Sécurité Globale
HORIZONS STRATÉGIQUES
HORS SERIE

ANSSI – XE ANNIVERSAIRE

Agence Nationale de la Sécurité des Systèmes d'Information

- Perspectives et défi d'une deuxième décennie – Guillaume Poupard
- Cyber-sécurité et monde digital du XXIe siècle
- L'âge du cyber et de la neuro-diversité
- Sujet administratif et e-gouvernement
- Ethique et numérique

Editions ESKA

NUMERO SPECIAL

INTRODUCTION

Perspectives et défis d'une deuxième décennie

Guillaume POUPARD[1]

A l'origine était le chiffre... C'est par ces mots que pourrait commencer la nouvelle décennie dans laquelle entre l'ANSSI, ouvrons nous vers le futur certes, mais d'où venons-nous ?

Les racines les plus anciennes de l'Agence et de la sécurité des systèmes d'information se trouvent dans la cryptographie. Richelieu déjà hésitait pas à dire que « savoir dissimuler est le savoir des rois ». Il s'attacha ainsi les services d'Antoine Rossignol, spécialiste en cryptographie, pour créer le «bureau de la partie secrète», premier service du chiffre en Europe. Ce serait notre plus lointain ancêtre institutionnel. Le plus proche date quant à lui de 1943. C'est à ce moment-là, en plein second conflit mondial que le Général de Gaulle, décide depuis Alger de poser une nouvelle doctrine : la création et la définition du chiffre sera confiée à un organe interministériel, la direction technique des chiffes, l'attaque (interception et cassages des codes adverses) revenant au BCRA, rapidement transformé en DGSS/DGER, dont descendent en ligne directe le SDECE puis la DGSE. Séparation de la Défense et de l'attaque. Les bases de notre doctrine sont posées et restent d'actualité.

Bien sûr au fur et à mesure des années l'évolution des technologies, l'essor de la numérisation et sa démocratisation ont dû être pris en compte. Notre écosystème a évolué, s'est développé. Cela se ressent dans les intitulés : Service Central Technique du Chiffre, Service Central des Chiffres et de la Sécurité des Télécommunications, Service Central de la Sécurité des Systèmes d'Information, Direction Centrale de la Sécurité des Systèmes d'Information et enfin Agence Nationale de la Sécurité des Systèmes d'Information. La crypto s'est fondue dans la sécurité des systèmes d'information, qui elle-même constituera plus tard une partie des concepts encore plus larges de cybersécurité ou de sécurité numérique.

© Editions ESKA

De cette séparation de l'offensif et du défensif découle notre posture : « La meilleure défense c'est la défense ».

Et cette posture doit être permanente. En effet, pour qui en doutait encore, le début de l'année 2019 est bien dans la continuité inquiétante de l'année 2018. Ces cinq premiers mois ont une nouvelle fois montré que la menace numérique n'est pas éthérée, et que les défis pour la sécurité et la stabilité du cyberespace restent immenses. Plus sophistiquées, mieux élaborées, plus destructrices et touchant désormais toute la société, du citoyen à la grande entreprise jusqu'à nos institutions démocratiques, les attaques informatiques sont entrées dans une dimension nouvelle.

Tous connectés, tous concernés, tous responsables : voilà l'approche fondamentale que nous nous efforçons de porter. La sécurité doit sortir de son domaine réservé pour associer l'ensemble des architectes de la société numérique. Car au-delà des menaces sur la société, l'économie, la souveraineté et la stabilité du cyberespace, il en va du développement même des technologies. En effet, les formidables usages rendus possibles par le numérique ne pourront être durables que s'ils recueillent la confiance des utilisateurs.

Cela implique tout d'abord de changer de regard sur la cybersécurité. Celle-ci ne peut plus être appréhendée uniquement comme un poste de coût ou un « patch » appliqué en bout de course de l'innovation. Interrogez les experts de l'ANSSI : la cybersécurité constitue en elle-même un champ d'innovation passionnant, d'une grande richesse scientifique, profondément transdisciplinaire et associant une grande variété d'acteurs, privés et publics, en France comme à l'international. Elle pose des défis intellectuels majeurs pour les innovateurs de tous bords.

Machine learning, santé connectée, informatique quantique… comment sécuriser les technologies de demain ? Le véhicule autonome et connecté, qui a connu des progrès majeurs ces dernières années, offre une bonne illustration de cette imbrication des usages et des impératifs de sécurité. La présence de voitures sans conducteurs sur nos routes reste en effet largement conditionnée à d'impérieuses questions de confiance et d'acceptabilité sociale. Or beaucoup reste à faire : le système de reconnaissance de ces véhicules peut encore être facilement berné par une altération légère des panneaux de signalisation, les conduisant à confondre les panneaux « stop » et « route prioritaire ».

Si ces défis concernent naturellement les ingénieurs, les artisans des politiques publiques, du droit et des relations internationales ne sont pas en reste. Comment œuvrer à la stabilité du cyberespace ? Doit-on permettre aux acteurs privés de se faire justice eux-mêmes, de riposter aux attaques dans un contexte où les entreprises deviennent elles-mêmes des « champs de bataille » ? La stabilité du cyberespace est un sujet qui bouscule les habitudes politiques, diplomatiques et militaires. Les questions sont nombreuses et les perspectives excitantes, passionnantes, structurantes.

Ingénieurs, juristes, designers, experts en politiques publiques, en relations internationales, ergonomes, startups, grands groupes, citoyens… la sécurité du numérique est définitivement l'affaire de tous.

Faire comprendre cette nécessité à tous est devenu un des axes d'effort de l'Agence. Pour remplir cette mission de sensibilisation quotidienne, l'ANSSI peut s'appuyer notamment sur l'action de ses délégués régionaux, sorte de frères convers, mais il est aussi nécessaire d'appréhender cette cybersécurité de manière plus prospective. C'est ainsi qu'a été créé il y a neuf mois l'Agora des 41.

L'Agora 41 est avant tout une tribune d'expression libre, multidisciplinaire qui propose à ses membres d'étudier des thématiques liées au numérique. Pour mener une réflexion transverse et innovante, l'Agora tire parti de la diversité des personnalités bénévoles qui la composent. Ce sont donc ses membres qui la font vivre grâce à un travail commun et ouvert sur des thématiques transverses.

Animée par l'ANSSI, les différentes rencontres qui ont déjà eu lieu ont permis à cette assemblée disparate de se constituer, aux membres de se connaitre et de partager leurs expériences.

Les échanges sont structurés sous forme de groupes de travail thématiques. Chaque membre a ainsi choisi un des 5 sujets proposés par l'ANSSI, qui ne couvrent pas son périmètre d'action :

- L'imaginaire : À la différence d'autres domaines technologiques (l'exploration spatiale, le monde du enseignement, la robotique, etc.), le numérique et plus particulièrement la cybersécurité n'ont pas (encore) conduit à l'émergence d'un imaginaire collectif Français ou Européen. Comment pourrait émerger une vision mobilisatrice ?
- La régulation du cyberespace : La transformation numérique de la société et de l'économie repose sur un écosystème numérique innovant, où les acteurs privés transnationaux occupent une place prépondérante. Faut-il co-réguler avec les géants du numérique ?
- Les Talents : la sécurité est l'un des piliers de la confiance nécessaire à la transformation numérique. Entreprises, administrations et collectivités ont une conscience croissante des risques et de la nécessité de renforcer leurs capacités pour y faire face. Si elles sont le nerf de la guerre, les ressources humaines sont pourtant l'un des points faibles de la démarche de renforcement de la sécurité numérique. Comment relever le défi de la formation aux métiers de la sécurité numérique ?
- Le Cyber moi : depuis plusieurs années les frontières entre monde « réel » et univers numérique tendent à disparaitre. Cette dynamique impacte également l'individu dans son quotidien et son identité. Comment envisager cette évolution vers une « cohabitation cordiale » entre l'individu et son cyber-moi, au niveau éthique, de la protection physique et des aspects identitaires.
- L'Ecosystème : Facteur (et acteur) de succès de la transformation numérique, la sécurité numérique est l'affaire de tous : utilisateurs individuels, entreprises, administrations et collectivités. Une interconnexion qui doit s'affirmer pour relever les enjeux communs de la sécurité du numérique. Quels facteurs clés pour la constitution d'un écosystème de la sécurité numérique cohérent et mobilisé ?

Les fruits de leurs réflexions seront destinés à être partagés publiquement au sein de l'écosystème de la transformation numérique mais également plus largement avec toute personne intéressée par les enjeux du numérique.

Le cahier de ce numéro consacré aux dix ans de l'Agence choisit lui aussi, comme le cyberfestival de soulever des problématiques tournées vers le futur : la cybersécurité pour un monde de plus en plus digital, le cyber et la neurodiversité, le moi administratif à l'aune des e gouvernements et enfin....

Les articles ont tous été rédigés bénévolement par des membres de l'Agora. Qu'ils en soient chaleureusement remerciés.

Note

1. Directeur général de l'ANSSI.

Revisiter l'idée de cybersécurité pour le monde digital du 21e siècle

Hélène LAVOIX[1]

Le monde fait l'objet d'une digitalisation croissante. Le numérique est omniprésent, pour tous les acteurs, dans tous les domaines de la vie, comme souligné dans la *Revue stratégique de cyberdéfense* de février 2018.

Il est donc crucial de prendre en compte ce changement en ce qui concerne la cybersécurité. Nous devons, en effet, nous assurer que cette omniprésence est bien intégrée par la notion de cybersécurité et idées connexes.

