

**INTERNATIONAL >**  
La coopération technologique  
internationale – CTI

**TERRITOIRE >**  
[cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr) :  
au cœur de la cybersécurité  
collective et collaborative

**JURIDIQUE >** Le US CLOUD-ACT  
vu de la France : craintes légitimes  
ou peurs inutiles ?



# REVUE

## de la gendarmerie nationale

REVUE TRIMESTRIELLE / JANVIER 2021 / N° 268 / PRIX 6 EUROS

***Pour une cybersécurité***  
coopérative et collaborative





© SIRPA-Gendarmerie

## LA GESTION DE L'ORDRE PUBLIC

L'ordre public consiste en un équilibre subtil entre la liberté de manifester et les libertés concurrentes de circuler, de travailler, etc. L'État est le garant de cet équilibre. La force publique en France n'est pas tyrannique. Sa mise en œuvre est auto-contrainte par l'État lui-même, de manière libérale, au nom des libertés publiques.

**RETROUVEZ À PARTIR  
DE LA PAGE 177,  
UNE ÉTUDE QUI  
MONTRE QUE  
LA LOI PEUT ÊTRE  
UN INSTRUMENT DE  
LA SOUVERAINETÉ  
NUMÉRIQUE  
EUROPÉENNE ET UN  
LEVIER DE RÉGULA-  
TION ÉCONOMIQUE  
DE PRATIQUES  
MONOPOLISTQUES  
ABUSIVES ET  
D'ATTEINTES AU  
DROIT DU TRAVAIL.  
EN CELA, ELLE EST  
UN FACTEUR  
DE DIVISION OU DE  
COLLABORATION  
POUR LA CYBERSÉ-  
CURITÉ EUROPÉENNE  
ET MONDIALE.**



© Scott Maxwell/AdobeStock

# Pour une cybersécurité coopérative et collaborative

**La confiance, qui a toujours sous-tendu des activités socio-économiques apaisées, repose en matière de cybersécurité sur une inclination vers des normes internationales, une authentification des transactions numériques et un équilibre contractuel entre les producteurs de service et les usagers.**

Cependant, la complexité des mœurs numériques et des systèmes d'information n'a d'égale que la diversification et la spécialisation des cybercriminels. La résilience des systèmes, la capacité de gestion de crise en cas d'attaque cyber, la détection des menaces ne peuvent plus résulter de capacités nationales. Les postures défensives ou offensives demandent un dialogue, une mutualisation des moyens de détection, des procédures de réponse aux attaques et un continuum de la recherche. Le cadre partenarial interétatique mais également Privé/Public semble adéquat pour instaurer une cybersécurité collaborative et coopérative. Le facteur humain prend toute son importance dans la conduite des projets, la gestion des crises et dans la conception de solutions innovantes requérant de l'intuition, une empathie et une capacité de rupture.

L'Union européenne, pour recouvrer une souveraineté numérique, se heurte aux intérêts de firmes internationales ou de groupes géo-stratégiques hégémoniques. Cependant, son corpus législatif sert maintenant de référence en matière de respect des droits fondamentaux des citoyens. Il porte des solutions, tant sur le plan éthique que technologique, qui permettront lentement de recadrer l'éco-sphère de l'Internet vers une option de service général dépassant une pratique mercantile. En effet, la convergence de compétences humaines doit s'asseoir sur un socle de valeurs communes qui se fondent sur une éthique et le respect fondamental des libertés individuelles.

Colonel (ER) Philippe Durand  
Rédacteur en chef de la revue de la Gendarmerie nationale



## EUROPE INTERNATIONALE

|                                                                                                                                |    |
|--------------------------------------------------------------------------------------------------------------------------------|----|
| <b>L'Europe de la cybersécurité au prisme de la souveraineté des flux et de l'intégration</b> .....                            | 4  |
| par Pierre Berthelet                                                                                                           |    |
| <b>Coopération Technologique Internationale : la nouvelle arme de la gendarmerie scientifique et des cyber-gendarmes</b> ..... | 14 |
| par Thibaut Heckmann                                                                                                           |    |
| <b>Une souveraineté des écosystèmes numériques par la voie de l'identité</b> .....                                             | 22 |
| par Guy de Felcourt et André Viau                                                                                              |    |



## TERRITOIRES ET DÉMARCHE COLLABORATIVE

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| <b>Dispositif national d'assistance aux victimes de cybermalveillance</b> ..... | 32 |
| par Jérôme Notin                                                                |    |
| <b>Cybersécurité des territoires</b> .....                                      | 40 |
| par Olivier Kempf                                                               |    |
| <b>Partenariats public-privé en cybersécurité</b> .....                         | 48 |
| par Cyril Bras                                                                  |    |
| <b>Données et collectivités territoriales</b> .....                             | 54 |
| par Jérôme Buzin                                                                |    |
| <b>La réserve numérique</b> .....                                               | 60 |
| par Florence Esselin                                                            |    |



## DOSSIER

|                                                        |    |
|--------------------------------------------------------|----|
| <b>Hygiène des organisations et des systèmes</b> ..... | 70 |
|--------------------------------------------------------|----|



## APPROCHE JUDICIAIRE

|                                                                                                            |     |
|------------------------------------------------------------------------------------------------------------|-----|
| <b>La loi : facteur de division ou de collaboration pour la cybersécurité européenne et mondiale</b> ..... | 176 |
| par Cécile Doutriaux                                                                                       |     |
| <b>Le US CLOUD-ACT vu de France : craintes légitimes ou peurs inutiles ?</b> .....                         | 198 |
| par Emmanuelle Legrand                                                                                     |     |
| <b>La réglementation de l'intelligence artificielle</b> .....                                              | 210 |
| par Sabine Marcellin                                                                                       |     |

# DOSSIER

## Hygiène des organisations et des systèmes

### Sécurité des données et transformation numérique

71

par Ludovic Petit

### SOC et IOC au travers de la Threat Intelligence

85

par Matthieu Thuaire et Robert Breedstraet

### Des « faits alternatifs » à la « Deepfake reality », vers la fin inéluctable de la vérité dans le cyberspace ?

95

par Franck Decloquement

### Cybersécurité et protection des données :

#### Pourquoi les entreprises sont-elles plus exposées après la crise ?

105

par Marie de Friminville

### Quelle cybersécurité face aux innovations numériques ?

111

par Myriam Quemener

### Les IOT : l'internet des objets

115

par François Bouchaud

### Cybermenaces : la transition numérique de la police

123

par Thomas Souvignet

### La CSPN, une certification en cybersécurité que l'Europe nous envie

131

par Gérard Peliks

### Blockchain, au service de la sécurité

137

par Jacques Favier

### De la genèse de la loi informatique et libertés à l'éloge de la transdisciplinarité

143

par Alice Louis

### L'ingénierie sociale et du rôle de l'utilisateur en tant qu'acteur de la sécurité

149

par Denise Gross

### La part humaine déterminante face aux crises majeures et son rôle dans la cybersécurité

155

par Daniel Guinier

### Expérience des Facteurs Humains

#### Organisationnels et culture de cybersécurité

163

par Joubert Marc-Xavier, Stéphane Deharvengt  
et Robert Breedstraet



## CYBERSÉCURITÉ COLLABORATIVE : DE LA SOUVERAINETÉ A L'INTÉGRATION

Cet article de chercheur esquisse les horizons de la construction d'une cybersécurité européenne collaborative selon trois approches. La première décrit des États qui rythment leur transposition nationale de la législation européenne, non sans lourdeur et quelques divergences liées à l'expression de souverainetés numériques, et qui freinent des progrès coordonnés au regard de contraintes géostratégiques et de la nature des cybermenaces. L'imbrication des actions sous la forme d'une gouvernance multiniveaux de réseaux et de capacités de recherche constitue une seconde voie. Ces collaborations transnationales favorisent les partenariats et la construction de projets européens et des réponses plurielles mais parfois complexes à appréhender dans une stratégie globale. Enfin, une intégration européenne par étapes, selon une approche néo-fonctionnaliste, reposerait sur l'obtention d'une cybersécurité normative et serait l'incarnation d'une méthode communautaire renouvelée. Sa conséquence directe serait un rapprochement des législations nationales qui caractériserait un modèle européen de cybersécurité collaborative dégageant un corpus juridique spécifique.

# L'Europe de la cybersécurité

au prisme de la souveraineté, des flux et de l'intégration

Par Pierre Berthelet

# L'

L'objectif de cet article est de présenter une lecture conceptuelle de la cybersécurité européenne voulue comme « collective et collaborative ». Il est possible de dégager trois grilles de lecture distinctes : une sécurité par « le bas » en adoptant une approche par la souveraineté nationale, une sécurité transversale en privilégiant une approche par les flux transnationaux et une imbrication des strates, enfin une sécurité par « le haut » en optant pour une approche par l'intégration européenne.



**PIERRE BERTHELET**

Docteur en droit, chercheur associé au CESICE (Université de Grenoble). Chercheur associé au CREOGN

La première lecture correspond à une sécurité « collective et collaborative » stato-centrée. Les États de l'Union définissent les contours de cette sécurité en concluant

un accord en vertu duquel ils considèrent que la sécurité de l'un d'entre eux est l'affaire de tous.

La deuxième lecture correspond à une sécurité « collective et collaborative » en réseau. Cette sécurité se présente comme une « forme d'auto-organisation non centralisée ».

La troisième et dernière lecture insiste sur le mouvement d'intégration que connaît la cybersécurité européenne. Cette dernière ne correspond pas à une sécurité surplombant celle des États membres. Elle est en revanche le fruit d'une construction progressive, expression de solidarités nationales toujours plus fortes.

## Une lecture sous l'angle de la souveraineté nationale

La théorie intergouvernementaliste souligne la prééminence du rôle des États dans le processus décisionnel européen.



(1) Hoffmann, S., « Obsolete or Obsolete? The Fate of the Nation-State and the Case of Western Europe », *Daedalus*, vol. 95, n° 3, 1966, p. 862-915.

Elle insiste sur leur poids dans ce processus et souligne les obstacles à l'intégration européenne inhérents à la souveraineté de chacun d'eux<sup>1</sup>.

Une telle théorie, qui met en évidence l'importance pour les États de coopérer, s'applique à la cybersécurité européenne. La coopération européenne menée en matière de cybersécurité n'interdit pas des avancées dans la construction européenne, bien au contraire. C'est le cas d'une plateforme en ligne restreinte entre la Commission et le Service européen pour l'action extérieure recensant les outils employés pour contrer les menaces hybrides. C'est aussi celui du projet d'une unité conjointe de cybersécurité visant à permettre une coordination opérationnelle englobant un mécanisme d'assistance mutuelle en période de crise.

La coopération opérationnelle se trouve au cœur de cette coordination qui se veut structurée. Ainsi, les États consentent à l'élaboration d'un socle commun de règles communes en matière de cybersécurité pour les institutions et organes de l'Union. Il s'agit de favoriser l'échange sécurisé d'informations des infrastructures numériques de ces institutions et organes de l'UE à partir d'une coopération opérationnelle articulée autour de l'équipe d'intervention en cas d'urgence informatique (CERT UE). Parmi d'autres avancées

en matière opérationnelle, il est possible d'évoquer le protocole de lutte contre les menaces hybrides de 2016 (EU Playbook). Cet outil s'inscrit dans une logique intergouvernementale, une telle action s'opérant à ce sujet en liaison avec d'autres organisations internationales, en premier lieu l'OTAN. Il complète ainsi d'autres structures telles que la cellule de fusion de l'Union européenne contre les menaces hybrides et qui constitue le point focal pour l'évaluation de telles menaces.

Les États rythment donc une collaboration qui rencontre un ensemble de limites. L'une d'entre elles a trait à la mise en œuvre effective de la législation en matière de cybercriminalité. L'Union s'est dotée d'un arsenal législatif conséquent mais le droit reste mal appliqué.

(2) Saurugger, S., F. Terpan. « Resisting 'New Modes of Governance' through Policy Instruments », *Comparative European Politics*, vol. 14, n° 1, 2016, p. 53-70.

Il ressort de certaines analyses juridiques que cette réticence n'est pas une anomalie de l'exécution du droit, mais au contraire une des conséquences directes du poids des

États sur la mise en œuvre des normes juridiques<sup>2</sup>.

Une autre limite concerne l'élaboration par l'Union de capacités propres. Ainsi en est-il de l'Agence européenne de cybersécurité (ENISA), qui ne constitue pas une agence disposant des capacités opérationnelles similaires à celles des États membres, telles que l'ANSSI en France. Un rapport



(3) Assemblée nationale, Rapport d'information déposé par la commission des affaires européennes sur l'avenir de la cybersécurité européenne, n° 2415, déposé(e) le jeudi 14 novembre 2019.

de l'Assemblée nationale rappelle à cet égard que l'ENISA constitue une agence facilitatrice, mais qu'elle n'est, en aucun cas, un organe supranational de cybersécurité de l'Union<sup>3</sup>.

