurité, est immédiatement déclaré coupable de défaillance et les leaders politiques qualifiés rapidement d'irresponsables, lorsque ces auteurs ne sont pas trouvés sur le champ, leur démission étant alors exigée.

Or, cette soif irrépressible de sécurité se retrouve en matière de cybersécurité. Elle pose des interrogations dans le domaine des libertés. Citant le Président de la République, un intervenant avait évoqué le « mais en même temps » de la cybersécurité : garantir la sécurité tout préservant les libertés.

Une telle articulation de valeurs antagoniques est évoquée dans le débat sur l'intelligence artificielle, puisqu'il s'agit de définir un modèle de société à l'ère numérique. Un intervenant avait identifié deux pôles correspondant au célèbre panoptique identifié par Jeremy Bentham : l'individu serait soumis à deux types distincts de surveillance, rappelant le modèle carcéral décrit par le célèbre philosophe anglais : une surveillance privée américaine d'un côté essentiellement à vocation marchande mais susceptible de dérives par ses utilisations en vue d'influencer les comportements, une surveillance publique chinoise, inspirée par une volonté de contrôle social de la part des autorités de l'autre. Ces deux types se traduisent, d'après cet intervenant, par deux modèles distincts : une «

[6] S. Cohen, *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, Londres, Routledge, 2011 [1972].

sécurité surveillée » opérée par le gouvernement chinois et réalisée avec l'appui du secteur privé d'une part, et une « liberté épiée » effectuée par les GAFAM américains avec une forme de contrôle social exercée par la communauté des réseaux sociaux et jusqu'ici une connivence des autorités publiques d'autre part. Les scandales médiatiques découlant des affaires dites « Snowden » et « Cambridge Analytica » ont conduit les Européens, toujours selon ce même intervenant, à opter en faveur d'un modèle singulier : celui de la « liberté sécurisée ». Les Institutions européennes s'efforcent de donner vie à ce modèle, qui concilierait la liberté « mais en même temps » la sécurité, par le biais d'une gouvernance par la règle, en d'autres termes par la mise en place d'un cadre réglementaire approprié dont le RGPD constitue une étape importante.

En matière numérique, le droit est vecteur de régulation et ceci, en dépit du fait que la « cyberspacialisation »[7] tende à redéfinir la norme juridique. Or, « le droit prend l'escalier… et il prend celui le plus tordu » avait déclaré un autre intervenant constatant les circonvolutions juridiques en matière d'intelligence artificielle (observations faites, au demeurant, par un autre intervenant encore sur le RGPD). Ce constat n'empêche pas des évolutions importantes, avec retard certes, mais notables malgré tout. De nombreux participants du colloque s'accordent ainsi sur les bienfaits du droit européen de la protection des données, devenant un modèle de préservation de la vie privée qui s'exporte dans le monde et ceci, en dépit du phénomène planétaire « désoccidentalisation des valeurs » selon l'un d'entre eux.

Au sujet des valeurs qui surplombent toute société, le débat sur l'intelligence artificielle a mis en exergue l'importance de l'éthique[8]. De nombreux intervenants de cette table ronde de l'IA se sont félicités de l'instauration de règles éthiques visant à régir celle-ci, dans le cadre soit d'une auto-régulation, soit d'une réglementation publique. En tout état de cause, tous ces intervenants ont, à des degrés divers, mis en exergue le fait que le numérique devait être conditionné par des valeurs humanistes.

Au fond, ce colloque a permis de faire ressortir une certaine conception de l'homme. Alors que celui-ci apparaissait comme une menace pour ses congénères (au sein de cette « anarchie hobbesienne numérique »), il est malgré tout un point d'aboutissement. Certes, la cybersécurité vise à sécuriser l'homme (y compris l'homme dans toute sa fragilité, en témoigne les efforts menés en matière d'inclusion numérique). Cependant, l'être humain se révèle être surtout une finalité. Dans cette perspective téléologique, l'homme apparaît comme un horizon à atteindre, un idéal, au sens où tant la cybersécurité que l'intelligence artificielle (l'un et l'autre tendant au demeurant à converger), sont modelés par une morale humaniste.

Conclusion

Cette vision humaniste de la cybersécurité, produit d'une pensée rappelant celle de Descartes sur l'humanisme philosophique, ou de celle Kant sur l'éthique déontologique, qui ressort particulièrement de la table ronde sur l'intelligence artificielle, mérite d'être appréciée à la lumière de la pensée d'un autre philosophe, Hans Jonas. Dans son ouvrage *Le principe de responsabilité* (*Das Prinzip Verantwortung*), celui-ci avait proposé une doctrine morale renouvelée questionnant la technologie

[7] P. Trudel, « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et société*, vol. 32, n° 2, 2000, p. 189-207 (p. 190).

[8] Et pour approfondir la question, M. A. Boden (dir.), *The Philosophy of Artificial Life*, Oxford, Oxford University Press, 1996 ; P. Boddington (dir.), *Towards a Code of Ethics for Artificial Intelligence*, Berlin, Springer, 2017.

contemporaine, source de destruction de l'homme et de l'environnement[9]. Or, les débats sur l'éthique de la cybersécurité et de l'IA sont sous-jacents d'un questionnement philosophique autour de l'urgence climatique. En effet, il ressort que pour bon nombre d'intervenants, ni la cybersécurité, ni l'IA ne sont une avancée en soi, manifestation tangible du progrès, entendu comme mythe gouvernant les civilisations occidentales. L'humanité se trouve confrontée à de nouveaux défis environnementaux, en premier lieu le réchauffement climatique. Si la cybersécurité constitue un problème (les technologies déployées contribuant à l'aggravation du problème), elle est également un remède. Pour autant, il ressort des travaux que les solutions préconisées par divers intervenants soulignent que les politiques publiques (l'un évoquant ainsi les choix des collectivités territoriales) et les outils numériques (l'autre évoquant, par exemple, le fait que la cybersécurité servirait à contrôler des libertés désormais restreintes au nom de cette urgence climatique) étaient mis à disposition d'une finalité supérieure, en l'occurrence la préservation de l'environnement. Les propos tenus font précisément écho à cet humanisme moral à l'aune de ce *Principe de responsabilité* : l'homme définit des devoirs ainsi que des interdits éthiques de manière à ce que ses actions soient, comme le rappelle Jonas, « compatibles avec la permanence d'une vie authentiquement humaine sur Terre ».

[9] H. Jonas, *Le principe de responsabilité : Une éthique pour la civilisation technologique*, Paris, Flammarion, coll. Champs [1979].