Nous verrons donc tout d'abord comment la digitalisation du monde nous demande de dépasser l'idée actuelle de cybersécurité, et comment ce changement doit être opéré de façon impérative par les autorités politiques, puisqu'il met en jeu leur légitimité. Nous nous tournerons ensuite vers la façon dont l'espace où opèrent les opérateurs de cybersécurité évolue, le cyberespace devant maintenant aussi prendre en compte le lien entre le digital et le matériel ou physique, alors que les cyber attaques peuvent aussi devenir létales. Finalement, nous soulignerons que les entreprises commerciales, elles aussi, doivent faire face aux mêmes évolutions, sont des acteurs indispensables de la nouvelle cybersécurité et pourraient également développer une vision et pratique nouvelle de cybersécurité élargie.

Vers une nouvelle compréhension de la cybersécurité

Digitalisation du monde et cybersécurité technique

La cybersécurité a été, jusqu'à présent, définie comme un secteur spécifique, expert, ou technique, et pensée comme concernant la sécurité des systèmes d'information. Ainsi, l'ANSSI la définit comme un "État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre

© Editions ESKA

la cybercriminalité et sur la mise en place d'une cyberdéfense" (site internet, 2018).

Microsoft, pour prendre l'exemple d'un des géants américains des technologies de l'information utilise une définition similaire. La cybersécurité est "la protection de systèmes connectés et réseaux, et des données stockées sur ces systèmes et transférés via ces réseaux, d'attaques, dommages ou accès non autorisé" (Cybersecurity Policy Framework).

Cette approche reste, bien entendu, vraie, mais, elle fut créée pour un monde passé, où les systèmes d'information étaient certes importants mais n'avaient pas envahi chaque espace et chaque geste de la vie.

Or, maintenant et de façon croissante, chaque instant, chaque acte de la vie des citoyens et des acteurs économiques inclut un recours à la numérisation ou même dépend de cette dernière. La digitalisation n'est plus limitée à quelques acteurs individuels privilégiés et à la pointe du progrès ou à de grosses entreprises, comme cela pouvait être le cas il y a vingt ans ou même dix ans. La numérisation fait maintenant partie de la trame même du tissu social, elle régit les relations économiques et est un médium essentiel du lien entre l'Etat et les citoyens, de la fiscalité à la santé.

Cette digitalisation généralisée demande donc qu'à l'idée de cybersécurité technique soit ajoutée une perspective de cybersécurité élargie qui corresponde justement à la réalité du monde présent et futur.

L'expertise qui s'est construite jusqu'à présent sur la cybersécurité technique sera un des piliers qui permettra de construire et de maintenir une nouvelle cybersécurité élargie.

Vers une définition de la cybersécurité élargie, pour les autorités politiques

Cette cybersécurité élargie se comprend comme l'état d'un monde digitalisé bénéficiant de sécurité. La sécurité est, d'ailleurs, la mission principale des autorités politiques d'une société. Ces autorités politiques sont comprises comme un certain système d'Etat, un régime et un gouvernement, quelques soient les formes spécifiques prises par chacun[2].

C'est d'ailleurs parce que la sécurité est la mission principale des autorités politiques et parce que, donc, l'assurer conditionne la légitimité de ces autorités, que l'élargissement de la définition de cybersécurité est un impératif.[3]

Brièvement, nous rappellerons que la sécurité, au coeur du contrat social entre "dirigés" et "dirigeants" se décline autour de trois grands axes[4] :

- Protection des ennemis étrangers (c'est à dire ceux qui sont extérieurs à la sphère du nous) ;
- Maintenance de la paix et de l'ordre ;
- Contribution à la sécurité matérielle, c'est à dire "sécurité contre des menaces super-naturelles, naturelles et humaines à la provision de nourriture et autres supports de la vie quotidienne coutumière".

Par ailleurs, utilisant la définition du Larousse, la sécurité est "la situation de quelqu'un qui se sent à l'abris du danger,

qui est rassuré". Nous avons donc ici à la fois une réalité objective et une impression subjective, qui, toutes deux, constituent des éléments cruciaux de la sécurité.

Donc, pour les autorités politiques et leurs agents, la cybersécurité devient une situation où les "dirigés" sont non seulement à l'abri du danger, mais également se sentent comme tels dans leurs interactions impliquant et/ou nécessitant une digitalisation, et ce tant dans le cyberespace que dans l'espace réel ou plus exactement physique ou matériel.

Cyberespace et lien cyberespace – espace physique/matériel

L'ANSSI définit le cyberespace comme "l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques."

Afin de faciliter plus avant la compréhension et l'action, il semble utile d'ajouter à la définition du cyberespace sa caractérisation par Olivier Kempf : le cyberespace peut se concevoir selon un modèle en trois couches : l'infrastructure, la couche logique (les logiciels) et la couche sémantique.[5]

Prendre en compte l'aspect sémantique, en effet, est crucial compte tenu notamment de la multiplication des possibilités de propagande d'une part, de rumeurs d'autre part - redécouvertes sous le vocable de "fake news", du fait de la digitalisation.

La cybersécurité devra donc être assurée dans ces trois dimensions du cyberespace. Qui plus est, compte tenu des interactions grandissantes entre cyberespace et monde physique, du fait notamment de la numérisation il devient impossible de ne regarder que la cybersécurité au sein du cyberespace.

En effet, pour pouvoir assurer pleinement une cybersécurité élargie, il faut dorénavant, en vertu des interactions grandissantes avec le monde physique, non seulement traiter du cyberespace, mais aussi prendre en compte l'espace matériel ou physique - comme d'ailleurs lorsque la dimension infrastructurelle du cyberespace est considérée - ainsi que l'imbrication entre digital et matériel.

Notamment, il n'est plus vrai que les interactions dans le cyberespace ont un caractère de non-létalité, comme l'imaginait déjà d'ailleurs Olivier Kempf en 2013 en réduisant son propos de non-létalité des cyber-attaques à un temps spécifique. D'ailleurs, par example, le Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC) de la Defense Threat Reduction Agency (DTRA) a publié un appel à projet en mars 2018 pour l'année fiscale 2019, où, entre autre, le gouvernement américain recherche une évaluation de la façon dont l'internet des objets commercial pourrait éventuellement impacter les capacités américaines à lutter contre les armes de destruction massive. Comme autre exemple, on peut également imaginer que des groupes terroristes cherchent à commettre des actes de cyber-malveillance ayant pour but d'utiliser des voitures autonomes comme armes.

Des exemples moins extrêmes mais également disruptifs démontrant le lien entre réalité physique et cyberespace vont de

l'impact d'actes de cyber malveillance affectant les marchés financiers et donc les entreprises, à ceux affectant la réputation de citoyens, en passant par le vol d'identité. En décembre 2018, un journal anglophone, Business Insider publiait un article rappelant les dommages qui pourraient résulter de ceux qui réussiraient à mettre un pays "offline"[6]. Ces exemples peuvent se multiplier presqu'à l'infini.

Cybersécurité et sociétés commerciales

Il importe également de garder à l'esprit que, dans un monde digitalisé et compétitif, pouvoir continuer à utiliser au mieux cette digitalisation fait aussi partie de la cybersécurité élargie.

Si les autorités politiques doivent assurer les conditions de cette cybersécurité, comme vu ci-dessus, elles ne peuvent le faire qu'avec les agents économiques.

Les sociétés commerciales devront donc interagir avec les autorités politiques au sujet de la cybersécurité élargie publique, comme cela est le cas, par exemple dans le cadre des opérateurs d'importance vitale (OIV).[7]

Qui plus est, elles devront assurer la partie privée de leur cybersécurité. Faisant face aux mêmes évolutions du monde que les autorités politiques, donc à la même digitalisation omniprésente, l'idée de cybersécurité utilisée par les sociétés commerciales doit de la même façon être élargie pour dépasser celle de la seule sécurité des systèmes d'informations.

Nous nous bornerons ici à définir et donner les premiers jalons de ce que devrait être la cybersécurité élargie commerciale.

La différence principale entre une compagnie privée et une autorité politique est que l'entreprise n'a pas pour mission primordiale la sécurité des "dirigés" mais, dans des systèmes capitalistes comme ceux qui régissent le monde, le profit, ou, tout du moins, la pérennisation d'une activité profitable.

Si l'entreprise n'a pas à assurer sa fonction et sa légitimité auprès des "dirigés", elle n'en a pas moins à faire face à un impératif crucial, qui est, au pire, celui de sa survie en cas d'inadaptation au monde. Donc, si les enjeux sont différents ils n'en sont pas moins cruciaux.

Donc, pour une entreprise commerciale, la cybersécurité élargie devient l'état d'un monde digitalisé (le monde de cette entreprise) bénéficiant de sécurité, y compris pour la réussite de son objectif principal. Cela signifie que "le monde de cette entreprise" est non-seulement à l'abri du danger mais également que ceux qui y évoluent se sentent comme tels, notamment dans le cadre de leur travail, dans leurs interactions impliquant et/ou nécessitant une digitalisation, et ce tant dans le cyberespace que dans l'espace physique ou matériel.

Les trois domaines de sécurité utilisés pour les autorités politiques pourront également être adaptés pour les acteurs commerciaux privés :

- Protection des acteurs extérieurs (y compris étrangers - par exemple protection de l'espionnage industriel) ;

- Maintenance de la paix et de l'ordre (à l'intérieur, en fonction du cadre légal) ;
- Contribution à la sécurité matérielle des employés, en fonction du cadre légal.

De la même façon, le cyberespace devra être compris par les entreprises dans ses trois dimensions, et les liens digital-matériel devront être spécifiquement inclus dans le champ de la cybersécurité.

La diversité des entreprises nécessitera d'adapter ce cadre général à la spécificité de chacune.