Selon la pensée intergouvernementaliste, la structuration de la cybersécurité européenne dépend de la volonté des États, en particulier en matière d'infrastructures critiques. Ceux-ci possèdent la liberté de renforcer leur collaboration certes, mais aussi ils ont aussi la capacité de la limiter. À cet égard, la structuration impliquant les « opérateurs d'importance vitales » (OIV), ou les opérateurs de services essentiels

(4) Dunn-Cavelty, M., « The socio-political dimensions of critical information infrastructure protection (CIIP) », *International Journal of Critical Infrastructures*, 1(2), 2005, p. 258-268.

(OES) dans le jargon européen, constitue une limite. Il s'agit d'un secteur sensible au sein duquel les États membres demeurent en charge de la désignation et de la gestion de ces infrastructures<sup>4</sup>.

(5) La directive (UE)2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union<sup>1</sup> (directiveSRI).

Un rapport remis par la Commission européenne sur l'évaluation de la directive SRI<sup>5</sup> précise que si ce texte a enclenché un processus crucial d'augmentation et d'amélioration des pratiques de gestion du risque des opérateurs dans les

secteurs critiques, il souligne que l'identification des OES demeure encore considérablement fragmentée dans l'ensemble de l'Union. Ainsi, il existe une résistance étatique forte qui freine la construction européenne. D'ailleurs, ce rapport ne promeut pas une révision de la directive, mais seulement davantage de réunions de groupes de travail et l'instauration de lignes directrices afin de faire converger les approches nationales.

### Une lecture sous l'angle des flux transnationaux

Pour une autre approche, cette grille de lecture sous l'angle de rapport opposant les États soucieux de préserver leur souveraineté et l'Union n'est pas pertinente. Suggérant une conception transversale de la cybersécurité, elle part de l'idée qu'il existe une interpénétration des sphères conduisant à un brouillage des secteurs (public et privé) et des niveaux (national et européen).

La cybersécurité européenne se déploie sous forme d'interactions diverses. Les analyses de la gouvernance multi-niveaux,

(6) Hooghe, L., Marks, G., *Multi-Level Governance and European Integration*, Lanham, Rowman & Littlefield Publishers, coll. Governance in Europe Series, 2001.

comme théorie alternative à l'intergouvernementalisme, appréhende l'Union sous l'angle d'une imbrication de différentes strates<sup>6</sup>. La cybersécurité européenne, en tant que « sécurité coopérative et collaborative », apparaît ainsi sous la

perspective d'une sécurité de nature multi-niveaux. La création du Réseau judiciaire européen anti-cybercriminalité, élaboré en 2016, apparaît comme l'illustration de ce mouvement de réticularisation à l'œuvre, à l'instar du Réseau de compétences en cybersécurité qui fait

(7) <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52018PC0630&qid=1537349553647&sortOrder=asc>

l'objet depuis 2019 d'une proposition de règlement en cours de discussion<sup>7</sup>.

Ce réseau, connecté au Centre européen de

compétences industrielles, technologiques et de recherche en matière de cybersécurité visera à assurer la mise en commun et le partage des capacités de recherche ainsi que des résultats en matière de cybersécurité.

Tous ces réseaux constituent des enceintes de dialogue et de réflexion propices à l'adoption de normes techniques et de droit mou (soft law).

L'action menée par l'Union concernant les infrastructures liées à la 5G est un autre exemple. Cette action s'organise autour d'une recommandation non contraignante de la Commission européenne. Le constat est un risque de perturbations systémiques et généralisées de ces réseaux. Différentes mesures ont été adoptées au sein de ce cadre d'une gouvernance informelle, dans le contexte d'une « boîte à outils » relative à la 5G. Elle incarne le caractère innovant des instruments mis en place, souligné par les tenants de la gouvernance multi-niveaux.



La voie de programmes mobilisant des acteurs multidisciplinaires et provenant tant des puissances étatiques que des groupes privés permet de fait la production d'une norme qui s'impose aux tenants de thèses souverainistes.

Ces outils, fondés sur des dispositifs contraignants, promeuvent une approche horizontale visant à mettre en réseau des acteurs existants ; le but est de faciliter certains flux, en l'occurrence des données.

Le système d'alerte rapide de l'UE en matière de cybercriminalité est un exemple. Élaboré conjointement entre Europol et l'ENISA, il vise à permettre une meilleure circulation de l'information en cas d'aggravation de la cybercriminalité, vue elle-même comme un phénomène fluctuant, qu'il importe de mesurer et d'endiguer.

Les programmes financiers européens constituent un levier de l'action publique de l'Union destiné à promouvoir la collaboration d'acteurs pluriels (parties prenantes ou « stakeholders ») à l'élaboration d'une cybersécurité européenne. Ces programmes favorisent, au moyen de la subvention publique, cet effet d'imbrication des différents niveaux de prise de décision et associent

(8) Berthelet, P., « La coopération public-privé à l'échelle de l'UE. L'émergence d'un «Etat régulateur» européen en matière de cybersécurité », note du Centre de recherche de l'Ecole nationale de la Gendarmerie (CREOGN), note n° 29, décembre 2017.

étroitement les secteurs privé et public. Ils renforcent les collaborations transnationales en dehors des canaux classiques de coopération<sup>8</sup>. Le partenariat public-privé européen sur la cybersécurité, lancé en 2016, sur la base des financements

du programme Horizon 2020, est une illustration de cet entrelacement.

Dans le cadre de ce programme pour la recherche et l'innovation, les collaborations se forgent par l'encouragement et la stimulation.

En effet, la cybersécurité européenne est vue comme une réponse collective et plurielle impliquant toutes les composantes de la société. Autrement dit, les procédés d'identification des menaces, autant que ceux qui concernent la résilience et la réaction, requièrent une action coordonnée et des acteurs diversifiés : institutions et agences de l'Union, États membres, entreprises, milieux universitaires, associations et particuliers. Le futur plan d'action en matière d'éducation numérique prévoit à cet égard, une série de mesures destinées à renforcer les compétences informatiques des citoyens. Or, cet effort de formation s'appuie sur les divers niveaux d'action : institutions européennes, États membres et société civile, en particulier le milieu associatif impliqué dans la sensibilisation de certaines catégories de la population (enfants, demandeurs d'emploi, personnes âgées, etc.).

(9) Coen, D., Thatcher, M., « Network governance and multi-level delegation: European networks of regulatory agencies », *Journal of Public Policy*, vol. 28, n° 1, avril 2008, p. 49-71.

Les différentes structures et agences européennes sont donc impliquées dans le contexte de cette action coordonnée et multi-acteurs. Cependant,

dans cette perspective multiniveaux, elles constituent des systèmes non-hiérarchiques de négociation et de régulation<sup>9</sup>.

C'est le cas d'Europol et de l'ENISA, qui ont vu chacune leurs compétences renforcées respectivement en 2017 et en 2019. Enfin, cette mise en réseau se traduit d'une part, par une multiplication des acteurs qu'ils soient publics ou privés, par exemple ceux du marché

(10) Sterlini, P. et al., *Governance Challenges for European CyberSecurity Policy: Stakeholders Views*, EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe, Povo di Trento, University of Trento, 2019.

de la cybersécurité, représentés par l'organisation européenne pour la cybersécurité (ECSSO), et d'autre part, par une démultiplication des sphères de collaboration, avec, par exemple,

le groupe consultatif créé par l'Acte de cybersécurité<sup>10</sup>.

Ce foisonnement d'enceintes est l'expression de cette configuration européenne multi-niveaux, fondée sur des interdépendances toujours plus fortes en matière de cybersécurité. La lecture néofonctionnaliste analyse aussi la construction européenne sous l'angle des interdépendances, mais ses conclusions sont radicalement différentes, conduisant à une grille de lecture distincte de la cybersécurité.

### Une lecture sous l'angle de l'intégration européenne

#### L'élaboration d'un modèle européen de cybersécurité

La cybersécurité européenne, comme sécurité « coopérative et collaborative », peut enfin être analysée sous le prisme de

l'intégration, même si sa structuration ne correspond pas à un saut qualitatif voulu par les partisans d'une Europe fédérale.

(11) Lindberg, L. N., Scheingold, S. A., *Europe's would-be polity: Patterns of change in the European Community*, Prentice Hall, Englewood Cliffs, 1970.

Elle a trait davantage à un processus incrémental correspondant à l'ap-proche néo-fonctionnaliste. Selon les tenants de cette théorie, l'Europe se construit par étapes<sup>11</sup>.

La cybersécurité européenne peut être lue sous cet angle. D'abord, l'Union a développé un ensemble de mesures dans le cadre du marché unique, qu'elle a étendues au domaine numérique. La cybersécurité apparaît comme un complément à la protection de ce marché, l'existence de législations divergentes générant des décalages préjudiciables à son bon fonctionnement. De même, en matière de répression pénale dans le cyberspace, l'Union a pu étendre les mesures déjà prises dans le contexte de l'espace de liberté, de sécurité et de justice, en particulier les dispositifs de reconnaissance mutuelle des décisions judiciaires nationales. Là encore, une répression efficace et uniforme dans le cyberspace apparaît comme une nécessité afin d'éviter que

(12) Le *spill-over* est la notion selon laquelle l'intégration dans un certain domaine fonctionnel entraîne de facto l'intégration dans les domaines connexes.

les cyberdélinquants ne trouvent refuge dans les mondes numériques. Le processus de *spill-over*<sup>12</sup> s'opère du moment que l'Union ne conçoit plus la cybersécurité comme une

annexe des politiques déjà en place, mais comme une politique en soi. C'est ce qu'elle a fait en 2013 avec l'élaboration d'un agenda spécialisé. Force est de constater que par effet de « petit pas » mis

(13) Kasper, A.; Vernygora, V. A., « Towards a 'Cyber Maastricht': Two Steps Forward, One Step Back », in Harwood, M., Moncada, S., Pace, R. (dir.), *The Future of the European Union: Demisting the Debate*, 2020, p. 186–210.

en évidence par les analyses néofonctionnalistes, l'Union développe et structure son action dans ce domaine<sup>13</sup>. En particulier, un rapport de la Commission européenne, de 2017, révèle que la directive dite « cyberat-

tiques », adoptée au moyen de la méthode communautaire, a contribué à accomplir des progrès substantiels en matière de criminalisation des cyberattaques, à un niveau comparable dans tous les États membres. L'élaboration d'un socle commun de normes contraignantes, adopté dans un contexte de prise de décision européenne qui ne relève pas, ou plus, de la méthode intergouvernementale, est l'illustration de cet effacement progressif des souverainetés.

La nouvelle stratégie, destinée à remplacer celle de 2017, va être adoptée dans les mois à venir. Elle marque un nouveau stade de cette Europe de la cybersécurité normative. La sédimentation des textes juridiques européens contribue à piéger les souverainetés nationales, en créant progressivement un cadre de plus en plus élaboré et en limitant les marges de manœuvre des États membres et des acteurs

économiques. C'est le cas de la proposition de règlement relative à la prévention de la diffusion en ligne de contenus à caractère terroriste qui impose un cadre contraignant à l'égard des opérateurs privés.

Cela étant dit, il est inexact de réduire l'Europe de la cybersécurité à sa seule dimension normative. La construction européenne porte également sur l'élaboration de capacités spécifiques, incarnation d'une méthode communautaire renouvelée. À cet égard, l'Union se dote de capacités de plus en plus conséquentes en matière de lutte contre les cyberrisques et les cybermenaces. De prime abord, la création de celles-ci s'opère à côté et en complément des capacités étatiques. Pour autant, il est possible de considérer que ces capacités ne se limitent pas à des outils européens à la disposition des acteurs nationaux.

(14) European center crime ou centre européen de lutte contre la cybercriminalité. <https://www.europol.europa.eu/about-europol/european-cyber-crime-centre-ec3>

Ainsi, Europol se dote depuis les années 2000 de structures dans ce domaine, notamment l'EC3<sup>14</sup> qui est l'unité anti-cybercriminalité ou plus récemment la

plateforme dite « NAI » visant notamment à aider les États membres, les agences européennes et les réseaux de professionnels, à partager les connaissances entre les services répressifs dans l'ensemble de l'UE sur les manières d'effectuer des

analyses criminelles. Ce renforcement d'Europol s'opère dans le cadre d'un mouvement permettant à l'Union de se doter de capacités autonomes concourant à façonner et préserver à un intérêt supranational. Contrairement aux tenants de l'intergouvernementalisme pour qui la construction européenne se heurte à une forme de plafond de verre, les partisans du néofonctionnalisme estiment quant à eux, que le plafond de verre se fissure progressivement. Le Procureur européen, opérationnel en 2020, est, quant à lui, l'illustration archétypique de ce processus en

(15) Majone, G., « The new European agencies: regulation by information », *Journal of European Public Policy*, vol. 4, n° 2, 1997, p. 262 -275.

matière d'atteintes aux intérêts financiers de l'Union, qui englobe la lutte contre la criminalité numérique ayant trait à ce domaine<sup>15</sup>.