La numérisation croissante du monde nous présente donc avec un nouvel impératif, celui de redéfinir ce que nous entendons par cybersécurité. Cette re-conceptualisation doit s'opérer tant au niveau des autorités, que de la compréhension de l'espace dans lequel les acteurs de la cybersécurité évoluent qui n'est plus seulement digital mais et digital et physique, que des entreprises, qui elles aussi vont avoir opérer un changement profownd. L'adoption, qui sera certainement progressive, de cette nouvelle idée de cybersécurité élargie sera également une opportunité pour ceux qui l'utiliseront pour forger les cadres de pensée et les outils idoines de demain.

Notes

1. Hélène LAVOIX est titulaire d'un doctorat en sciences politiques et relations internationales de la School of Oriental et African Studies de l'Université de Londres et a suivi les cours de l'Institut supérieur de commerce dont elle est sortie major en 1987.Depuis, elle partage ses activités entre Sciences Po Paris (Paris School of International affairs) où elle enseigne en tant que professeur vacataire depuis 2015 et le cabinet qu'elle a créé en 2013, The red team analysis society (RTAS). Ce cabinet est dédié à la prospective stratégique, aux systèmes d'alerte précoce et aux enjeux de sécurité conventionnels ou non.
2. Parmi bien d'autres, Max Weber, Le savant et le politique, (Paris : 10/18, 1963) originally «Wissenschaft als Beruf » & « Politik als Beruf » 1919; John S. Migdal, Strong societies and weak states : state-society relations and state capabilities in the Third World (Princeton: Princeton University Press, 1988); Barrington Moore, Injustice: Social bases of Obedience and Revolt, (London: Macmillan, 1978); John Nettl, "The state as a conceptual variable," World Politics, vol. XX, N° 4, July 1968, pp. 559-592; Thomas Ertman, Birth of the Leviathan: Building States and Regimes in Medieval and Early Modern Europe. Cambridge, UK ; New York: Cambridge University Press, 1997. Helene Lavoix,"Identifier L'État Fragile Avant L'Heure: Le Rôle Des Indicateurs De Prévision", Edited volume, Etats et Sociétés fragiles (Agence Française de Développement and French Ministère des Affaires Etrangères) – January 2007.
3. Ibid.
4. Barrington Moore, Injustice...
5. Olivier Kempf, "Stratégie du cyberespace", La Revue Géopolitique, 13 février 2013.
6. Jim Edwards, "Someone is trying to take entire countries offline and cybersecurity experts say 'it's a matter of time because it's really easy'", Business Insider, 22 Dec 2018, consulté le 4 janvier 2019 https://www.businessinsider.fr/us/can-hackers-take-entire-countries-offline-2018-12
7. "L'article R. 1332-1 du code de la défense précise que les opérateurs d'importance vitale sont désignés parmi les opérateurs publics ou privés mentionnés à l'article L. 1332-1 du même code, ou parmi les gestionnaires d'établissements mentionnés à l'article L. 1332-2. Un opérateur d'importance vitale : exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ; gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population." ANSSI.

L'Âge du cyber et la neuro-diversité

Hugo HORIOT[1]

Certains diront qu'il est sans foi ni loi, d'autres qu'il change les règles. Le cyber univers ne connait aucune limite et abolit les frontières. La cyberpuissance de Pékin déroule ses ambitions sur la route de la soie. Contrôle rigoureux des médias, vols de technologies et espionnage industriel, nos démocraties semblent comprendre à leur dépend si ce n'est savoir déjà, que leurs données sensibles sont en péril, mais surtout qu'elles ont un prix. Fatal. Celui de leur existence. La révolution numérique bouleverse nos champs de bataille, notre économie et nos modes de vie. Après l'âge de pierre, du fer et du bronze, l'imprimerie et trois révolutions industrielles, voici notre temps, celui d'un nouvel âge de la guerre : la cyberguerre. Alors que s'opposent dans nos rues les pavés aux grenades, les transpalettes aux portes des ministères et le pillage au capitalisme, d'autres étendent leur souveraineté numérique et *construisent « une communauté de destins pour l'humanité »*.

La cyber-époque

La quatrième révolution industrielle expose à des troubles inconnus, annonce de nouveaux dangers, ouvre de nouveaux horizons et crée de nouvelles opportunités. Le marché de l'Union Européenne où se disputent les géants des BATX et des GAFAM, comptera quelques dizaines de milliards d'objets connectés d'ici 2020. 69 % des entreprises n'ont qu'une compréhension de base, ou n'ont pas de compréhension de leur exposition aux cyber-risques. 51 % des Européens se sentent peu informés au sujet des cyber menaces. Les attaques informatiques au moyen de rançongiciels ont triplé entre 2015 et 2017. Les effets de la cybercriminalité sur l'économie ont été multipliés par cinq depuis 2013 et on estime que les cyberattaques coûtent quelque 400 milliards d'euros par an à l'économie mondiale. (source : Conseil Européen)

L'arsenal informatique en Europe ne peut se permettre d'être une passoire ! Or en Allemagne, un autodidacte désœuvré de 20 ans parvient à déstabiliser la démocratie. Dans un monde où il n'y a pas d'amis, un monde connecté où il n'y a que des contacts, un monde peuplé d'alliés temporaires, de partenaires et d'adversaires, nos Chefs d'État sont sur écoute. Dans ce nouvel âge de la guerre, la Chine, la Russie et les États-Unis

© Editions ESKA

éprouvent sans relâche nos secrets, nos défenses, nos démocraties et la garantie de nos intérêts dans le monde.

La bombe nucléaire était l'arme de dissuasion massive du XXe siècle. La cyberguerre est l'enjeu géo stratégique du XXIe siècle. La sauvegarde de nos droits fondamentaux et de nos libertés individuelles semble fragile. Voici qu'elle repose sur notre seule aptitude à l'échelon national comme à l'échelon européen à sécuriser nos systèmes d'information au sein du cyberespace.

La création, la maîtrise et le développement d'une technologie, aussi perfectionnée soit-elle, dépend toujours d'humains. Dans une atmosphère tendue et incertaine et devant l'urgence de la situation, gouvernements et entreprises se livrent sans merci à une guerre des talents. On évoque souvent la pénurie de main d'œuvre engendrée par ce contexte de profonde mutation, lequel exige de nouvelles compétences, balaie des emplois et en crée d'autres : Ingénieur en cryptographie appliquée, ingénieur test et validation, veilleur de permanence opérationnelle, analyste des modes opératoires en cyberattaques, développeur (SDN et SDO), analyste des vulnérabilités et codes malveillants, Analyste sécurité en détection d'intrusions, Architect en Big Data, Auditeur technique, Expert en sécurité des radiocommunications cellulaires, expert en analyse des protocoles de communication, expert en sécurisation des composants...

La guerre des talents

Selon une récente enquête, les employeurs sont désormais 54% à investir dans des plateformes d'apprentissage et des outils de développement pour construire leur propre vivier de talents, alors qu'ils n'étaient que 20% à s'inscrire dans cette démarche en 2014. Des milliards d'euros sont investis pour multiplier les formations aux nouveaux métiers du numérique et les rendre accessibles à un maximum de monde. On souligne, de plus en plus et à raison, l'importance de veiller à la diversité du personnel et notamment, par le biais de la parité, à la féminisation des emplois techniques liés à ce nouveau secteur.

Face à des situations nouvelles, incertaines et complexes, pour atteindre un résultat précis contre la montre, un groupe doit avoir la capacité en un temps minimum de formuler et d'exécuter une stratégie. Face à conditions, il est prouvé que les équipes diversifiées en termes d'âge, d'origine ethnique et de sexe, sont d'avantage susceptibles d'être créatives et productives. Mais jusqu'à présent, aucune corrélation précise n'a pu être établie entre ce type de diversité et la performance. Si ce n'est diversité, qu'est-ce qui explique une telle variable dans la cohésion, la productivité et l'accomplissement ?

Certaines séries à succès nous donnent de éléments de réponse. La récente saison du Bureau ou des Légendes, sur fond de cyber espionnage aborde la thématique « du syndrome d'Asperger ». Mindhunter ou Sherlock mettent en scène des enquêteurs dans le spectre de l'autisme. Mais la réalité dépasse souvent la fiction. La diversité cognitive du personnel commence à être observée de près. Elle est maintenant appréhendée comme un atout concurrentiel chez les GAFAM. Des entreprises et des gouvernements dans le monde s'intéressent aujourd'hui à une cible particulière : les

« profils atypiques ». Les autistes font la cible de nombreux programmes de recrutement chez Microsoft. Le sens du détail et la mémoire visuelle de certains sont devenus des pièces maîtresses de la Défense d'Israël, qui met en œuvre des programmes de détection des profils surdoués dès l'École. Prédite par aucun facteur de sexe, d'origine ethnique ou d'âge, la diversité cognitive s'éprouve comme une différence de perspective ou de style de traitement de l'information. Elle influe sur la façon dont les individus réfléchissent et s'engagent dans des situations d'urgence, de changement, de nouveauté : un phénomène de société, une culture.

La neuro-diversité, terme né chez les anglo-saxons dans les années 90' commence à émerger en France. Elle désigne, entre autres, la variabilité neurologique de l'espèce humaine. Au-delà du schéma « neuro-typique », c'est-à-dire le profil cognitif majoritaire de notre espèce, les variantes évolutives du genre humain se déclinent en plusieurs minorités cognitives. Parmi celles-ci, le spectre de l'autisme bien sûr, mais aussi les THQI (Très Haut Quotient Intellectuel), les TDAH (Trouble du Déficit de l'Attention/Hyperactivité), les dyslexiques (altération spécifique et significative de la lecture), les dyspraxiques (difficulté ou impossibilité à automatiser les enchaînements moteurs qui se déclenchent normalement à l'évocation d'un but - par exemple faire ses nœuds de lacets).