Qui plus est, les travaux de ces agences, en particulier ceux d'Europol, comme le rapport sur l'état de la cybercriminalité en Europe (iOCTA), favorisent une convergence des vues sur les cybermenaces. Dans le même registre, les efforts se concentrent actuellement sur le développement d'une conscience situationnelle. À cet effet, la Commission européenne et le Service européen pour l'action extérieure œuvrent conjointement sur l'intégration des flux d'information émanant des agences européennes (Europol, ENISA, Frontex) et des États membres, ainsi que d'agences de l'UE.

Cette convergence de vues se combine avec un rapprochement des législations nationales aux fins d'établissement d'un modèle européen de sécurité. L'adoption du Cybersecurity Act en 2019 établit à cet égard un cadre européen de certification de cybersécurité, élément destiné à assurer la sécurité du marché unique numérique européen et à renforcer la compétitivité de l'Union sur le marché mondial. Ce texte établit un nouveau cadre de certification de cybersécurité contribuant à une culture de la cybersécurité dès la conception.

Il est possible d'évoquer également l'établissement en cours d'un instrument sur les preuves numériques (e-evidence) visant à accélérer, grâce à une injonction judiciaire européenne, le recueil des preuves détenues par des fournisseurs de services sur le territoire de l'Union. Il importe enfin de mentionner le RGPD qui incarne à lui seul, les valeurs défendues par l'Union en matière de protection de la vie privée. Or, ces textes réglementaires constituent un cadre normatif contraignant auquel les États membres doivent se plier. Ils concourent à façonner un modèle original, distinct des États membres et que l'Union entend exporter. Ce cadre normatif, qui repose sur un ensemble de valeurs, constitue les fondements de l'action de l'Union, qui, en tant que puissance normative, entend promouvoir son modèle de cybersécurité sur la scène internationale.



© Par beebright pour AdobeStock

## L'AUTEUR

Diplômé de l'Université d'Oxford au RU et de l'Université catholique de Louvain en Belgique, Pierre BERTHELET est docteur en droit et spécialisé en droit de l'UE.

Il est chercheur associé sur les questions de droit & sécurité à l'Université de Grenoble (CESICE), à l'Université d'Aix-Marseille (CERIC) et auprès de la Gendarmerie nationale (CREOGN).

Diplômé de l'Université de Cambridge en anglais, il a fait un post-doctorat en criminologie & relations internationales à l'Université de Laval (Québec).

Ancien conseiller ministériel, il est l'auteur de nombreux travaux universitaires, dont plusieurs ouvrages. Il est intervenant à la faculté de droit de l'Université de Strasbourg et il l'a été pendant plusieurs années auprès de l'École Nationale d'Administration (ENA).





## LA COOPÉRATION INTERNATIONALE POUR ANTICIPER L'ÉVOLUTION DE LA CYBERCRIMINALITÉ

L'évolution des menaces numériques et le chiffrement généralisé des données impose aux forces de polices européennes de densifier leurs échanges techniques et de mutualiser des moyens matériels. La création de plateformes multidisciplinaires européennes contre les menaces criminelles facilite des coopérations techniques en matière de cybermenaces. Dans ce fil, la création de groupes de travail d'action contre la cybercriminalité, la mise en œuvre ponctuelle de bureaux mobiles d'Europol ou la mobilisation de laboratoires détenant des expertises spécifiques participent à cette démarche collaborative. La Gendarmerie nationale a pris le parti de s'orienter vers une forte coopération avec le monde universitaire et de construire un dispositif incitatif aux travaux de recherches via des mesures d'accompagnement prenant en compte des innovations de rupture. Elle participe, aux côtés d'industriels et d'universitaires, à des programmes internationaux de financement de recherches orientées vers les besoins des forces de l'ordre.

# Coopération Technologique

Internationale (CTI): la nouvelle arme de la gendarmerie scientifique et des cyber-gendarmes

Par Thibaut Heckman

**L**

Les criminels suivent de très près l'évolution des technologies numériques et sont plus particulièrement attentifs aux technologies de chiffrement leur promettant une impunité totale (confidentialité, authentification et intégrité). Les supports de stockages sécurisés par mot de passe, les messageries chiffrées (WhatsApp, Telegram, Signal) et les téléphones portables sur-sécurisés sont systématiquement utilisés pour



**THIBAUT HECKMANN**

Capitaine de Gendarmerie.  
Docteur en Mathématiques de l'ENS-Paris.  
Chargé de Projets au CREOGN

les communications entre membres de puissants réseaux criminels ou terroristes dans le cadre de leurs diverses activités. Devant la difficulté technique d'absorber les technologies de chiffrement de plus en plus complexes et pour faire face aux crimes

organisés et à la cybermenace, les forces de sécurité intérieure n'ont pas d'autre choix que de multiplier les Coopération Technologiques Internationales (CTI) en s'ouvrant à de nouveaux partenariats et en développant des échanges techniques avec les forces de sécurité étrangères, les industriels et les universitaires.

Ainsi, pour la gendarmerie scientifique et les cyber-gendarmes, la coopération technologique internationale se concrétise principalement sous trois formes : les échanges techniques et la mutualisation des moyens matériels avec les forces de police étrangères, la coopération technique avec le monde universitaire/industriel international et la participation à des programmes de recherche internationaux impliquant des acteurs similaires. Si la première forme de collaboration est active depuis de nombreuses années, les deux dernières formes sont bien plus

récentes et immédiatement dépendantes des difficultés techniques générées par l'évolution des nouvelles technologies.

### Les grandes organisations internationales, un pilier solide mais non suffisant de la chaîne de coopération technique...

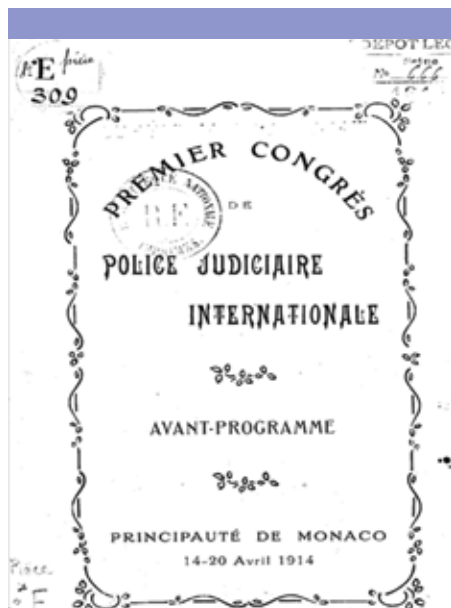
L'organisation internationale de police criminelle (*Interpol*), dont le siège se trouve à Lyon, a été créée en 1923 afin d'initier et de faciliter la coopération policière inter-

(1) Statut adopté par l'Assemblée générale de l'Organisation en sa 25<sup>e</sup> session (Vienne-1956).

nationale (*elle s'appelait alors Commission internationale de police criminelle*<sup>(1)</sup>). L'idée de la création d'Interpol est née

lors du premier Congrès de police judiciaire internationale, qui s'est tenu du 14 au 20 avril 1914 à Monaco, et dont les conférences portaient notamment sur la nécessité de réaliser des échanges techniques en identification humaine (*section sur l'anthropométrie préventive internationale des conscrits dirigée par le célèbre policier français Alphonse Bertillon*).

Interpol est forte aujourd'hui de 194 États membres. Chaque pays membre dispose d'un bureau central national, véritable point d'entrée des demandes de coopération policière, judiciaire et technique. La coopération scientifique entre forces de police étrangères fait d'Interpol le véritable précurseur de la CTI des forces de l'ordre. Mais devant la montée croissante des nouvelles menaces numériques et les



Affiche du Congrès de police judiciaire international de 1914.

© Interpol

difficultés techniques posées par la généralisation du chiffrage des données dans les affaires criminelles, les forces de police européennes avaient besoin d'une force de frappe spécialisée afin de densifier les échanges techniques et les mutualisations de moyens matériels. C'est ainsi qu'en 2013 a été créé le Centre européen de lutte contre la cybercriminalité (European Cyber Crime Centre – EC3<sup>(2)</sup>)

(2) Commission Européenne IP/12/37 et MEMO/12/221, Brussels, 28 Mars 2012.

dirigé par EUROPOL sous l'égide de l'Union Européenne, dans le but de lutter plus efficacement contre la cybercriminalité.



L'EC3 soutient techniquement les services de police dans la lutte contre la criminalité organisée. Dans ce sens, plusieurs leviers ont été mis en place par Europol pour contrer le crime numérique : une plateforme multidisciplinaire européenne contre les menaces criminelles via les programmes quadriennaux EMPACT (European Multidisciplinary Platform Against Criminal Threats) véritables facilitateurs des coopérations techniques en matière de cybermenaces ; la création d'un groupe de travail conjoint d'action contre la cybercriminalité (*Joint Cybercrime Action Taskforce*) pour aider les enquêteurs nationaux ; la

création des bureaux mobiles d'Europol dans le cadre d'opérations majeures et enfin la création des journées d'actions communes (*Joint Action Days*).

Du point de vue de la criminalistique, la coopération européenne a été facilitée par la création en 1995 de l'ENFSI (European Network of Forensic Science

Institutes<sup>(3)</sup> qui regroupe les laboratoires de police technique et scientifique de l'UE. Dix-sept groupes

de travail ont été instaurés permettant aux experts internationaux d'échanger leurs résultats mais également de mutualiser

(3) Founding Meeting on October 20, 1995 in Rijswijk (The Hague).

leurs moyens techniques et humains (stages, formations, conférences). Ainsi, les experts français de l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), acteur majeur de l'ENFSI, intègrent l'ensemble de ces groupes. Ils ont ainsi vu les échanges techniques et humains se multiplier ces dernières années. Des ateliers techniques et des conférences internationales majeures sont organisés pour inciter à l'innovation comme par exemple la conférence de l'EAFS (*European Academy of Forensic Science*) qui est un événement public triennal organisé par l'ENFSI et permettant à l'ensemble de la communauté criminalistique internationale de se réunir.

Enfin, d'autres organismes européens comme le collège européen de police (CEPOL), ou le collège européen de sécurité et de défense (CESD), permettent des échanges européens et le perfectionnement des militaires de la gendarmerie. La coopération scientifique internationale entre forces de l'ordre est également grandement favorisée par l'échange d'officiers de liaison.

**La tuerie de San Bernardino, un tournant décisif dans la coopération entre les forces de sécurité intérieure et le monde universitaire dans l'échange de techniques de déchiffrement**

De l'enquête sur la tuerie de San Bernardi-

no (USA) en 2015, l'histoire retiendra surtout la procédure judiciaire intentée par le FBI contre Apple pour contraindre l'entreprise à développer un logiciel permettant d'extraire et de déchiffrer les données du téléphone portable du tueur. La procédure n'était pas allée à son terme puisque le FBI avait finalement reçu une solution provenant de partenaires universitaires (*comme l'université de Cam*

(4) Skorobogatov, Sergei. «The bumpy road towards iPhone 5c NAND mirroring.» arXiv preprint arXiv:1609.04327 (2016).

*bridge qui proposa une technique publiée<sup>(4)</sup>*) ou d'autres entités privées étrangères alors restées anonymes. Le directeur du FBI indiqua en

conférence de presse avoir payé la solution plus d'un million d'euros. Le FBI qui était, avant la tuerie de San Bernardino, opposé à échanger techniquement (*culture du secret et développement interne de ses propres solutions*) s'est alors ouvert à la coopération technologique extérieure. Les mêmes questions se sont posées au niveau des forces de sécurité intérieure françaises. La Gendarmerie nationale a alors pris le parti de se réorganiser et de s'orienter vers une forte coopération avec le monde universitaire en participant à de nombreux projets de recherche nationaux et européens. Elle a construit un dispositif incitatif afin d'encourager les gendarmes à réaliser des travaux de recherches via des mesures d'accompagnement innovantes (*temps réservé à la rédaction, publications, conférences, dépôts des brevets industriels, thèses*)

et en décidant de scolarités alternatives à l'École de guerre pour ses futurs chefs (*formations universitaires de hauts niveaux, doctorat, Master of Business Administration, préparation d'Habilitations à Diriger des Recherches*). En 2018, elle a créé le programme « DISRUPT » pour soutenir l'innovation de rupture via des thèses et des études scientifiques autour du numérique, du big data, de l'intelligence artificielle, de la robotique, de l'humain augmenté et de l'identification humaine. Pour pérenniser et renforcer ce rapprochement avec le monde universitaire, elle a signé en 2019 un accord-cadre avec le CNRS ainsi qu'une convention avec la Conférence des Présidents d'Universités.

La gendarmerie accueille également de nombreux étudiants du cursus Licence, Master, Doctorat ou des grandes écoles d'ingénieurs (*X, ENS, mines*) leur permettant de travailler sur des sujets d'intérêt pour l'Institution avec la perspective également de constituer un vivier de recrutement. La Gendarmerie nationale compte actuellement dans ses rangs près de 350 docteurs et doctorants, toutes disciplines confondues, et ce chiffre ne cesse de croître chaque année. Le CREOGN (*Centre de recherche de l'école des officiers de la gendarmerie nationale*) a notamment pour mission de recenser, d'encourager et de valoriser les militaires de la gendarmerie qui mènent des activités de recherche. Ainsi, un dialogue régulier

et des invitations aux événements scientifiques permettent aux personnels de la gendarmerie et aux chercheurs du monde entier de se rencontrer et d'échanger autour de la recherche et de l'innovation.