Notre environnement, dans ses processus de sélection, de l'école à l'emploi, échoue de façon cruelle à déceler les potentiels doués de ces fonctionnements différents. Pour évoluer favorablement, un profil dit « autiste » devra avant tout déployer une énergie considérable à assimiler les codes, faits et gestes dans le but de passer inaperçu, c'est-à-dire de correspondre en apparence à la norme, notion arbitraire au-delà de laquelle s'étend le monde de l'étrange, du bizarre et de l'extraordinaire.

De telles sur adaptations, si couteuses en temps et en énergie, participent fatalement au sentiment de perte de sens et se soldent par des parcours brisés, parfois pudiquement appelés « burn out ». A défaut d'être inclus dans un milieu uniforme, inhospitalier et hostile, devant l'impossibilité d'y développer ses compétences et d'y exercer son talent, se situer dans une minorité cognitive exige d'être plus que tout autre capable de s'aménager un environnement sur mesure. C'est en tout cas ce que racontent certains chiffres, comme cette récente étude au Royaume-Uni ou la population dyslexique se voit représentée à hauteur de 20% parmi les chefs et les créateurs d'entreprise contre à peine 4% dans la population générale. Il en est de même aux États-Unis ou 1 entrepreneur sur 3 se déclare comme tel.

Certes, aucune destinée et aucun succès ne se bâti sans confrontation à l'adversité ni combat personnel. Mais discriminer une part importante de la population en vouant ses conditions de réussite à la seule capacité à entreprendre, n'est-il pas profondément inégalitaire et injuste ? Les militants de la neuro-diversité soutiennent que ces fonctionnements neurologiques divers, alternatifs, doivent cesser d'être vus sous l'angle exclusif d'une lacune vis-à-vis de la norme socio-culturelle. Dans une société pensée, construite et organisée au mépris de la diversité cognitive, notre époque s'éveille enfin à l'intérêt de la neuro-diversité face aux défis de la révolution numérique.

Norme et diversité

Le devoir de bâtir monde ou la diversité est la norme et non plus l'exception pose un défi à l'ensemble du système. Alors qu'il serait judicieux de créer des filières d'excellence prenant en compte le facteur de la diversité cognitive, cette notion est trop souvent ignorée, quand ce n'est pas négligée par l'ensemble de notre appareil. En témoignent les statistiques de l'échec collectif d'une couteuse politique du désaveu. Nombre sont d'exclus, de façon insidieuse par des barrières culturelles. Accablés par une contrainte d'adaptation permanente, pas assez ou parfois trop efficaces, décalés, prisonniers, ils se heurtent à un monde égalitariste et morose qui les juge non conforme, inaptes au culte de la performance.

La capacité d'innovation se prive de ces parts de diversité. Les atouts précieux de ces alternatives de percevoir et d'analyser les informations sont rejetées. Si la diversité cognitive est mise à mal par le chômage, c'est bien moins le manque d'habilité technique que les comportements sociaux particuliers, les décalages face à des fonctionnements étriqués, qui en sont la cause. Des processus rigides échouent dans leur globalité à valoriser les compétences réelles de chacun. On parle beaucoup de leadership authentique, d'être soi-même. Mais le plus important pour commander avec sagesse ne serait-il ailleurs ? Comme de permettre aux autres d'être eux-mêmes ?

Selon une récente étude, la part du chiffre d'affaires réalisé grâce à l'innovation est quasiment deux fois plus importante dans les entreprises où la diversité du management est plus élevée que chez les employeurs les moins inclusifs (45% versus 24%). Responsable diversité, manager de la diversité, chargé de mission diversité, chaque entreprise son titre. Trois sujets dominent : égalité homme/femme, handicap et l'intergénérationnel. Et un quatrième, plus comme critère de différenciation par rapport à des concurrents, regroupe les sujets LGBT, lutte contre le racisme et discriminations selon l'origine sociale ou ethnique. Pour l'anthropologue Charles Gardou, auteur de « La société inclusive, parlons-en ! », « la transformation des esprits et des pratiques prendra du temps, mais la nécessité est là. La vie de la Cité ne peut se jouer à huis clos. Chacun a le droit inaliénable d'y prendre part, toute sa part ».

La paie sociale s'annonçant fragile et menacée dans une économie industrielle devenant une économie numérique, les États capables d'assurer leur position sur le plan géopolitique ou les groupes aptes à s'assurer ou maintenir une position de premier plan sur la scène internationale ne pourront le faire sans s'appuyer sur la diversité cognitive de leur personnel, clé du succès, de la maîtrise de la technologie et de l'inventivité. Dans cette ère nouvelle, la norme n'est pas une réponse.

Et si le meilleur choix pour maîtriser notre cyberespace commençait par rendre le monde plus respirable ? De changer radicalement notre rapport à l'étrange ? Comment mieux accepter celui ne nous ressemble pas ? Au-delà des différences ethniques, d'âge ou de genre, dans un monde normal ou l'employeur recrute « à son image », il est banal que s'assemblent des équipes aux vues similaires, au mode d'expression identique, qui engendrent des groupes homogènes décodant de la même

manière les signaux d'une menace aux multiples visages. N'est-ce pas là laisser se dessiner un monde ou à défaut d'être tous égaux, nous finirions tous semblables ? Unis, mais semblables. Semblables face aux bouleversements, aux révolutions et aux changements qui nous attendent ? Semblables face à l'adversité. Être unis dans la diversité est un autre chemin.

Note

1. Hugo HORIOT est né le 3 août 1982 à Dijon. Autiste non-verbal jusqu'à 6 ans, il est comédien, écrivain et conférencier. Suite à une formation d'acteur au Théâtre, il publie en 2013 son premier livre L'Empereur c'est moi, best-seller et lauréat du prix « Paroles de patients », livre adapté au théâtre. Il publie en 2016 son second livre Carnet d'un Imposteur puis en mars 2018 : Autisme : J'accuse !, essai-manifeste qui démontre la puissance de « l'intelligence atypique » et notamment des autistes et vise à changer notre regard, faussé par les critères de normalité, sur la différence. Il aborde les prédispositions naturelles d'une part non-négligeable de ces populations dotées d'intelligences atypiques avec ce qui est lié à l'intelligence artificielle et le rôle qu'elles jouent et ont à jouer à l'ère du digital.

Qui suis–je administrativement en France à l'aune des e–gouvernements ?

Marguerite QUICHAUD, Pierre Michaël MICCALETI, Renaud GAUBERT [1]

NDLR : Ce billet, comme voulu par les auteurs, est une étude initiale menée dans le cadre d'un des groupes de travail de l'Agora. Certaines des questions soulevées par les lignes qui suivent sont encore à l'étude.

* * *

Dans le cadre d'une réflexion globale menée sous l'impulsion de l'ANSSI, il a été créé l'Agora des 41, club de réflexion transverse sur des problématiques liées à la cyberdéfense. Un groupe de travail s'intéresse plus particulièrement au Cybermoi.

Comment donc peut-on envisager cette évolution vers une « cohabitation cordiale » entre l'individu et son cyber-moi, d'une manière aussi bien éthique que dans des aspects de protection autant physique qu'identitaire. En un mot, comment garder confiance dans le numérique ?

A l'instar des « virus » informatiques, le terme même montrant la porosité par analogie entre monde physique, celui du vivant et du numérique. Dès lors comment baliser les sujets risques/sécurité/juridique pour les cybers citoyens du monde, européens, français ? Quelles grilles de lectures imaginer ? Quid de vols d'identité, d'usurpations, de détournements, etc., dès lors une criminalité dont on n'ose imaginer les méfaits ? Quelles mesures et quels organismes instruiront pour le citoyen cette protection ? Existera-il un ministère de la santé numérique ?

« Comment vivre avec mon futur CYBER-MOI ? Quels enjeux cette nouvelle entité, extension de mon identité physique, posera-t-elle aux individus et aux sociétés dans leur relation à ce nouvel espace/temps ? » Voici donc les questions qui auront prévalu à alimenter une réflexion sommairement résumée dans ce titre un peu étrange et provocateur de « Cyber-moi », mélange et cocktail de multiples concepts tirés de la science-fiction. Faire l'exercice de formaliser ces interrogations permet de

© Editions ESKA

mesurer l'immensité qu'ouvre le champ de la cyber-dimension et de son appréhension pour agir et y vivre en conscience.

Ce billet n'a pas la prétention de couvrir l'ensemble des questions précédentes sur les nombreux sujets qu'elles pourraient soulever mais plutôt de porter un premier regard, non exhaustif, pour répondre à la question suivante : « *Qui suis-je administrativement en France à l'aune des e-gouvernents* » *il préfigure une réflexion qui alimentera des productions futures dans le cadre des travaux du groupe cybermoi de l'Agora des 41. Pour ce groupe* « *cybermoi* »*, il est apparu essentiel de comprendre dans un premier temps ce que pouvait recouvrir le terme de cybermoi sur une dimension de*

L'identité est un élément central de la vie des individus, quelle que soit la définition et la société à laquelle il appartient. En bon néophyte, il est légitime de s'interroger : où commence-t-elle et où finit-elle ? De sa naissance à sa mort, avant et après d'ailleurs, l'individu sera confronté à ses éléments de gestion et de régulation, on pourrait dire familièrement que celle-ci lui colle à la peau.