### Le financement de la recherche, le nerf de la guerre...

Comme dans toute structure, qu'elle soit publique ou privée, la recherche et le développement ont un coût important qui constitue bien souvent une grosse partie du budget de fonctionnement. Afin d'augmenter considérablement ce budget, la Gendarmerie nationale participe, aux côtés d'industriels et d'universitaires, à des programmes internationaux de financement de recherches orientés vers les besoins des forces de l'ordre tels qu'Horizon 2020, OLAF, le Fonds de Sécurité Intérieure de l'Union Européenne. La gendarmerie est déjà présente dans bons nombres d'entre eux (*CERBERUS, EXFILES, Shuttle, OP-MoPS, ILEAnet, ...*) et continuera à l'être dans les prochains programmes (Horizon Europe). À compter de 2021, la Commission Européenne proposera un budget de 94 milliards d'euros pour Horizon Europe en remplacement du programme Horizon 2020 (*doté de 77 milliards d'euros*).

### Les résultats prometteurs de la gendarmerie dans la Coopération Technologique Internationale

En France, la criminalité organisée est réprimée plus sévèrement. Cette

répression se retrouve à deux niveaux sur le plan pénal : la circonstance aggravante de bande organisée (*132-71 du code pénal*) et l'infraction d'association de malfaiteurs (*l'article 450-1 du Code pénal*). Du fait de cette répression, les réseaux criminels se sont protégés et se sont rapprochés des nouvelles technologies afin de laisser un minimum de traces, rendant difficile le travail de la justice. Le stockage des données et les communications entre les membres des réseaux criminels se sont donc portés naturellement vers les nouvelles techniques de chiffrement. L'une d'elles a fait la une des médias en juillet 2020. La société Encrochat commercialisait des téléphones portables sécurisés à destination de milliers de criminels (*basés sur Android mais utilisant des surcouches logicielles de chiffrement*). La caméra, le micro et le GPS étaient physiquement retirés pour écarter tout risque d'interception et traçage par les forces de l'ordre. Le réseau Encrochat a été démantelé en 2020 par la gendarmerie française dans le cadre d'une coopération technologique internationale exemplaire.

Début 2019, le projet de recherche européen CERBERUS, piloté par la Gendarmerie nationale et financé par les Fonds de Sécurité Intérieure de l'Union Européenne, permettait d'accélérer les recherches de l'IRCGN et du centre de lutte contre les criminalités numériques (C3N) sur ces téléphones. Devant l'ampleur

des résultats obtenus, en avril 2020, il a été décidé, de créer une Équipe Commune d'Enquête (ECE) entre la France et les Pays-Bas, sous l'égide d'EUROJUST avec le soutien d'EUROPOL. Au terme de cette opération, des centaines de criminels ont été interpellés dans toute l'Europe, 10 tonnes de cocaïne et 1 200 kg de cristal méthamphétamine ont été saisis, dix-neuf laboratoires clandestins de drogues synthétiques démantelés et des projets d'assassinats stoppés.

L'action de la gendarmerie scientifique et des cyber-gendarmes en coopération technique étroite avec les forces étrangères a permis de démanteler ce réseau de grande envergure, avec des arrestations et des saisies records à la clé. Cette action illustre parfaitement les résultats directs de la Coopération Technologique Internationale et elles seront très certainement encore plus nombreuses dans les années à venir.





Le projet CERBERUS, co-financé par le Fond de Sécurité Intérieure de la Commission Européenne, a pour principal objectif la mise au clair de la donnée dans un contexte de lutte contre la criminalité organisée. L'IRCGN (France) est porteur du projet, avec pour partenaires le NFI (Pays-Bas) et l'Irlande (UCD Dublin).

## L'AUTEUR

Le capitaine Thibaut Heckmann est docteur en mathématiques de l'École normale supérieure de Paris et chercheur associé à l'ENS depuis 2018. Ancien chercheur associé à l'université de Londres et à l'université de Cambridge, en 2017 et 2018, il a rejoint le CREOGN en août 2020. Il a été de 2015 à 2020 expert à l'IRCGN et a notamment dirigé l'unité d'expertise extraction des données. Il a obtenu en 2018 le prix Européen Emerging Forensic Scientist Award 2018-2021 de l'académie européenne de police technique et scientifique (ENFSI) et le Trophée de cybersécurité du Cercle K2 en 2020. Il est membre du comité d'organisation de nombreuses conférences internationales et projets européens.



## UN ÉCOSYSTÈME DE L'IDENTITÉ NUMÉRIQUE À CONSTRUIRE

Les autorités européennes et françaises ont perçu l'importance stratégique de l'instauration d'identités numériques de confiance, à vocation sociale et économique, au service des personnes physiques et morales.

L'identité numérique exige des garanties de sécurité, d'interopérabilité et de maîtrise des données qui définissent la qualité de ce nouvel écosystème. Cependant, il se pose la question de son organisation, de son infrastructure et de sa gouvernance.

L'enjeu est de transformer progressivement les accès aux comptes et les connexions propriétaires des services et plateformes logicielles ainsi que les échanges sur les attributs d'identité et les conditions de leurs validations. Il reste également à mettre en place une interopérabilité plus grande sur les plans technique, juridique et organisationnel au travers d'une standardisation des normes. La gouvernance touchera, outre une politique incitative, à l'éducation des personnes physiques aux avantages qu'elles retireront de leur participation à un écosystème présentant une liberté de choix, une garantie de sécurité et un environnement juridique européen.

# Une souveraineté

## des écosystèmes numériques

### par la voie de l'identité

Par Guy de Felcourt

# A

A l'heure où nous vivons toujours plus connectés à des plateformes logicielles, les initiatives se multiplient pour promouvoir des identités pivots de vastes écosystèmes conciliant ergonomie, sécurité, et interopérabilité. Les enjeux portent sur la réalisation de la société et l'intégration de l'économie dans une dimension numérique pervasive, mais aussi de savoir quelle sera la souveraineté des États et de l'Union Européenne sur les territoires numériques qui se dessinent ? Alors que



**GUY DE FELCOURT**

Consultant  
spécialisé  
Co-fondateurs  
de l'ID Forum

les vingt premières années du siècle ont vu des débats animés sur la question de l'émission des identités numériques régaliennes, les vingt prochaines promettent d'être davantage centrées sur la question de la

**gouvernance des écosystèmes d'identités, avec comme enjeu les exercices de souveraineté notamment en matière juridique, financière et fiscale.**

Dans l'histoire du numérique, il y aura sans doute un avant et un après Coronavirus, tant la crise sanitaire a eu pour effet une accélération de l'utilisation des plateformes numériques pour le travail et la vie en société. Des milliards de personnes dans le monde ont dû changer leurs habitudes et vivre plus intensément leurs vies économiques, professionnelles (avec le télétravail) et sociales à travers les interfaces numériques. Nous pouvons même affirmer que pour beaucoup l'écosystème numérique est devenu le principal visage de la société et de l'économie.

Dans ce contexte, les autorités européennes et françaises ont semble-t-il perçu l'importance de renforcer leurs stratégies de mise en place d'identités numériques

de confiance au service des personnes physiques et morales afin que celles-ci puissent mieux exercer leurs missions dans le cadre de leurs différents rôles économiques et sociaux. Sur le plan européen, une nouvelle consultation a été lancée pour moderniser, élargir et rendre plus effectif

(1) <https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/referentiel-documentaire-lie-au-reglement-eidas/>

le règlement eIDAS<sup>1</sup> portant sur les services de confiance numérique et l'interopérabilité des identités numériques reconnues officiellement par les États membres.

En France, l'année 2021 devrait voir se concrétiser auprès du grand public les actions de la mission Interministérielle sur l'identité numérique, à commencer par l'arrivée de la nouvelle carte nationale d'identité électronique (CNIE).

Pour mieux comprendre les actions en cours, il convient de distinguer plusieurs types d'enjeux sur le déploiement des identités numériques. Un premier niveau d'enjeu est l'émission d'identités numériques de confiance utilisables par le grand public. C'est une réalité dans près de la moitié des pays d'Europe mais cela commence à peine en France. Le deuxième enjeu, plus ambitieux, se situe dans la capacité de fonctionnement d'une société obligée de vivre dans l'espace numérique. Il s'agit alors d'organiser un écosystème d'identités numériques, avec son infrastructure, son interopérabilité, sa gouvernance et ses incitations pratiques et juridiques.

Enfin le troisième enjeu est celui de la souveraineté tant nationale qu'européenne dans un espace qui est appelé à devenir progressivement avec la maturité des écosystèmes et le maillage des identités, un véritable « territoire numérique ».

### Rechercher l'optimisation de l'ergonomie et de la sécurité :

L'identité numérique, dans sa forme la plus élémentaire, utilise quelques données personnelles (qualifiées d'attributs de l'identité) dans une dimension à la fois structurée et dynamique en fonction du contexte d'usage et en vue d'une finalité d'un accès à un service. Elle est susceptible d'utiliser des technologies logicielles et matérielles diverses, y compris la biométrie et la cryptographie. Elle implique une dimension de confiance qui exige des garanties dans les conditions de sécurité, d'interopérabilité, ainsi que de maîtrise (au minimum de consentement) sur les données utilisées.

La recherche de l'identité numérique est née non seulement du besoin d'une relation à distance qui puisse garantir l'authenticité des parties qui interagissent, mais aussi d'un grand souci de simplification, puisque nous ne sommes pas capables de gérer efficacement les centaines de comptes numériques que nous possédons.

Les enjeux de fonctionnement de l'identité numérique s'élargissent en pénétrant

aussi dans des environnements physiques. Que nous soyons en présence ou à distance, les étapes de l'identification et l'authentification portent davantage de flux. Il peut s'agir de transactions d'achat, de paiement ou d'autres types d'interactions comme l'accès à des informations et des services personnalisés.

Dans la vie physique, les automates et les objets connectés continuent à se substituer aux personnes. Pour obtenir un ticket de transport, passer en caisse ou solliciter un service, l'identité numérique est convoquée comme le Sésame de nos interactions avec les machines, afin de nous authentifier.

L'évolution va vers des solutions à la fois robustes, multi-usages et surtout ergonomiques pour les utilisateurs. Ce dernier point suppose de renforcer constamment le confort, la rapidité et la simplicité d'usage. C'est ainsi que nous assistons depuis quelques années à une croissance des solutions combinant la biométrie et l'usage du téléphone mobile notamment.

En termes de confiance et de sécurité, tantôt on cherchera à garantir la chaîne de confiance, dans la dérivation d'identité permettant de remonter jusqu'à une identité officielle et à travers elle des données d'état civil, tantôt on visera à garantir la sécurité des informations grâce à un ensemble de conditions techniques

permettant d'attribuer à l'identité produite, reconnue et utilisée un niveau de confiance. Le plus souvent les deux simultanément dans le cadre des usages du secteur public.

### L'État émetteur d'identités

Pendant les deux premières décennies du XXI<sup>e</sup> siècle, l'axe privilégié du débat sur l'identité numérique a été le rôle de l'État en tant qu'émetteur d'identités. Certains pays ont fait le choix d'un État essentiellement contrôleur des identités numériques émises par le secteur privé (Royaume Uni, Suisse, ou en grande parties des pays scandinaves privilégiant des identités numériques bancaires), d'autres ont privilégié une position, parfois durant des années de quasi-monopole, d'émission des identités numériques officielles (Allemagne, Estonie, Belgique).

En France, le rôle de l'État comme émetteur d'une ou plusieurs solutions d'identités numériques n'a jamais été mis en cause. Cela s'explique d'une part par la tradition de citoyenneté républicaine et le devoir d'inclusion numérique et d'accès aux services publics. D'autre part, le secteur privé n'a pu ou su au cours des deux premières décennies mettre en place des solutions, faute d'usages, de modèle économique, d'ergonomie appétente pour les utilisateurs et de garantie de pérennité par l'État.

Pour autant l'émission des identités

numériques par l'État Français dotées d'un niveau de confiance substantiel ou élevé va tout juste commencer en 2021 avec la nouvelle CNIE et/ou d'autres solutions

(2) Alicem est une application pour smartphone développée par le ministère de l'Intérieur et l'Agence nationale des titres sécurisés (ANTS) qui permet à tout particulier, qui décide de l'utiliser, de prouver son identité sur Internet de manière sécurisée, à l'aide de son smartphone et de son passeport ou de son titre de séjour.

(Alicem<sup>2</sup>,...), c'est-à-dire avec une vingtaine d'années de retard sur les premiers pays européens comme la Finlande, la Belgique ou l'Estonie.