Une simple requête sur l'expression « concept d'identité » en français dans le moteur de recherche google retourne environ 1 390 000 résultats indexés... On peut y lire en 1re proposition issue de l'encyclopédie en ligne Wikipédia l'extrait suivant :

« L'identité de l'individu est, en psychologie sociale, la reconnaissance de ce qu'il est, par lui-même ou par les autres. La notion d'identité est au croisement de la sociologie et de la psychologie, mais intéresse aussi la biologie, la philosophie et la géographie. »

Si l'on continue, encore un peu à scruter les résultats retournés, sans être un quelconque expert des domaines cités, on fera le bilan d'une littérature abondante dans les disciplines les plus variées. On pourra dès lors de la même manière, acquérir un savoir minimum à travers les nombreuses thèses scientifiques ayant traité de ce sujet. On pourra aussi être surpris au passage en découvrant qu'elle touche un ensemble de secteurs voire quasi tous ceux qui composent notre quotidien aujourd'hui avec une digitalisation globale des usages dans nos « cyber vies », avec en contrepoint la fameuse notion d'anonymat

En regard de ce constat, au moment de l'explosion des données individuelles, des traces produites dans chacune de nos actions dans nos sociétés de l'information (et le mot est certainement encore faible) comment ne pas être saisi à minima d'interrogations quant à l'évolution de ce concept à l'ère de l'intelligence artificielle sinon de vertige voire d'angoisse si par hasard, on affectait à cette "identité" sa propre singularité !

Il s'agira donc aujourd'hui, dans le contexte d'émergence d'une nouvelle dimension d'espace et de temps dans un cybermonde informationnel bouillonnant de pouvoir, se rassurer et interagir dans des modèles adaptés qui devront permettre de conjuguer de manière fluide et éthique deux formes en apparence opposées mais au fond pas du tout : entre « anonymat et identité forte ».

Ce nouveau paradigme pose ainsi une dynamique d'évolution des pratiques qui a vu la naissance de plusieurs entités et instances nouvelles, dans nos quotidiens : du simple login/mot de passe, clef basique d'accès à des espaces de services plus ou moins

élaborés à la signature électronique, identificateurs biométriques, objets connectés, chatbots, assistants en tous genres..., etc. Le tout ne cessant de se complexifier à la lumière des progrès technologiques fulgurants.

Ainsi, l'identité pour le service public est devenue un enjeu essentiel pour sa propre survie, aux multiples propriétés, dans le développement des services publics/privés en ligne. Par ailleurs, elle est aussi centrale dans de nombreuses interactions entre personnes (physiques ou morales) sur le plan de la vie privée.

L'émission d'une identité par l'Etat semble encore, de nos jours, rester dans ses attributions les plus fondamentales... Autorité régalienne historique, l'Etat s'impose encore donc naturellement comme l'acteur de référence. A la différence du monde physique, dans le monde numérique l'utilisateur peut disposer de multitudes d'identités gratuites non officielles pour les administrations la plupart du temps, assorties d'avatars et valides pour la/des plateforme donnée. Des passerelles techniques contractualisées entre elles faisant office d'arbitre et garant pour leur relation quant aux données de leurs utilisateurs. Grace à ses facilitations où tout semble devenir transparent dans sa navigation, on se trouve face à une marée noire de données personnelles émises qui peuvent donner le tournis. Il est légitime alors de se demander quel peut être le rôle de l'Etat dans la maitrise de l'identité des citoyens.

On notera aussi qu'on peut de manière simplifier la décliner selon plusieurs axes selon le schéma suivant en composants, processus et procédés :

- Par composant on peut entendre sur le plan technique par exemple ce qui pourrait être le premier maillon universel consenti et historique, entrant de fait sous le sens commun d'une « carte d'identité numérique » et/ou d'un laisser-passer, le sacro-saint « **login/mot de passe** », première « paire atomique » constituante de ce que l'on nomme : son ID !
- Par processus on peut entendre aussi :
  - Des mécanismes d'authentification, pour lesquels nous allons le voir, beaucoup de pays font le choix procédural de certificats de chiffrement aujourd'hui.
  - Des services publics, auxquels cela donne accès : service des impôts en ligne en France, ouverture de compte en banque sous 15 minutes en Estonie...
  - Des services privés que cela a permis de développer, par exemple la signature de contrats entre citoyens.
- Par procédé : pour beaucoup de pays, l'identité passe par une connexion en ligne passe via des certificats de chiffrement via avec des techniques de cryptologie, délivrés par des organismes habilités à cet effet. Ces certificats permettent tout d'abord de certifier de son identité. Il reste à rappeler que les techniques de cryptographie sont autorisées quand elles répondent aux exigences de déchiffrement des services de renseignement...

Ces certificats ont pour fonction par ailleurs d'assurer la garantie de l'intégrité (pas d'altération du message/document/fichier, la non répudiation de ce document ainsi que le secret de la communication).

Ainsi, on utilise ce trio - composant-procédé-processus - afin de signer des documents électroniques, attestant ainsi de l'identité de

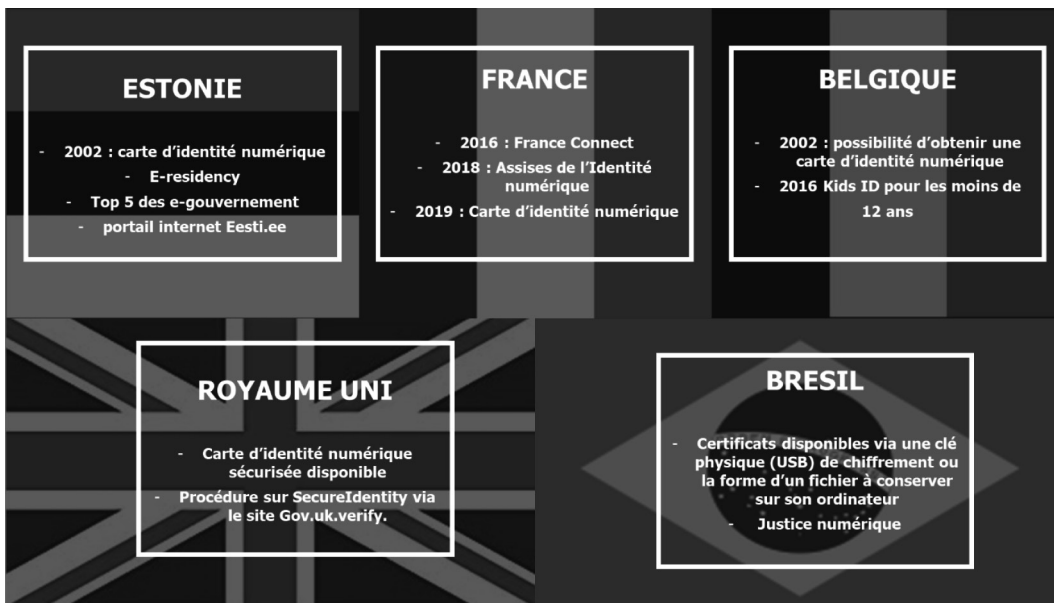
la personne, mais aussi garantissant dans le futur qu'elle ne puisse répudier cet acte et protégeant alors contre toute altération possible du contrat.

Approche comparative : quelques dispositifs singuliers

En 2016, la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) a lancé France Connect[2], un fédérateur d'identité. Grâce à cet organisme, les utilisateurs choisissent entre différents fournisseurs (Impots.gouv.fr, service-public.fr, Ameli.fr, La Poste...) pour se connecter avec un identifiant unique. La plateforme permet de garantir l'identité de la personne par les registres d'Etat. Ce système assure un premier niveau de sécurité attendu par les usagers pour adhérer en confiance à une administration qui a entamé la dématérialisation de ces usages.

D'autres initiatives ont été avortées ces dernières années. En 2012, la France avait déjà tenté le pari de la carte d'identité biométrique dotée d'une puce permettant de s'identifier sur les réseaux de communication électroniques et de mettre en œuvre sa signature électronique. Elle sera plus tard jugée inconstitutionnelle : «l e législateur a méconnu l'étendue de sa compétence » avait estimé le Conseil. Par ailleurs, le conseil constitutionnel avait aussi censuré le deuxième article majeur de ce projet de loi : la création d'un fichier unique rassemblant les biométries de tous les détenteurs de la carte nationale d'identité.

Durant les Assises de l'Identité numérique en 2018, Mounir Majoubi alors secrétaire d'Etat au numérique avait évoqué la relance du projet de carte d'identité numérique « *qu'avec l'identité numérique publique, les services en ligne seront plus simples et plus sécurisés. Ce sera la fin des usurpations d'identité sur Internet* »[3] . La carte



d'identité numérique devrait apparaitre au grand jour courant 2019.

A cet égard, il est essentiel de se détacher d'une vision ethno centrée pour constituer une approche comparative de la notion d'identité numérique.

L'Estonie est très souvent prise pour exemple de **e-gouvernement**. Depuis 2002, la carte d'identité numérique est distribuée aux citoyens estoniens. Celle-ci regroupe différents services : permis de conduire, carte de sécurité sociale, carte électorale, carte de métro...

Grâce à la PKI (infrastructure de cryptographie), les services sont consultables de manière sécurisée.

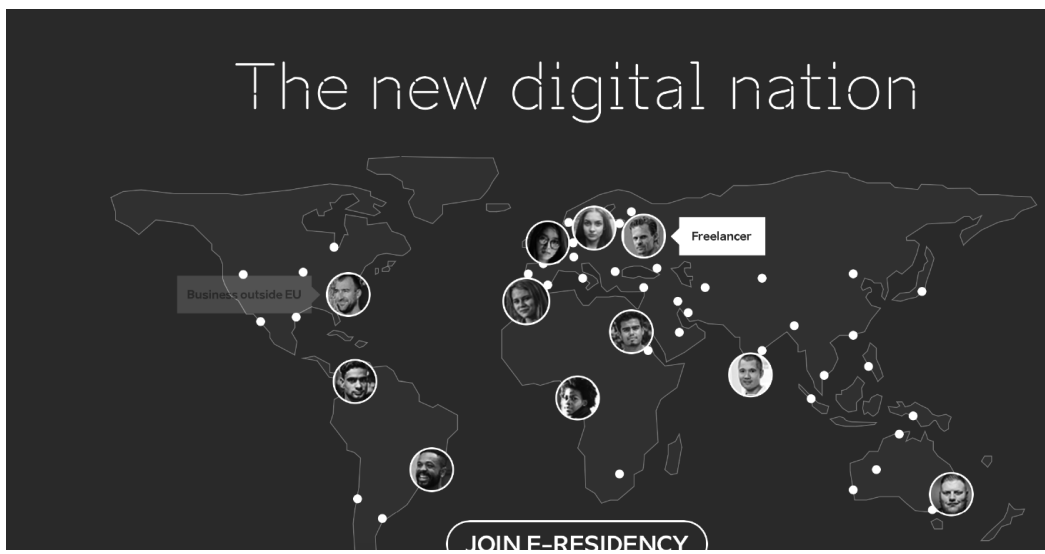
Tout citoyen a un accès, 24 heures sur 24, aux différents services publics et privés, avec un guichet numérique commun : le portail internet ***Eesti.ee***.