Il est vrai que pendant de nombreuses années la culture dominante a fait de l'identité dans notre pays non pas une valeur positive d'insertion éco-

nomique et sociale et d'accès aux droits, comme elle est présentée par les Nations Unies, mais au contraire un instrument de la vision post 68 d'une logique du « surveiller et punir ». Dans un paradoxe comme notre pays les aime, l'État « devait » faire mais « ne pouvait pas » faire.

Cette situation est désormais derrière nous, car outre les garanties des grandes

(3) <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/>

(4) <https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/>

législations européennes sur l'interopérabilité et la vie privée (Règlements eIDAS<sup>3</sup>

(2014) et RGPD<sup>4</sup>(2018)) plus personne aujourd'hui ne peut contester le besoin d'identités numériques de confiance

alors que le monde entier est pour

des conditions sanitaires « obligé de vivre en ligne ». Lorsqu'un professeur d'école se plaint de messages perturbant les cours en ligne émis sous des pseudonymes dont on ne sait quel élève (ou si même s'il a la qualité d'élève), ce n'est qu'un des nombreux faits révélateurs du besoin d'identité numérique afin de reproduire en ligne les conditions de protection de l'enfance promus dans une classe avec des murs et une porte.

### La gouvernance d'un écosystème d'identités numériques

Nos identités numériques ont encore des progrès à faire pour nous permettre des relations plus harmonieuses et responsables. La qualité de l'écosystème d'identités numériques en termes d'ergonomie, d'interopérabilité et de sécurité en représente une dimension fondamentale. Si la discussion sur l'Etat émetteur d'identités numériques semble avoir baissé d'intensité, cela est une bonne chose afin de pouvoir aborder une question bien plus critique à l'heure où l'intermédiation par l'identité devient un enjeu global, cette question est celle de l'organisation de l'écosystème des identités numériques, de son infrastructure et de sa gouvernance.

L'enjeu est important et vise à transformer progressivement les accès aux comptes et les connexions propriétaires des services et plateformes logicielles ainsi que les échanges sur les attributs d'identité et les conditions de leurs validations.

Pour les grands opérateurs du numérique, comme pour les acteurs privés, cet enjeu s'exprime avant tout en termes d'intermédiation dans leurs activités économiques et commerciales. L'identité est devenue la brique sans doute la plus essentielle dans la relation client et aussi le positionnement des chaînes de valeurs sectorielles.

Les premières réponses ont été apportées avec la mise en place d'une interopérabilité plus grande sur les plans techniques, juridiques et organisationnels.

Ces réponses se sont traduites par une progression de la standardisation des solutions d'identité. Les normes autour des identités numériques des personnes permettent de construire de larges interopérabilités et de se substituer aux logiques de fédérations d'identité, souvent lourdes à administrer.

Mais l'interopérabilité ne fait pas tout, il faut pour gouverner ces écosystèmes de manière adéquate, construire une politique à la fois incitative et responsabilisante vis-à-vis des acteurs sociaux et économiques. Il faut informer et parfois éduquer les personnes physiques sur les avantages qu'elles peuvent retirer de leur participation à un écosystème d'identités interopérables avec des garanties en termes de liberté de choix, de sécurité, de validité juridique effective et de maîtrise des données personnelles. Vis-à-vis des entreprises et des administrations, il faut développer une politique incitative et responsabilisante.

De nombreuses obligations de conformité, d'audit et de gestion des risques des entreprises sont directement traduisibles par les niveaux de confiance des identités alors pourquoi ne pas formuler ces exigences, ce qui simplifierait au passage aussi la gestion administrative.

Il est temps de prendre de la mesure que l'organisation de la société numérique passe par l'organisation d'un écosystème d'identités approprié.

Longtemps les États ont perçu surtout l'enjeu défensif des identités numériques et celui de la cybersécurité, notamment, puisque la qualité des enregistrements d'identités associée à la solidité des titres électroniques et des processus d'authentifications permet de pallier la plupart des risques. Puis est venu le temps de la simplification administrative (*dites-le nous une fois*) et du bon fonctionnement des administrations alliant déploiement d'une confiance et d'une relation personnalisée dans l'accès aux services. Ce fut le temps de la naissance de *France Connect*.

Aujourd'hui il s'agit d'aller bien plus loin car la gouvernance d'un écosystème d'identités numériques devient une question prioritaire de souveraineté vis-à-vis d'un nombre croissant d'échanges économiques, administratifs et sociétaux réalisés en ligne.



Sur les dix dernières années, le temps moyen d'exposition aux écrans n'a cessé de progresser. En 2020 pendant les mois du confinement, il a explosé atteignant selon les sources entre 9h et 13 heures par jour. Télétravail, relations sociales et loisirs numériques ont tous contribué à ce changement. Même si nous avons rééquilibré cette tendance depuis, nous sommes devenus de fait des citoyens numériques.

### Une souveraineté à construire sur des « territoires numériques »

Un écosystème d'identités peut permettre de structurer en cohérence les approches de demain pour la santé, la monnaie numérique, le droit exerçable dans les relations des parties qui l'utilisent. On peut estimer raisonnablement que grâce à lui, il existe la possibilité d'une nouvelle territorialité numérique. D'ailleurs cela tend à se manifester déjà aujourd'hui sous de nombreuses formes. Par exemple, quand le gouvernement britannique défend la prééminence du serveur et du réseau dans une affaire judiciaire, il ne fait que reconnaître l'existence et la prééminence de cette nouvelle forme de territorialité numérique. Il en est de même pour plusieurs des pratiques internationales souvent qualifiées d'extraterritoriales et qui en fait prennent en compte de nouveaux faits de rattachement des personnes à des territoires nationaux numériques et financiers mais non géographiques.

Nous pouvons crier à l'injustice juridique et fiscale du numérique et tenter de réclamer aux États-Unis et à la Chine la promulgation de nouvelles règles. Cependant, nous serions sans doute bien inspirés aussi d'agir en construisant un écosystème d'identités numériques qui permettra de porter demain les règles juridiques et fiscales vers un territoire numérique national et d'apporter une effectivité plus forte à nos règles de droit et de fiscalité.

Cela est-il possible ? En commençant notre révolution culturelle pour percevoir que notre territoire n'est plus seulement physique. Le territoire sent d'ailleurs de moins en moins le « terroir » aussi regrettable que ce soit. Jean Bodin, au XVI<sup>e</sup> siècle, puis l'époque Westphalienne avaient déjà privilégié une approche juridictionnelle de la souveraineté.



Photo libre de droit : La signature du traité de Munster en 1648 par le peintre néerlandais Gerard ter Borch (Rijks Museum Amsterdam).

La paix de Westphalie marque la consécration de la souveraineté des nations. Près de 400 ans plus tard les nations européennes arriveront elles à organiser leur « territoire numérique » et à y asseoir leur souveraineté ?

Plus récemment l'écrivain américain Charles Maier a qualifié le territoire d'espace de décision politique, d'activités, d'identités et d'appartenance. La supposée indépendance de l'Internet et du cyberspace rendue célèbre par la proclamation de Perry Barlow dans les années 1990 a vécu. L'espace numérique n'est pas un espace neutre, en tout cas moins que les océans, l'espace sidéral ou les pôles géographiques. Le territoire numérique a ses infrastructures propres : serveurs, réseaux, espaces de stockage, satellites, *etc.* Son architecture, même si elle comporte plusieurs couches applicatives, tend à démontrer que les comptes, les identités ou les données structurées ont un rôle essentiel car ils peuvent donner une organisation à ce territoire ou du moins une effectivité, et demain leur dimension la plus importante : la « vitalité ».

Le défi est important, l'Europe et la France s'y attellent mais nous devons les encourager afin de ne pas désespérer d'une souveraineté numérique qui puisse donner plus de satisfaction aux citoyens, aux organisations et aux États. Quelle satisfaction demain grâce aux territoires et aux identités numériques de pouvoir exercer notre citoyenneté nationale pleinement et ceci partout dans le monde !



## L'AUTEUR

Après une carrière dans la monétique et les services d'assistance, Guy de Felcourt est devenu depuis 2015 consultant spécialisé sur les questions de société et d'identité numérique. Il intervient sur la conception et la stratégie des programmes d'identités tant pour des gouvernements que des entreprises. Il est un des co-fondateurs de l'ID Forum aux côtés du Général d'armées (2S) Watin-Augouard et du Préfet André Viau. Il est l'auteur d'un livre sur l'usurpation d'identité (CNRS) et enseigne l'identité numérique dans certaines universités.

## ID-FORUM

Premier évènement en France consacré spécifiquement au développement de l'identité numérique, il réunit les acteurs privés et publics afin de débattre les enjeux politiques, stratégiques, économiques et opérationnels de l'identité numérique en Europe et en France. Plus d'informations sur <https://id-forum.eu/>

# TERRITOIRES ET DÉMARCHE COLLABORATIVE



**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*



Assistance et prévention  
en sécurité numérique

© ACYMA

## UNE DÉMARCHE COLLABORATIVE AU PROFIT DES VICTIMES

Le dispositif national d'assistance aux victimes : [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) reflète une démarche collaborative fédérant des acteurs publics et privés : particuliers, entreprises, collectivités et associations.

Le dispositif a une capacité à accompagner la victime dans sa démarche judiciaire et à l'orienter vers des experts pour gérer une crise. Le dispositif a lancé un label, élaboré en partenariat avec l'AFNOR et les associations professionnelles, qui signale la fiabilité et les compétences de prestataires spécialisés en matière de cybersécurité.

Une de ses spécificités est de savoir identifier des phénomènes à partir d'événements discrets et épars et de les assembler pour mettre en évidence une stratégie d'attaque sérielle et d'un volume important.

Sa force est également d'être un outil de prévention en donnant l'accès aux documents recensant les bonnes pratiques. Il joue un rôle majeur en concentrant des expertises, en assistant les structures en difficultés, répondant ainsi à la mission d'intérêt public que lui a assigné L'État.

# Cybermalveillance.gouv.fr :

au cœur de la cybersécurité collective et collaborative

Par Jérôme Notin

# L

**Lancé en octobre 2017, le dispositif national d'assistance aux victimes cybermalveillance.gouv.fr, piloté par le Groupement d'Intérêt Public ACYMA, est par essence une démarche collective et collaborative qui fédère des acteurs publics et privés pour une meilleure cybersécurité.**

La stratégie nationale pour la sécurité du numérique, qui appelait à la création du



**JÉRÔME NOTIN**

Directeur général  
du GIP ACYMA  
Chef d'escadron  
de la réserve  
citoyenne  
cyberdéfense  
de la gendarmerie

dispositif d'assistance aux victimes d'actes de cybermalveillance, indiquait dès 2015 : « Le dispositif adoptera une forme juridique et une organisation lui permettant de bénéficier de l'apport des acteurs économiques du secteur de la cybersécurité - éditeurs de logiciels, plateformes

numériques, fournisseurs de solutions ».

Notre collectif était né.

## Rappel sur l'organisation

Cybermalveillance.gouv.fr a trois missions :

- la sensibilisation et la prévention par la diffusion de bonnes pratiques en cybersécurité et la diffusion d'alertes contextualisées ;
- l'assistance aux victimes par une aide au diagnostic du problème, des conseils simples et adaptés, une orientation vers les services compétents, voire vers des prestataires spécialisés de proximité en capacité de les assister ;
- l'observation de la menace afin de détecter les phénomènes émergents pour pouvoir les anticiper et y répondre.

Les publics du dispositif sont les particuliers, les entreprises, les collectivités et les associations, hors opérateurs d'importance vitale et de services essentiels.

Le choix du vecteur administratif retenu a été de créer un groupement d'intérêt public (GIP), le GIP ACYMA. Ce partenariat public-privé rassemble les acteurs de l'État et de la société civile engagés dans sa mission d'intérêt public de lutte contre la cybermalveillance, qui travaillent de manière collaborative au quotidien.

Parmi les membres du GIP, on peut ainsi citer l'ANSSI, qui relève des services du Premier ministre et le ministère de l'Intérieur qui ont co-piloté sa conception, ainsi que le ministère de la Justice, le ministère de l'Économie et des Finances et le secrétariat d'État en charge du numérique.

À leurs côtés travaillent de nombreux acteurs de la société civile comme des associations de consommateurs et d'aide aux victimes, des représentations professionnelles de type fédérations ou syndicats, des assureurs, des opérateurs, des constructeurs, des éditeurs...

Fin 2020, le groupement d'intérêt public est fort de 47 membres. Outre leur soutien financier, ces membres renforcent et démultiplient les actions du dispositif en participant à des groupes de travail pilotés par les agents du GIP.

### **Un capteur en temps réel de la cybermalveillance**

Une originalité du dispositif est qu'il intervient généralement en amont des autres services de l'État lorsque la victime rencontre un incident. Il est en cela un capteur très intéressant pour les pouvoirs

publics de la cybermalveillance pour des victimes qui n'envisagent pas toujours en première intention de déposer plainte parce qu'elles n'ont pas conscience que leur incident pourrait faire l'objet de poursuites, qu'elles pensent que les poursuites dans la sphère cyber ont peu de chance d'aboutir ou enfin qu'elles ont honte et craignent pour leur image. Le dispositif intervient notamment en incitant systématiquement la victime au dépôt de plainte chaque fois qu'une infraction peut être retenue, mais aussi en l'aidant dans sa démarche au travers des conseils élaborés en collaboration étroite avec le ministère de l'Intérieur.