Alors qu'en France on tente de diffuser le programme « Dites-le nous une fois » DLNUF, en Estonie une loi interdit à l'administration de demander à deux reprises la même donnée au citoyen.

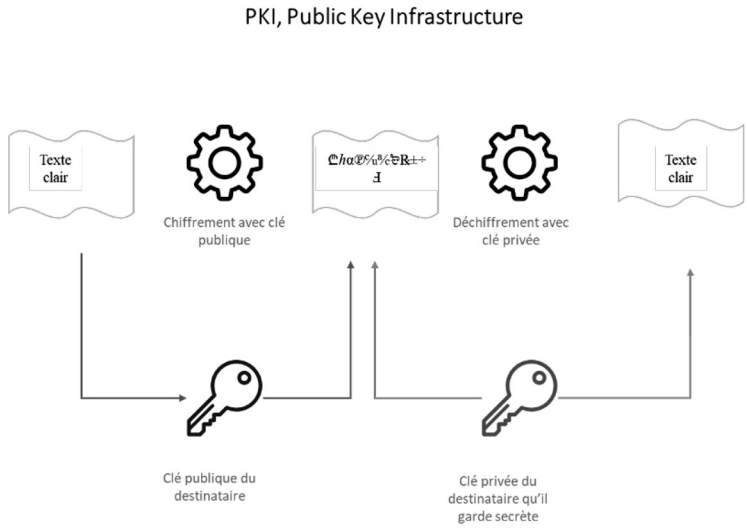
Aussi, le gouvernement a fait le choix d'ouvrir un système d'e-residency[4] permettant à des citoyens d'autres pays d'acquérir un statut de e-resident (création d'entreprise, compte en banque dans des délais très court)[5].

Concrètement, le citoyen estonien peut profiter de ce service via sa carte d'identité, quant au e-resident il postule en ligne et se présente à l'ambassade pour obtenir une carte avec un lecteur approprié. Ce programme d'e-residency a permis à l'Estonie de s'imposer dans le top 5 des e-gouvernements.

En septembre 2017, la présidente estonienne avait même souligné le risque « d'obsolescence des Etats » s'ils n'entreprenaient pas leur transition numérique assez rapidement.



Source : https://e-resident.gov.ee



-Zoom sur la PKI[6]

En Belgique, les citoyens peuvent être équipés d'une carte d'identité électronique depuis 2002 (Kids ID depuis 2016 pour les enfants de moins de 12 ans). Dans une approche de « Citizen-Centric Government », le gouvernement a souhaité permettre aux citoyens d'accéder aux services plus rapidement et de manière sécurisée[7].

Outre-manche, peu après la mise en circulation d'une quantité limitée de cartes d'identité numériques en 2009[8], ces dernières se sont montrées très vulnérables puisqu'en douze minutes Adam Laurie, consultant en sécurité informatique, avait réussi à la pirater.[9] Depuis, le Royaume Uni investit dans la sécurité des procédures en ligne. Les utilisateurs des nouvelles cartes doivent maintenant attester de leur identité en se connectant sur Secure Identity[10] via le site Gov.uk.verify. Ce dernier vise à numériser les accès aux services publics grâce à l'authentification. Par ailleurs, le gouvernement a également choisi de certifier des services de vérification de l'âge en ligne afin de mettre en oeuvre son interdiction des contenus pornographiques en ligne pour les mineurs. Derrière ces services certifiés par le gouvernement on retrouve des entreprises telles que MindGeek qui possède et exploite Pornhub, RedTube ou encore YouPorn. Sans même parler des risques liés à la création d'une telle base de données, les enjeux en termes de protection de la vie privée sont évidemment extrêmement forts sur ce sujet.

De l'autre côté de l'Atlantique, le Brésil s'est tourné très tôt vers le numérique (2000-2005). Le système fourni s'est constitué, sur la fourniture de certificats disponibles via une clé physique (USB) de chiffrement ou directement sous la forme d'un fichier que l'on peut conserver sur son ordinateur. A partir de cette nouvelle forme de matérialité de l'identité, le gouvernement brésilien a créé un nombre important d'initiatives publiques et privées.

Ces comparaisons ne sont pas exhaustives et seront poursuivies dans des productions.

On peut tout de même déjà remarquer que le « cybermoi administratif » est appréhendé par les Etats de manière très disparate mais semble s'inscrire dans les agendas des gouvernements depuis quelques années. On notera aussi que dans cette perspective, il y a, au-delà d'une vision risques/sécurité, l'émergence d'opportunités pouvant se matérialiser dans des stratégies de positionnement extrêmement compétitives quant à la performance de l'intervention des états. Cette identité administrative numérique permettrait la création de nombreux services, notamment à l'initiative d'entreprises privées.

On ne peut que constater à travers l'apparition de ces nouvelles plateformes d'e-gouvernement, l'envahissement galopant de l'environnement, par de multiples dispositifs numériques, puces invisibles, rfid généralisé, navigo, vélib, vidéosurveillance, carte vitale, domotique... Cet ensemble constituera à terme, en superposition de l'actuel réseau internet, une surcouche logique d'enrichissement d'information, tel un système nerveux virtuel qui s'élabore avec ses règles propres. Apparait ainsi la création d'une forme d'intelligence qui va s'insérer dans chacun de nos actes de vie, consommation, santé, géolocalisation, profiling, holographie, psychosociologie ...Cela fait penser au fameux « techno-cocon » évoqué par l'écrivain de Science-Fiction Alain Damasio[11].

Le résultat final de l'agrégation de ces données autogénérées et de leur exploitation dans ce nouvel espace multiple, au-delà de l'idée épouvantail liée à la notion de « surveillance globale » dont certains brandissent le spectre, interroge sur la capacité des individus à vivre avec cette nouvelle représentation d'eux-mêmes

Bibliographie

- Articles

CAPRIOLI, Eric, « Les enjeux de l'identité numérique », Janvier 2018, *Usine Nouvelle*, (https://www.usine-digitale.fr/article/les-enjeux-de-l-identite-numerique.N795374)

DUMOULIN, Sebastien, « L'Estonie, vitrine mondiale de l'e-gouvernement », *Les Echos*, Juin 2017, (https://www.lesechos.fr/2017/06/lestonie-vitrine-mondiale-de-le-gouvernement-172258)

GEORGES, Fanny, « L'identité numérique sous emprise culturelle. De l'expression de soi à sa standardisation. » 2011, Les cahiers du numérique (7), (https://www.cairn.info/revue-les-cahiers-du-numerique-2011-1-page-31.htm?contenu=resume)

LAUSSON, Julien « Carte d'identité électronique : un sénateur relance le débat », Juillet 2018, *Numerama* (https://www.numerama.com/politique/393319-carte-didentite-electronique-un-senateur-relance-le-debat.html)

LE GOFF, Delphine « Alain Damasio : le techno-cocon est en fait une prison », Juin 2015 (http://www.strategies.fr/etudes-tendances/tendances/1015142W/alain-damasio-le-techno-cocon-est-en-fait-une-prison-.html)

MEE, Franck « La future carte d'identité britannique déjà craquée », Aout 2009, Les Numériques, (https://www.lesnumeriques.com/loisirs/future-carte-identite-britannique-deja-craquee-n10089.html)

- Dossiers

« L'Estonie et la transformation numérique de l'Etat », Janvier 2018, *Atelier Europe*, (https://www.atelier-europe.eu/blog/2018/01/lestonie-transformation-numerique-de-letat.html)

« Identité numérique : la révolution invisible », Octobre 2018, Cabinet Caprioli (https://www.caprioli-avocats.com/fr/informations/identite-numerique--la-revolution-invisible--dematerialisation-et-archivage-21-308-0.html)

United Nations e-government survey 2018, (https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf)

- Sites

Site officiel belge d'information et des services officiels, https://www.belgium.be/fr/famille/identite/carte_d_identite

Site officiel du gouvernement du royaume uni, introduction de Gov Uk Verify (https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify)

Le site officiel estonien pour les e résidents, https://e-resident.gov.ee

Le site de France Connect https://franceconnect.gouv.fr/

Le site de Wikipédia https://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal

Le site du groupe cybermoi de l'Agora41 https://cybermoi.agora41.fr/

Notes

1. Marguerite QUICHAUD est une « junior » de l'Agora, tout juste diplômé d'un master sécurité défense de l'université Paris 2 ASSAS, et actuellement consultante chez Wavestone. Depuis 2014, **Pierre-Michaël MICALETTI** est conseiller du directeur du Laboratoire d'Intégration des Sciences et Technologies au sein du Commissariat à l'Énergie Atomique et aux Énergies Alternatives.
Il axe ses conseils sur ses domaines d'expertise que sont l'intelligence stratégique et économique. De 2007 à 2014, Pierre-Michaël MICALETTI a participé au projet de la Philharmonie de Paris où il était responsable du management stratégique de l'information, sur un projet à dimension étatique, hautement Sensible, réunissant le ministère de la Culture et la Mairie de Paris. Auparavant, il fut Responsable des systèmes d'information et de sécurité pour l'établissement public du musée du quai Branly.
Renaud GAUBERT est diplômé de l'École pour l'Informatique et les Techniques avancées (EPITA) où il a obtenu un Master en sciences informatiques, spécialisé en machine Learning, et un MBA en management de l'intelligence stratégique à l'École de Guerre économique en 2017-2018.
Professionnellement, Renaud GAUBERT a déjà travaillé pour deux entreprises : Arista Network à Vancouver (Canada) où il a œuvré sur l'installation de Vxlans sur les commutateurs de réseaux Arista, et pour le groupe Nvidia.
2. Site de France Connect https://franceconnect.gouv.fr/
3. LAUSSON, Julien « Carte d'identité électronique : un sénateur relance le débat », Juillet 2018, Numerama
(https://www.numerama.com/politique/393319-carte-didentite-electronique-un-senateur-relance-le-debat.html)
4. Le site officiel estonien pour les e résidents, https://e-resident.gov.ee
5. « L'Estonie et la transformation numérique de l'Etat », Janvier 2018, (https://www.atelier-europe.eu/blog/2018/01/lestonie-transformation-numerique-de-letat.html)
6. « Ensemble de composants, fonctions et procédures dédié à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique » Politique de Certification Type - Ministère de l'Économie, des Finances et de l'Industrie
7. Site officiel belge d'information et des services officiels, https://www.belgium.be/fr/famille/identite/carte_d_identite
8. MEE, Franck « La future carte d'identité britannique déjà craquée », Aout 2009, (https://www.lesnumeriques.com/loisirs/future-carte-identite-britannique-deja-craquee-n10089.html)
9. « La carte d'identité UK piratée en 12' » le blog BUGBROTHER sur leMonde.fr (http://bugbrother.blog.lemonde.fr/2009/08/06/la-carte-didentite-uk-piratee-en-12/)
10. Site officiel du gouvernement du royaume uni, introduction de Gov Uk Verify (https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
11. LE GOFF, Delphine « Alain Damasio : le techno-cocon est en fait une prison », Juin 2015 http://www.strategies.fr/etudes-tendances/tendances/1015142W/alain-damasio-le-techno-cocon-est-en-fait-une-prison-.html

Pourquoi l'éthique ?

Milad DOUEIHI[1]

L'observateur aujourd'hui ne peut que constater la popularité des interrogations éthiques concernant les effets de la culture numérique sur nos sociétés, ni nier leur importance. Il est peut-être pertinent de rappeler rapidement leur histoire afin de mieux saisir les enjeux actuels et de rendre compte des mutations portées par le développement actuel des sciences numériques.

C'est Norbert Wiener[2], le père de la Cybernétique qui est justement considéré comme le fondateur des réflexions éthique associées à l'émergence de ce qui a été désigné comme l'âge des machines. Pour Wiener, ce sont les questions d'automatisaion, de contrôle et surtout du potentiel de l'émergence de machines relativement autonomes qui oint nourri ses analyses, voire même ses inquiétudes pour ne pas dire ses angoisses vis-à-vis le rôle et le statut des « valeurs humaines » dans une société peuplée par des machines apprenantes. Ainsi, on retrouve déjà, certes sous des formes élémentaires, les questions socio-économiques aujourd'hui représentées par le Digital Labor et tout ce qu'elles impliquent sur les possibles re-structurations de l'espace social. En même temps, l'automatisation conduit nécessairement, du moins dans le cas de Wiener et certains de ses successeurs, de se poser la question des nouvelles relations entre l'autonomie et l'automatisation, l'autonomie des humains (individus ou collectivités) et celle des machines, ainsi mettant en scène une première version de ce qui semble occuper une place éminente actuellement sans notre paysage culturel: comment penser les modalités de co-habitation ou, mieux encore, de délégation, entre les humains et les agents non-humains dits intelligents. Dans la vision de Wiener, il fallait mener des recherches et des consultations afin d'éviter que les seuls prérogatives de pouvoir et de profit ne viennent dominer les choix et imposer de m « mauvais » modèles. Si cette vision paraît pessimiste, il s'est avéré qu'elle a été en partie assez réaliste.

Un second élément central dans la pensée de Wiener portait sur la nature de l'information elle-même. Pour Wiener, l'information est une matière à part entière, avec ses propriétés, ses structures qu'il faut identifier et reconnaître. Ce matérialisme est on ne peut plus important car il justifie en grande partie la nécessité de re-visiter des normes

© Editions ESKA

et des conventions qui nous ont permis pendant une longue période de gérer la sphère publique, l'économie de la propriété intellectuelle et les valorisations symboliques qui leur sont associées. L'économie de l'attention, formulée pour la première fois par Herbert Simon[3] en 1969 ne fait en fait que donner un sens plus fort et plus précis à ce matérialisme. Selon Simon, une société humaine est « un système de traitement d'information ». Ainsi, le couple informatique-information introduit une rupture majeurs dans notre histoire en substituant la surabondance informationnelle à sa rareté avec, pour conséquence, le déplacement de la valeur vers la captation de l'attention des individus et des décideurs. Pour Simon, le point fondamental de cette mutation ne réside point dans le cumul de l'information ni nécessairement dans l'optimisation de son traitement, mais plutôt dans son interprétation et ce que ce tte interprétation rend possible comme action. On voit ici émerger un second aspect « éthique » : l'accès et, plus précisément le « be soin de savoir » [« t*he need to know* »] au cœur des interrogations éthiques dans nos sociétés. Avec Simon, les questions économiques sont indissociables des questions informatiques, et nous dirons aujourd'hui numériques. Et cette nouvelle conjecture explique en quelque sorte les premières crises des intermédiaires (la presse, etc.), mais en met en relief également, en tout cas selon Simon, une autre mutation plus importante. Il s'agit de ce que « savoir représente et veut dire (« *The change in information-processing technology demands a fundamental change in the meaning attached to the familiar verb 'to know'*. »). Une version, avant la lettre de la « fracture numérique » et qui n'a rien perdu de sa pertinence. Et qui aujourd'hui peut s'appliquer au « savoir » produit par des machines apprenantes mais aussi à l'éthique des pratiques de recherche des communautés qui produisent le savoir, qui le font circuler et qui l'évaluent. L'économie du savoir « numérique » n'est pas la même que l'économie du savoir tout court.

Depuis Wiener et Simon, les travaux sur l'éthique et le numérique ont bien évolué pour prendre en compte le nouveau paysage culturel et socio-politique. Mais curieusement, leur manière d'identifier les mutations et de les inscrire dans une double perspective (matérialisme et social, matérialisme et savoir, pour résumer) a l'avantage de ne pas se focaliser exclusivement sur le réseau, la sociabilité numérique et la massification des données et leurs exploitations actuelles.

Le Web, la résurgence récente de l'intelligence artificielle portée par de nouvelles méthodes d'apprentissage et la robotique, les questions de cybersécurité dans le contexte d'une numérisation généralisée, la sociabilité numérique et les données personnelles sont aujourd'hui les grands vecteurs qui nourrissent les interrogations éthiques. Se sont succédées[4] des « éthique de l'information », des « machines morales », « éthique de la communication ». On voit même paraître une sorte de « manichéisme » à peine voilé avec des formulations comme « AI for Good » (le Bien et le Mal structurait déjà la pensée de Wiener. Il renvoie explicitement aux débats chers aux théologiens entre Saint Augustin et les manichéens sur la nature du Mal.).

Mais la question qui se pose (pour reprendre une formule attribuée à H. Poincaré) est de se demander pourquoi l'éthique? Est-ce que l'éthique, en tout cas dans notre histoire, a eu un tel pouvoir, une telle influence pour

éviter des catastrophes et des conflits ? Il me semble qu'il faut interroger cette tournure éthique elle-même non pas pour nier la réalité des soucis associés à des usages et pratiques certes problématiques. Pour certains, les initiatives actuelles portant sur l'éthique et émanant des grands acteurs du numérique ne sont que des efforts pour s'acheter une conscience et en même éviter des régulations qui auront des effets négatifs sur leur chiffre d'affaire. Pour d'autres encore, il s'agit de ré-introduire la confiance dans un milieu dans lequel elle joue un rôle déterminant mais le plus souvent fragilisé par des abus et par le potentiel de nature même du réseau et du code informatique.

Assiste-t-on aujourd'hui à la fin d'une époque, celle des promesses de l'utopie Internet caractérisée par la libre circulation de l'information, la disparition des frontières et les promesses démocratiques du village global? Que reste-t-il de cet héritage des fondateurs et visionnaires du réseau incarné par la célèbre *Déclaration d'indépendance du cyberespace* au moment où on évoque quotidiennement cyberattaques, cyberguerres, intrusions, chantages et les dangers associés a l'Internet des objets, pour ne rien dire des polémiques concernant la surveillance ?

L'effet réseau, la sociabilité numérique et l'émergence des Données massives ne font qu'accentuer cette nouvelle configuration de l'espace numérique comme un lieu de conflits potentiels opposants, dans certains cas, des acteurs anonymes, des réseaux criminels, et des états. Comment penser ces mutations, en prenant en compte la complexité d'une possible gouvernance (pour ne pas dire l'impossibilité, selon des modèles occidentaux) du Web, les enjeux économiques et politiques ? Si on assiste à un retour massif des frontières (et avec elles des appels de plus en plus fréquents pour une « éthique »), qu'en est-il de l'espace numérique devenu de fait un espace habité et habitable comme presque tout autre espace, aussi important concrètement et symboliquement que les lieux conventionnels ? Ces questions, au-delà des aspects de sécurité, sont en même temps inséparables d'un autre versant de l'éthique: les FakeNews, la soi-disant PostVérité et tout ce que ces usages impliquent sur la circulation, la vérification et l'attribution des discours et de leur valeur de vérité.