Une des forces du dispositif est donc sa capacité à identifier des phénomènes à partir d'événements qui, parfois pris séparément, peuvent être considérés comme marginaux mais dont le rassemblement met en évidence leur caractère sériel voire massif. C'est ainsi que le dispositif a pu contribuer dès ses premiers mois de fonctionnement à l'identification du phénomène cybercriminel de masse qu'est « l'arnaque au faux support technique ». L'identification de l'ampleur de cette catégorie d'escroquerie a pu être réalisée en grande partie grâce aux rapports techniques d'intervention sur le terrain qui lui sont remontés par ses prestataires référencés. Dans la grande majorité des cas, si les victimes avaient bien eu l'impression à un moment ou un autre de s'être faites arnaquer,



elles n'envisageaient généralement pas pour autant de déposer plainte, pour les raisons évoquées précédemment.

L'identification de ce phénomène cyber-criminel et les échanges opérationnels qui ont pu être conduits avec les services des ministères de l'Intérieur et de la Justice ont conduit à l'ouverture d'une enquête par la section de lutte contre la cybercriminalité du parquet de Paris, en mars 2018. Cette enquête, confiée au centre de lutte contre les criminalités numériques (C3N) du pôle judiciaire de la Gendarmerie nationale, a conduit à l'interpellation et la mise en examen de trois individus ayant fait près de 8 000 victimes et la saisie de près de 2 millions d'euros début 2019. D'autres enquêtes sur ce phénomène, qui perdure et fait encore quotidiennement de nombreuses victimes, sont aujourd'hui toujours en cours.

Le début 2019 a également vu l'amplification des campagnes de « crypto-porno » (chantage à la webcam prétendue piratée) et, par conséquent, du nombre de victimes. Ce phénomène est rapidement identifié par le dispositif et les magistrats spécialisés du pôle cybercriminalité. Ces magistrats élaborent aussitôt un modèle de lettre plainte électronique en collaboration avec la SDLC. Cybermalveillance.gouv.fr a mis à disposition le document sur sa plateforme, permettant aux victimes de formaliser leur plainte et de partager des données techniques avec les enquêteurs.

28 000 concitoyens transmettent alors les éléments. Grâce aux informations collectées, les services d'enquête identifient deux personnes. Elles sont interpellées en septembre, puis en décembre 2019.

Cette possibilité d'identification des menaces au plus près de leur apparition permet également au dispositif d'alerter les populations sur son site Internet et/ou ses réseaux sociaux (Twitter, Facebook, LinkedIn). Grâce à l'appui de ses membres, plusieurs alertes émises par le dispositif ont été largement reprises par les médias grands publics (Presse, émissions et journaux télévisés de grand audience comme des 20h00), démultipliant ainsi les capacités d'atteindre le plus grand nombre de victimes potentielles.

### Un outil de sensibilisation

La sensibilisation reste la meilleure arme pour éviter les cyberattaques. Cette sensibilisation aux cybermenaces et aux bonnes pratiques à adopter pour les détecter et les éviter est donc primordiale. En effet, ce sont les utilisateurs qui par leurs pratiques et leur vigilance pourront être les premiers remparts de la cybersécurité. Ils doivent être considérés comme des acteurs à part entière. Or, cela reste souvent un exercice difficile, car les sujets de sécurité numérique sont généralement ressentis comme rébarbatifs et sources de contraintes pour les utilisateurs.



© ACYMA

C'est en partant de ce constat, issu des travaux conduits avec ses membres, que le dispositif a réalisé en 2018 le premier volet de son kit de sensibilisation, le plus facile d'accès possible.

(1) Etalab est un département de la direction interministérielle du numérique (DINUM), dont les missions et l'organisation sont fixées par le décret du 30 Octobre 2019. Il coordonne notamment la conception et la mise en œuvre de la stratégie de l'État dans le domaine de la donnée. Il coordonne les actions des administrations de l'Etat et leur apporte son appui pour faciliter la diffusion et la réutilisation de leurs informations publiques.

Le kit complet a été finalisé en juin 2019. Il peut être téléchargé gratuitement. Il comprend différents types de supports (courtes vidéos, infographies, fiches pratiques, mémo...). Il vise les usages personnels de manière pédagogique et illustrée, sur des sujets qui peuvent également intéresser l'entreprise dans ses pratiques professionnels. Par exemple, si une personne sait détecter et réagir à un message d'ha-



© Acyma - Gendarmerie

Au titre de la prévention et de la sensibilisation, on peut également citer la campagne partenariale avec la Gendarmerie nationale, sur une initiative du GGD88, avec la diffusion de bonnes pratiques sur des supports du quotidien : 800 000 fourreaux à pain ont été distribués par huit groupements : dispositif R-Mess, Prix de la Prévention 2019 de la Gendarmerie nationale.

meçonnage (*phishing*) dans ses usages personnels, elle saura également le faire dans ses usages professionnels. Un choix fort a été de le publier sous licence *Etalab 2.0'*, qui permet à toute entité de le modifier, et donc d'ajouter ou supprimer du contenu. Beaucoup de structures ont par exemple simplement ajouté le logo de leur entité afin que l'adhésion des collaborateurs soit encore plus forte.

### La période Covid-19

Comme lors de toute crise, les cybercriminels savent très vite s'adapter pour en tirer profit. Le GIP a donc rapidement proposé un contenu de prévention spécifique.

Dès la veille du confinement, nous avons publié sur notre site un appel au renforcement de la vigilance en termes de sécurité en présageant d'un certain nombre de menaces que la situation pourrait engendrer, tant pour les particuliers que pour les professionnels. Force a été malheureusement de constater que nos prévisions se sont avérées exactes. Cet article a d'ailleurs battu un record de consultation sur notre site en quelques semaines.

Dans les premiers jours du confinement, une autre production majeure a été diffusée sur le télétravail en situation de crise proposant des recommandations de cybersécurité pour répondre au besoin tant des employeurs que de leurs collaborateurs.

La plate-forme a ainsi fonctionné à plein régime avec un taux de fréquentation qui a augmenté de 400 % durant les premières semaines du confinement. Elle a dans le même temps continué à recevoir des mises à jour régulières de fonctionnalités et de contenus. Côté assistance aux victimes et relations avec les professionnels référencés, la réactivité a été assurée.

A noter que le dispositif a finalisé trois projets structurants durant cette période. Le premier est le lancement de son label

ExpertCyber auprès des prestataires, initié en 2019. Ce label, élaboré en par-



© ACYMA

tenariat avec l'AFNOR et les associations professionnelles vise à apporter un niveau de reconnaissance des compétences des prestataires spécialisées en cybersécurité.

Le GIP a également conçu une campagne télévisée de spots de sensibilisation grand public, réalisée en partenariat avec France Télévisions et diffusée en mai et juin sur ses chaînes ainsi que sur celles des groupes TF1 et Canal+. Les quatre clips de 30 secondes ont été réalisés en moins de trois semaines.

Enfin, au regard du besoin lié au confinement, une intégration d'un lien vers la brigade numérique de la Gendarmerie nationale a été réalisée dans les espaces privés des professionnels et depuis l'apparition de certaines cybermalveillances les concernant. Les victimes peuvent désormais avoir directement une l'assistance pour déposer une plainte lorsqu'une cybermalveillance

cible leur entité. Projet initié en janvier 2020 avec la Gendarmerie, il a été jugé utile de le rendre accessible au plus vite du fait des contraintes du confinement et de l'augmentation de la menace.

Tout ceci en parallèle du travail de fond réalisé par le dispositif.

### Et demain ?

L'avenir du GIP s'annonce toujours plus collectif et productif, du fait du renforcement de son équipe avec l'arrivée de 3 nouveaux agents mis à disposition par le ministère de l'Intérieur et par l'intégration de nouveaux membres au sein du GIP, comme le ministère des Armées.

L'année 2021 sera également marquée par le lancement au FIC du label ExpertCyber. Ce label a vocation à apporter une reconnaissance des compétences des professionnels de la cybersécurité et garantir un accompagnement de qualité ainsi qu'une meilleure lisibilité des prestations et services aux publics professionnels (entreprises, associations, collectivités).

Plusieurs nouveaux supports de sensibilisation aux bonnes pratiques de la cybersécurité et d'assistance face aux cybermenaces en cours de finalisation seront également publiés dans les prochains mois.

Enfin, de nombreux projets sont en gestation avec nos membres en bilatéral

ou réunis au sein de groupes de travail.

Pour faire face à la problématique de la cybermalveillance, une démarche collaborative et collective avec tous les acteurs impliqués est indispensable, car il serait évidemment illusoire de penser que l'on puisse vaincre seul ce fléau. Qu'il s'agisse des pouvoirs publics, des acteurs de la société civile ou même du simple citoyen, chacun peut avoir un rôle à jouer et une contribution à apporter en fonction de ses prérogatives et moyens dans la prévention et l'assistance aux victimes de la cybermalveillance. A ce titre, le dispositif Cybermalveillance.gouv.fr joue un rôle majeur en concentrant et fédérant les énergies et bonnes volontés pour en amplifier les effets au service de la mission d'intérêt public qui lui a été assignée par L'État.

## À propos de Cybermalveillance.gouv.fr

Lancé en octobre 2017, Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes de cybermalveillance. Ce dispositif a été incubé par l'Agence nationale de sécurité des systèmes d'information (ANSSI) en copilotage avec le ministère de l'Intérieur et avec le soutien des ministères de l'Économie et des Finances, de la Justice et du secrétariat d'État chargé du Numérique. Il est désormais piloté par le Groupement d'Intérêt Public (GIP) ACYMA.

### SES PUBLICS SONT :

- les particuliers
- les entreprises (hors opérateurs critiques – OIV)
- les collectivités (hors opérateurs critiques – OIV)

### SES MISSIONS SONT :

- l'assistance aux victimes d'actes de cybermalveillance
- l'information et la sensibilisation au niveau national sur la sécurité numérique
- l'observation du risque numérique pour pouvoir l'anticiper

### SES MEMBRES SONT :



## L'AUTEUR

Impliqué dans la sécurité numérique depuis de nombreuses années, Jérôme Notin dispose d'expériences dans la création et la direction d'entreprises. Il a rejoint l'ANSSI en mai 2016 en qualité de préfigurateur du dispositif et a été nommé, en mars 2017, directeur général du GIP ACYMA lors de sa création. Il est par ailleurs ancien gendarme auxiliaire (94/10 PSIG de Blois) et réserviste citoyen de défense et de sécurité de la Gendarmerie nationale.

# TERRITOIRES ET DÉMARCHE COLLABORATIVE



## UNE CONVERGENCE D'INTÉRÊTS POUR UNE CYBERSÉCURITÉ DE TERRITOIRES NUMÉRIQUES

Les territoires d'influence diffèrent des limites administratives : bassins d'emplois, agglomérations, réseaux de communication, etc. Un territoire est constitué d'acteurs à l'activité imbriquée, porteurs d'intérêts communs ou divergents. Maint d'entre eux : établissements, PME et PMI et indépendants, gèrent des données sensibles et ne perçoivent pas qu'ils constituent des cibles privilégiées. Une mobilisation pour asseoir une cybersécurité ne peut que reposer sur un mode collaboratif. Elle doit fédérer tous les acteurs, responsables territoriaux (maires, présidents d'intercommunalités, préfets, Gendarmerie nationale) ou de secteurs économiques (associations professionnelles, dirigeants d'entreprises, syndicats mixtes spécialisés,...). Le cyberspace permet une convergence objective : des acteurs, aux intérêts hétérogènes, peuvent se rassembler sur un projet pour produire une action numérique, multimodale selon leurs besoins, et co-produire une architecture de cybersécurité. Il se pose, en conséquence, la question du niveau territorial efficient et d'un seuil critique de ressources humaine et financière permettant de se doter des structures et des compétences propres à instaurer une sûreté des systèmes d'information.



# Cybersécurité collaborative

## des territoires

Par Olivier Kempf

L

La cybersécurité collaborative est à l'ordre du jour. Pourtant, elle est aujourd'hui surtout une préoccupation des grandes structures, publiques ou privées, qui cherchent une approche à 360 degrés de leur cybersécurité. Or, les territoires ont aussi besoin de cybersécurité et force est de constater qu'ils sont loin de pouvoir mettre en œuvre des politiques de sécurité des systèmes d'informations. Pourtant ils sont autant victimes que d'autres et leur situation nécessite

également une approche multi-acteurs. En conséquence la cybersécurité des territoires ne pourra être que collaborative. C'est le cœur du programme du nouvel Institut national de la



**OLIVIER KEMPF**

Docteur en science politique  
Vice-président  
de l'INCRT

cybersécurité et la résilience des territoires<sup>(1)</sup> (INCRT) : aller écouter les

(1) <https://www.cyberterritoires.fr/>

besoins et tenter de trouver les réponses adaptées et concrètes à chaque situation.