La question pourquoi l'éthique nous incite à proposer plusieurs suggestions. Une première, d'ordre anthropologique. Depuis Wiener jusqu'aux travaux les plus récents sur la robotique et certains aspects de l'Intelligence Artificielle, on est dane une situation inédite dans notre histoire. C'est la question de l'humain comme *comparable*. L'humain est un incomparable qui anime et nourrit tous les régimes de la comparaison. Est-ce à dire qu'il correspond au non-computable? D'où probablement les angoisses et inquiétudes suscités par, entre autres, l'IA ou, pour être précis, certaines de ses représentations ou receptions fantasmées. Or cette "intelligence" est fondamentalement une comparaison (tous les modèles de l'apprentissage...), certes complexe, mais néanmoins une comparaison. Par le calcul, la computation et les sciences qui donnent à voir les affects, la cognition et maintenant l'apprentissage, ce privilège de l'humain semble se fragiliser. Mieux encore, pour certains, il risque de s'éclipser devant la puissance des machines (c'est bien le scénario hollywoodien le plus privilégié). Ainsi la question du comparable se

transforme en question éthique car elle a pour objet l'autonomie, la souveraineté de l'humain sur ses créations et sa maîtrise de son environnement. L'éthique ici se substitue à la théologie (mais une théologie monothéiste[5]. D'où l'admirable titre de l'essai de Wiener *God and Golem, Inc.*) pour nous donner des principes et des valeurs. Or, l'originalité du numérique c'est qu'il su, qu'il a pu créer des êtres qui ont la capacité de communiquer avec les humais (mais surtout entre eux) et nos morales et éthiques sont des morales et des éthiques de personnes et de valeurs humaines. C'est juste pour suggérer qu'il nous importe de penser le vivant computationnel dans un sens élargi pour éviter les pièges de la ressemblance.

Une second observation porte sur des aspects de la gouvernance, des dimensions plus collectives et politiques. Peut-être une formule ancienne suffira pour en donner une idée: l'impératif territorial. Les « *soft borders* » ne sont presque plus de mise. Les états, les autorités publiques et les régulateurs ré-introduisent les frontières dans un monde qui a été conçu pour les dépasser et les éliminer. Certes, la convergences des données de géolocalisation, la gestions des adresses IP, tout comme le rôle prépondérant des grands acteurs du Web aujourd'hui, ont nécessité de nouvelles règles, plus adaptées aux réalités de l'espace numérique. La protection des données ne fait qu'inscrire dans la loi une mutation importante de la gestion de l'identité (naguère sol et sang) et qui est devenue partie intégrale des traces et des données personnelles. Cet aspect ne fait qu'expliquer le retour sur des concepts comme la souveraineté. Privilège des états, elle est aussi censée porter des valeurs. D'où parfois l'oscillation, dans les discours, entre éthique, valeur et souveraineté. L'impératif territorial a bénéficié dans le passé de traditions éthiques (ou morales) qui, en théorie, définissait les conditions d'une guerre dite juste. Or la reconfiguration de l'espace numérique évacue en grande partie les éléments essentiels de ces discours. La « mollesse » des frontières, la nature du hacking, la difficulté de l'attribution, la fluctuation identitaire des acteurs (black et grey hackers, alliances temporaires, circulation des failles et des exploits entre tous les acteurs potentiels, etc.).

Ces questions nous invitent à re-visiter les liens entre frontières et intérêts économiques et politiques à l'ère numérique, acteurs publiques et modèles de légitimité. Quels sont les modèles historiques toujours pertinents aujourd'hui dans ce nouveau contexte, incertain et en évolution permanente? Le droit international, par exemple? Ou bien faut-il privilégier la protection des infrastructures, des priorités nationales et économiques (parfois paradoxales vu la diversité des options politiques adoptées dans nos sociétés occidentales mais dans un contexte de mondialisation) ? est-il possible d'envisager une paix numérique qui va au-delà des simples souhaits et qui puisse imposer des règles de comportement diplomatiques à la hauteur des enjeux et des défis actuels? Le territorial, dans sa nouvelle version, devient le site d'une nécessaire invention de ses pratiques dites justes et justifiées, mais qui ont toujours entretenues des relations difficiles avec des idéaux éthiques.

Finalement, peut-on répondre, au-delà des régulations ou de normes de bon sens et de bonnes pratiques, au défi numérique ? Peut-être une voie parmi d'autres serait

de se poser la question de la comparaison. Comparer à l'ère de la computation, c'est bien se construire des outils et des concepts appropriés pour l'âge des machines. Retracer les modèles de ces construction des comparables, leurs histoires, leurs mutations et surtout, de notre point de vue, la manière dont ils permettent de saisir l'enjeu premier et déterminant de la comparaison elle-même en tant que schéma structurant d'une interrogation scientifique et épistémologique.

Notes

1. Milad DOUEIHI est un universitaire au parcours multiple. Diplômé d'un BA de l'université de Syracuse complété par un PhD de la Cromwell University à New York, il est aussi docteur Honoris Causa des facultés de Louvain et du Mans. Milad DOUEIHI est l'auteur de nombreux ouvrages parmi lesquels « La confiance à l'ère numérique, sous la direction de M. DOUEIHI et J. DOMENICUCCI (BergerLevrault, Mai 2018) ; Du matérialisme numérique (avec F LOUZEAU, Hermann, 2017) ; Qu'est-ce que le numérique ?(Paris, PUF, Octobre 2013) ; ou enfin La grande conversion numérique, suivi de Rêveries d'un promeneur numérique (Paris, Seuil, Points Essais, 2011)
2. Pour Norbert Wiener, voir surtout God and Golem, Inc. (MIT Press, 1964) et Cybernetics or Control and Communication in the Animal and the Machine (Hermann, 1948).
3. Pour le texte fondtaeur de Herbert Simon, voir les actes du colloque (1969) publiés sous le titre Computers, communication, and the public interest (Johns Hopkins University Press, 1971), sous la direction de M. Greenberger, pp 38-72.
4. Juste un exemple, le volume Information Technology and Moral Philosophy, éd. J. Van Den Hoven et J. Weckert (Cambridge University press, 2008).
5. Ce qui n'implique en aucun cas le recours à d'autres systèmes religieux, polythéistes ou autres.

BULLETIN D'ABONNEMENT OU DE RÉABONNEMENT

Sécurité Globale

Bulletin d'abonnement ou de réabonnement

À retourner accompagné de votre règlement aux
Éditions ESKA – 12, rue du Quatre-Septembre, 75002 PARIS
Tél. : 01 42 86 55 65 – Fax : 01 42 60 45 35

http://www.eska.fr

M, Mme, Mlle _____ Prénom _____

Société/Institution _____

N° _____ Rue _____

Code postal _____ Ville _____

Pays _____

Adresse électronique _____

TARIFS D'ABONNEMENTS*

	France particulier	France société/ institution	Etranger particulier	Etranger société/ institution
1 an (2019)	❑ 111 €	❑ 141 €	❑ 136 €	❑ 167 €
2 ans (2019 et 2020)	❑ 200 €	❑ 250 €	❑ 240 €	❑ 299 €

* Abonnements souscrits à l'année civile (janvier à décembre).

❑ Je souscris un abonnement pour ❑ 1 an ❑ 2 ans

Je joins mon règlement de ..... Euros

❑ par chèque bancaire à l'ordre des Éditions ESKA

❑ par virement bancaire aux Éditions ESKA – BNP Paris Champs Elysées 30004/00804/ compte : 00010139858 36

❑ par carte bancaire : merci d'indiquer votre numéro de compte et la date d'expiration

N° carte bancaire : ❑ Visa ❑ Eurocard/Mastercard

|_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|

Date d'expiration : |_|_|_|_| Signature :

Derniers numéros parus

Sécurité globale 17 | 2019 (nouvelle série) : Géopolitique, Sécurité-Légalité
Sécurité globale 16 | 2018 (nouvelle série) : Brésil demain : Sécurité, économie, écologie
Sécurité globale 15 | 2018 (nouvelle série) : Cybermonde : état des lieux, perspectives, risques et périls
Sécurité globale 14 | 2018 (nouvelle série) : Géopolitique – Terrorismes et crime organisé
Sécurité globale 13 | 2018 (nouvelle série) : Terrorisme – Criminologie
Sécurité globale 12 | 2017 (nouvelle série) : Terrorisme – Criminologie
Sécurité globale 11 | 2017 (nouvelle série) : Géopolitique – Criminologie – Terrorisme
Sécurité globale 10 | 2017 (nouvelle série) : Le chi'isme paramilitaire
Sécurité globale 9 | 2017 (nouvelle série) : Les habits neufs de l'impérialisme
Sécurité globale 8 | 2016 (nouvelle série) : Cyber-chaos et sécurité numérique
Sécurité globale 7 | 2016 (nouvelle série) : Islam activiste, réaction et révolution
Sécurité globale 6 | 2016 (nouvelle série) : Le monde criminel à l'horizon 2025
Sécurité globale 5 | 2016 (nouvelle série) : Dossier Stupéfiants
Sécurité globale 3-4 | 2015 (nouvelle série) : Toujours plus cyber-menacées : les collectivités territoriales / « Police prédictive » : les belles histoires de l'Oncle Predpol
Sécurité globale 2 | 2015 (nouvelle série) : Bandes, Braquages, Terreur
Sécurité globale 1 | 2015 (nouvelle série) : Iran 2015 : Qui gouverne à Téhéran (et comment) ?

ÉDITIONS ESKA
12 rue du Quatre-Septembre - 75002 Paris, France
Tél. : 01 42 86 55 65 | Fax : 01 42 60 45 35
http://www.eska.fr