### La Cybersécurité collaborative, préoccupation des grosses structures

Il n'existe à vrai dire pas de définition agréée de la cybersécurité collaborative. Constatons tout d'abord que nombre de pratiques du cyberspace sont fondées sur des méthodes collaboratives, permises d'ailleurs par des outils mis à la disposition de tous : ainsi, Wikipedia (comme tous les processus Wiki) part de la contribution de beaucoup pour fonder, petit à petit, un corpus encyclopédique désormais reconnu, malgré les quelques critiques qu'il peut encore susciter.

De même, le phénomène des logiciels en source ouverte (open source) part

(2) [http://www.senat.fr/espace\\_presse/actualites/201606/quelle\\_supervision\\_internationale\\_de\\_li-cann.html](http://www.senat.fr/espace_presse/actualites/201606/quelle_supervision_internationale_de_li-cann.html)

(3) <https://www.diplomatie.gouv.fr/fr/politique-et-rangere-de-la-france/diplomatie-numerique/les-domaines-d-action-de-la-diplomatie-numerique-francaise/garantir-la-securite-internationale-du-cyberespace-a-travers-le-renforcement-de/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la>

du principe que tout un chacun peut contribuer à l'élaboration puis à l'amélioration du code logiciel mis à disposition (gratuitement) du public. En termes de sécurité, d'aucuns pensent d'ailleurs que cette ouverture du code, en évitant structurellement les portes dérobées et autres failles cachées, permet donc une meilleure sécurité. Enfin, en termes de gouvernance du cyberspace, beaucoup ont reproché la mainmise

des grands Etats ou des grands acteurs de l'Internet. Ainsi, la notion d'approche « multi-acteurs » a été promue il y a quelques années lors des débats sur la gouvernance de l'ICANN<sup>2</sup>. Une telle approche a d'ailleurs été reprise récemment lors de l'appel de Paris<sup>3</sup>.

Cette diversité d'exemples montre que le monde numérique connaît, depuis longtemps, les méthodes collaboratives. Elles existent également dans le domaine spécifique de la cybersécurité. Le cyberspace permet tout d'abord des phénomènes de coalescence : divers acteurs, à l'origine ayant des intérêts divergents, se rassemblent sur tel ou tel projet pour produire une action numérique, positive ou négative selon leur mobile. Le premier exemple

qui vient à l'esprit est celui des *Anonymus*. Même s'ils ont perdu un peu de relief ces dernières années, ils s'assemblaient pour une cause qui leur semblait juste et visaient une cible de façon à lui faire corriger son comportement.

De même, on pourrait parler d'insécurité collaborative en pensant aux groupes de pirates qui s'assemblent pour augmenter leurs chances d'atteindre leurs cibles. Les dénis de service distribué (DDOS) constituent eux aussi des processus collaboratifs, puisque l'agresseur mobilise de nombreuses machines pour faire converger des requêtes sur la cible. De même, une des sources importantes d'insécurité vient de la mobilisation de machines utilisées à distance (sans la

(4) Le minage c'est le procédé par lequel les transactions Bitcoin sont sécurisées. A cette fin, les « mineurs » effectuent avec leur matériel informatique des calculs mathématiques pour le réseau Bitcoin. Comme récompense pour leurs services, ils collectent les bitcoins nouvellement créés ainsi que les frais des transactions qu'ils confirment.

connaissance de leur propriétaire) afin de miner<sup>4</sup> du bitcoin. Il y a ainsi de multiples façons de faire travailler des ordinateurs ensemble pour réaliser des actions illégales et construire une cyberinsécurité collaborative.

À l'inverse, des hackers blancs peuvent contribuer à la cybersécurité coopérative au moyen des systèmes de *Bug Bounty*, qui permettent à des individus de tester les failles de telle ou telle société qui le demande, avec récompense à la clef. Cette diversité constitue un atout



qui vient compléter les processus plus usuels de sécurité intégrée (*Security by design et Devsecops*) ou l'utilisation de sociétés d'audit qui font des tests de pénétration. Fondamentalement, on ne saurait réduire la cybersécurité collaborative à ces seuls exemples des logiciels en source ouverte ou des *Bug bounty*.

Elle désigne la coopération d'acteurs de niveaux différents, qu'ils soient au sein de l'organisation ou entre organisations de pied différent. Il peut s'agir de la coopération entre l'échelon de direction, les spécialistes techniques (DSI et RSSI) et les divisions techniques (production, marketing, communication). Cela peut surtout concerner la coopération entre des organisations du même secteur, le régulateur ou les autorités locales, les spécialistes du numérique (infrastructures, plateformes, grands comptes), les fournisseurs, les partenaires et les clients. Tous ont un point de vue et un intérêt bien différents mais partagent aussi une bonne sécurité de leurs systèmes (matériels, logiciels, données). Pour autant, bien peu sont prêts à faire l'effort nécessaire et chacun a tendance à reporter sur l'autre la responsabilité de cette sécurité et son coût associé. Pourtant, chacun participe à un certain écosystème et contribue à sa résilience, un des attributs de la cybersécurité.

### Les territoires ont un grand besoin de cybersécurité

Il reste que cette approche s'intéresse dans les faits aux grands organismes : États, grandes sociétés, OIV, grosses ETI, régions. L'échelon inférieur est négligé. Les spécialistes de la cybersécurité parlent bien sûr des individus (citoyens, consommateurs, usagers), ils s'intéressent aussi à leurs collaborateurs à qui il faut enseigner les règles d'hygiène numérique, mais cela ne va guère au-delà. C'est pourquoi il nous semble intéressant de partir de l'échelon du territoire pour aborder cette question de la sécurité collaborative. Constatons simplement qu'en fait, seule la collaboration peut permettre de faire émerger une certaine cybersécurité dans les territoires.

Tout d'abord, qu'est-ce qu'un territoire ? Disons pour commencer ce qu'il n'est pas : ce ne peut être une des très grosses agglomérations urbaines supérieures à 200 ou 300 000 habitants. À ce niveau de population et de densité, la problématique du responsable sera proche de celle d'un grand compte, public ou privé. Il aura un service informatique conséquent et une équipe constituée de spécialistes de la SSI, avec des outils appropriés à la défense de ses SI.

Dès lors, tout ce qui est en dessous répond à cette approche des territoires : il peut s'agir de l'échelon départemental, dont on a vu pendant la pandémie

qu'il avait une dimension optimale pour avoir d'une part assez de moyens d'action, d'autre part une proximité avec population que des plus grosses entités (les régions, l'Etat) n'ont pas. Il semble qu'il s'agit de l'échelon principal de résilience, quelle que soit la crise, sanitaire, catastrophique ou cyber.

Il peut s'agir ensuite des agglomérations moyennes, d'une taille entre 50 000 et 200 000 habitants : elles sont souvent structurées autour d'un pôle, qui n'est d'ailleurs pas forcément le chef-lieu du département et qui ordonne le territoire alentours. Cette notion est très contingente et empêche toute généralisation.

Le territoire d'influence dépend de plusieurs facteurs qui coïncident rarement avec les limites administratives : bassin d'emploi, situation économique et démographique, présence d'une agglomération concurrente à proximité (à plus ou moins de 50 km), structure des réseaux de communication (autoroutes, TGV), etc. Enfin, les agglomérations ont déjà des structures existantes de coopération, celles des établissements publics de coopération intercommunale (EPCI) et notamment des communautés d'agglomération.

Or, si le chef-lieu du territoire, à l'échelon de la ville, peut éventuellement avoir la taille suffisante pour conduire une politique de sécurité des systèmes d'information (PSSI), très rares sont les exemples de commu-

nautés d'agglomération qui s'en sont dotée. Pourtant, la communauté permet de rassembler de nombreuses communes limitrophes, d'une dizaine à plus d'une centaine selon les cas, mobilisant une population plus importante et exerçant une influence élargie sur le territoire et son environnement. Surtout, l'agglomération permet d'inclure des petites communes qui ont rarement par elles-mêmes la taille et les compétences pour définir et conduire une PSSI. Le plus souvent, ces communes comptent moins d'une dizaine de milliers d'habitants avec souvent une double préoccupation : celle de la proximité de la grande ville et celle d'une histoire rurale qui demeure prégnante.

Or, les communes sont comme les autres des victimes potentielles de cyberagressions : elles manipulent de nombreuses données sensibles, elles ont des budgets et font l'objet comme d'autres entités de rançonnages ou de rumeurs. La taille importe peu et l'on a constaté que même

(5) Pour avoir un point des différentes agressions contre les communes, voir O. Kempf, « Cybersécurité et résilience, les grandes oubliées des territoires », Notes de la FRS n° 30/2020, 14 mai 2020.

des petites communes étaient la cible de rançonnage<sup>5</sup>. Or, les édiles sont aujourd'hui peu sensibilisés à ces questions et s'imaginent, comme beaucoup de PME et PMI, que la commune est trop

petite pour constituer une cible. Funeste erreur, trop souvent partagée dans le monde économique, qui fait pourtant des dégâts.

Ne réduisons pourtant pas les territoires à leurs seules structures publiques, des EPCI aux différents syndicats mixtes. Les territoires incluent évidemment une population mais aussi une activité économique, constituée parfois de gros établissements, plus souvent de beaucoup de PME et PMI mais aussi d'indépendants. Certains de ceux-ci manient des données sensibles (notaires, médecins, comptables, pharmaciens, huissiers). Or, la plupart font confiance à un prestataire informatique de proximité, le plus souvent compétent en matière informatique mais plus rarement pour les questions de cybersécurité.

### La cybersécurité des territoires nécessite la collaboration

Un territoire est donc constitué de plusieurs acteurs à l'activité intriquée, des intérêts évidemment communs mais des préoccupations également divergentes. Il serait vain de demander à chacun de faire un effort si celui-ci n'était pas coordonné. La conclusion est évidente : dans un territoire, la cybersécurité ne peut être que collaborative. Elle doit mobiliser tous les acteurs, ceux responsables du bien public (maires, présidents d'intercommunalités, préfets, Gendarmerie nationale), mais aussi ceux ayant des préoccupations plus économiques (associations professionnelles, dirigeants d'entreprises locales, syndicats mixtes spécialisés).

Il faut d'abord écouter les besoins et mener des actions de sensibilisation. L'ANSSI a

ainsi mis en place une organisation territoriale, avec des délégués en région, et elle a récemment publié un guide consacré à l'essentiel de la réglementation de

(6) ANSSI, janvier 2020, « Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation ».

(7) <https://www.pole-excellence-cyber.org/presentation-du-pole/>

cybersécurité à destination des collectivités territoriales<sup>6</sup>. Le Pôle d'Excellence Cyber<sup>7</sup> a également rendu public, en novembre 2020, un guide pratique de cybersécurité des collectivités territoriales.

Certaines initiatives ont vu

le jour, comme celles de la Gendarmerie nationale dans le Morbihan (Hermès 56) ou encore certaines étapes du Cybercerclé en province, tandis que *cybermalveillance.fr* développe des actions décentralisées de sensibilisation ou que le magazine Acteurs publics publie régulièrement des articles sur le sujet. De même, quasiment toutes les régions ont lancé des initiatives sur la cybersécurité. Il faudra ensuite recenser l'existant, variable d'un territoire à l'autre, certains s'étant déjà saisis du problème alors que d'autres n'en sont qu'aux premières étapes de la prise de conscience. Enfin, il faudra imaginer des projets concrets, adaptés à chaque situation. La notion de « solution », souvent utilisée par des grands éditeurs de logiciels, s'applique finalement assez peu en la matière.

Il reste que ce travail doit être conduit car à l'heure du télétravail généralisé et de la néo-ruralisation (ou plus exacte-

ment, la sortie des grandes métropoles), la dimension numérique des territoires constitue un aspect essentiel de leur attractivité économique. Or, la cybersécurité constitue désormais une dimension essentielle de cette attractivité numérique. Souvent considérée comme un centre de coût, la cybersécurité est en train de devenir un centre de profit. On ne peut pas lancer de grands projets de *Smart city* sans inclure une forte dimension de cybersécurité.

Après les nombreuses initiatives lancées depuis une quinzaine d'années et la constitution d'un solide dispositif national (ANSSI, Livre blanc sur la cybersécurité, OIV, Pôle d'excellence cyber, COM CYBER, cybermalveillance.fr, Forum FIC, campus cyber, etc.), il est temps désormais de s'intéresser au maillage territorial de notre pays et de construire la résilience cyber et économique de cet écosystème.

## L'AUTEUR

Docteur en science politique, chercheur associé à l'IRIS, directeur de la lettre stratégique La Vigie, Olivier Kempf est consultant en stratégie digitale. Olivier Kempf est vice-président de l'INCRT. Il a publié avec François-Bernard Hyughe et Nicolas Mazzucchi : *Gagner le cyberconflit, au-delà du technique* (Economica, 2015, 175 pages). Olivier Kempf est l'auteur de : *Introduction à la cyberstratégie* (Economica, 2012) et *Alliances et mésalliances dans le cyberspace* (Economica, 2014).

## INCR.T

L'Institut National de la Cybersécurité et de la Résilience des Territoires (INCR.T) a été créé avec esprit et l'ambition d'être au plus près des territoires, de les accompagner et de les mettre en réseau, de promouvoir des réponses simples et pragmatiques, d'assurer une veille et de conduire des études pratiques répondant aux besoins identifiés. Il a vocation à aller là où les autres ne vont pas pour écouter ceux que l'on écoute peu et trouver à leurs côtés les moyens de construire, par le bas et de façon adaptée à chaque situation locale, une cybersécurité de terrain, forcément collaborative. L'INCR.T a pour président le Général d'Armée (2S) Watin-Augouard, ce qui garantit non seulement une profonde expérience des questions de cybersécurité mais aussi une connaissance fine des besoins des territoires.





# TERRITOIRES ET DÉMARCHE COLLABORATIVE

© Fotolia\_117874214\_Subscription\_XXL

## UNE PARTENARIAT PRIVÉ – PUBLIC SANS COMPLEXES

Un partenariat Public - Privé abouti permet de combiner des potentiels en matière de cybersécurité. Déjà engagé dans la pratique, il met en scène un Etat, fort de ses prérogatives régaliennes et de la puissance « historique » de ses institutions, qui appuie la sphère privée. Il profite en retour des capacités d'innovation de cette dernière, dictées par les règles concurrentielles, et d'une adaptation rapide aux évolutions du marché. Dans ce cadre, on peut privilégier trois axes de collaboration : la formation et les financements associés au maintien d'un continuum de recherches.

Dans les territoires, on peut envisager une mutualisation de moyens qui se trouvent à l'interface : État, Economie et Politique. Ce dispositif pourrait faciliter la relation avec les services de l'État en charge de la sécurité (prévention cyber, sécurité économique, plateformes spécialisées, etc.) et répondre aux attentes des entreprises et des collectivités territoriales. Il permettrait aux forces de sécurité de prendre la mesure de l'état de la menace cyber par un dialogue direct et permanent.

Cette combinaison de compétences passe également par des passerelles entre le Privé et le Public. Les experts y verront une alternance professionnelle valorisante et naturelle dans un parcours enrichi. Ces échanges auraient vocation à contribuer à l'intérêt général et à générer de nouveaux mécanismes économiques. Cette nouvelle forme collaborative passe cependant par des échanges privé-public décomplexés.

# Les partenariats

## public-privé en Cybersécurité

Par Cyril Bras

# N

**Note du rédacteur en chef : Cet article est un focus sur les travaux de la 2<sup>e</sup> session nationale « Souveraineté numérique & Cybersécurité de l'IHE-DN et l'INHESJ » sur les intérêts et les limites du partenariat public-privé. Les membres du groupe de travail sont dans l'ordre alphabétique : Cyril Bras, Rémi de Gouvion Saint-Cyr, Ludovic Haye, Brunon Le Jossec & Dominique Lestrade. Son intérêt a retenu notre attention. Rapporteur de ces travaux, Cyril Bras a bien voulu en retracer les problématiques essentielles qu'ils soulèvent en répondant à nos questions.**



**CYRIL BRAS**

Responsable RSSI  
Grenoble-Alpes  
Métropole.  
Ville de Grenoble  
et CCAS

### Comment définir le partenariat public/privé en Cybersécurité ?

Le contrat de partenariat public privé (PPP)

est un contrat administratif par lequel l'État ou une autorité publique confie à un prestataire privé la gestion et le financement d'équipements, d'ouvrages permettant d'assurer un service public.

Au-delà de cette définition générale, nous pouvons remarquer que des partenariats existent déjà dans le domaine de la Cybersécurité ; le FIC en est quelque part une illustration concrète.

C'est d'ailleurs au cours du FIC 2020 que Guillaume Poupard, directeur général de l'ANSSI, donnait sa perception de l'impérieuse nécessité d'une collaboration

« L'idée, c'est que le privé seul n'a pas la solution, le public non plus. On croit donc que la solution se trouve dans l'alliance des deux<sup>1</sup> ».

Ce partenariat permet la combinaison des forces et spécificités de ces deux

(1) L. Adm, « FIC 2020 : « Le privé seul n'a pas la solution, le public non plus », 29 Janvier 2020. [En ligne]. Available: <https://www.zdnet.fr/actualites/fic-2020-le-privé-seul-n-a-pas-la-solution-le-public-non-plus-39898215.htm> . [Accès le 25 Février 2020].



entités. L'État assure des missions de service public, la justice et la défense entre dans ses prérogatives régaliennes. Le secteur privé pour assurer sa survie face à la concurrence est une source continue d'innovations.

D'une certaine façon notre groupe de travail en est aussi une illustration puisque nous sommes issus des sphères publiques et privées.

### Outre le FIC, avez-vous des exemples de partenariats déjà en place ?

(2) T. de Coatpont, « La collaboration public-privé, nouvelle arme de la cybersécurité ? » 22 Mars 2019. [En ligne]. Available: <https://business.lesechos.fr/directions-numeriques/> [Accès le 25 Février 2020].

(3) UnderNews Actu, « La gendarmerie (C3N) met fin au botnet Retadup – 800 000 machines zombies, » 28 Août 2019. [En ligne]. Available: <https://www.undernews.fr/malwares-virus-antivirus/la-gendarmerie-c3n-met-fin-au-botnet-retadup-800-000-machines-zombies.html>. [Accès le 23 Mai 2020].

Le projet « No More Ransom », initié en juillet 2016, associe les acteurs publics de lutte contre la cybercriminalité et ceux du privé afin de détecter les attaques et d'apporter des solutions aux victimes<sup>2</sup>.

Nous pouvons également mentionner le démantèlement du Botnet Retadup, en août 2019, par la Gendarmerie Nationale en lien avec le fabriquant d'Antivirus Avast<sup>3</sup>, ce dernier fournissant les éléments techniques pour conduire l'enquête.

(4) Lorsque l'on parle de hack back, il s'agit d'une défense agressive, allant au-delà de ses propres systèmes. Les Etats-Unis travaillent à une formule qui donnerait à une entreprise un droit d'autodéfense cyber et d'attaquer le système qui serait à l'origine de l'intrusion.

(5) M. Duault, « Qu'est-ce que le Visa de sécurité délivré par l'ANSSI ? » 2018. [En ligne]. Available: <https://yousign.com/fr-fr/blog/visa-de-securite-anssi>. [Accès le 23 Mai 2020].

(6) RTBF.BE, « Un partenariat public-privé permet à 12 Bruxellois d'être diplômés en cybersécurité, » 20 Février 2020. [En ligne]. Available: [https://www.rtbf.be/info/regions/bruxelles/detail\\_un-partenariat-public-privé-permet-a-12-bruxellois-d-etre-diplomes-en-cybersecurite?id=10430222](https://www.rtbf.be/info/regions/bruxelles/detail_un-partenariat-public-privé-permet-a-12-bruxellois-d-etre-diplomes-en-cybersecurite?id=10430222). [Accès le 25 Février 2020].

Comme évoqué précédemment, certaines activités relèvent de la sphère étatique exclusive comme par exemple le « hack back »<sup>4</sup>. Cependant, il convient d'y associer les acteurs privés de la résilience cyber. Pour ce faire, les visas attribués par l'ANSSI<sup>5</sup> permettent notamment de garantir un niveau de confiance pour les utilisateurs publics de solutions de sécurité développées par des acteurs privés. Le privé apporte alors une partie de la solution au public.

Enfin nous pouvons encore citer une expérience menée à Bruxelles entre des entreprises privées et le ministère de l'emploi afin d'aider à la reconversion et à la réinsertion professionnelle vers le secteur de la Cybersécurité<sup>6</sup>.



© 132377290 Public Partnership concept on the gearwheels,  
3D rendering par Alexlmx – Adobe stock

Les sphères opérationnelles du secteur public et privé peuvent générer, par une interaction favorisant le partage d'expertises, de financements et de ressources humaines, des projets collaboratifs efficaces en matière de cybersécurité.

### Si ces partenariats existent déjà, quel apport donnerait une plus-value à ces interactions ?

Nous avons constaté de fortes disparités tant au niveau du public que du privé sur la prise en considération de la Cybersécurité. Les petites structures (PME-PMI, collectivités territoriales...) ne sont pas forcément aussi bien préparées à faire face à la menace cyber que de grands groupes ou tout simplement elles n'ont pas les moyens de mettre en œuvre les mesures nécessaires pour y faire face. Nous avons donc identifié 3 axes de coopération : la formation de la ressource humaine, sa mise à disposition par le biais de financements agiles et enfin

la garantie d'un continuum de compétence (recherche / public / privé).

### Actuellement le marché du travail en Cybersécurité est en tension, comment le secteur public peut-il attirer des talents ?

Le secteur public est en effet pénalisé par ses processus de recrutement ou ses conditions salariales. Certes, ce secteur propose des missions intéressantes mais qui ne suffisent pas toujours à compenser les rémunérations proposées dans le secteur privé. Dans le même temps ce dernier recherche des profils disposant de compétences qui ne peuvent être

acquises que dans les missions proposées par les services étatiques. Une de nos propositions consiste à ce que des entreprises privées apportent une contribution financière visant à verser un salaire aux étudiants pendant leur formation, à l'image des écoles militaires. Cet effort financier se poursuit dans un premier emploi au sein de L'État en apportant un complément au salaire pour le rendre attractif. En échange, l'étudiant s'engage à servir l'État pour une durée déterminée (5 ans). À défaut, il devra rembourser les frais de sa scolarité et les indemnités perçues. Ensuite, il pourra se voir proposer un poste dans une des entreprises qui a soutenu financièrement sa formation, avec une durée d'engagement. L'indemnité de rupture se calculera alors au prorata du temps passé en entreprise.

### Cette première solution s'applique plutôt aux grandes entreprises.

Dans vos réponses précédentes vous évoquiez la nécessité d'aider les petites structures, que proposez-vous dans ce cas ?

(7) B. Bellanger, « Baromètre des TPE/PME dans l'économie française en 2019, » 21 Janvier 2020. [En ligne]. Available: <https://solutions.lesechos.fr/comptage/c/> [Accès le 05 Aout 2020].

Le tissu économique français est en effet constitué de 99.9% de TPE/PME<sup>7</sup> qui sont de plus en plus victimes de cybermalveillances. Dans la plupart des cas, elles ne disposent pas des ressources nécessaires

pour se protéger contre cette menace,

quand celle-ci n'est pas tout simplement méconnue. Ce constat s'applique également aux petites collectivités.

Dans ce cas, nous proposons la mutualisation de moyens au travers d'acteurs locaux tels que les chambres consulaires, les agences locales de développement économique qui se trouvent à l'interface « État /Economie/Politique ». Ainsi, des petites entités pourraient contribuer financièrement au recrutement d'un RSSI qui serait alors mutualisé entre les différentes structures. Ce dispositif pourrait également faciliter la mise en relation avec les services de l'État en charge de la sécurité (prévention cyber, sécurité économique...) pour répondre aux attentes des entreprises mais aussi fournir du renseignement sur l'état de la menace pour la Gendarmerie nationale, la Police nationale et le GIP ACYMA.

### Reste-t-il d'autres pistes à explorer ?

Oui, nous pensons également qu'il faudrait repenser la réserve cyber en la rapprochant des territoires et de leurs acteurs.

Il conviendrait pour cela de dynamiser la réserve citoyenne et d'en faire un lien fort entre les sphères publique et privée. Elle pourrait partager des bonnes pratiques de Cybersécurité, participer à des actions de prévention ou d'investigation mais aussi apporter des compétences autres que cyber (intelligence économique, escroquerie financière ou encore travail illégal). Elle pourrait prendre exemple sur

l'expérimentation HERMES menée par le groupement du Morbilhan (56) ; ce dernier assiste les entreprises du département en leur proposant des conseils contre les menaces physiques et numériques ou encore en intelligence économique. Pour cela, l'introduction d'un niveau de confidentialité adapté et encadré par des dispositions réglementaires devra être mis en œuvre. Il conviendra également d'accepter un ancrage dans les territoires malgré la distance avec le cadre de l'ANSSI et du Comcyber. La gendarmerie a désigné des correspondants régionaux pour ses réserves numériques et cyber.

### Quelques mots pour conclure ?

Sans bouleverser les grands équilibres qui tiennent à la nature profonde des entités publiques et privées, il est possible de trouver dans les zones de contact entre les populations de ces deux sphères des partenariats enrichissants. Qu'il s'agisse d'une ressource qui a vocation à dessiner un parcours professionnel alternant les deux mondes, de personnels du privé qui souhaitent apporter leur contribution à l'intérêt général ou encore de mécanismes économiques qui permettent d'échanger des outils contre une plus forte souplesse en termes de charges, une grande variété de partenariats se dessine.

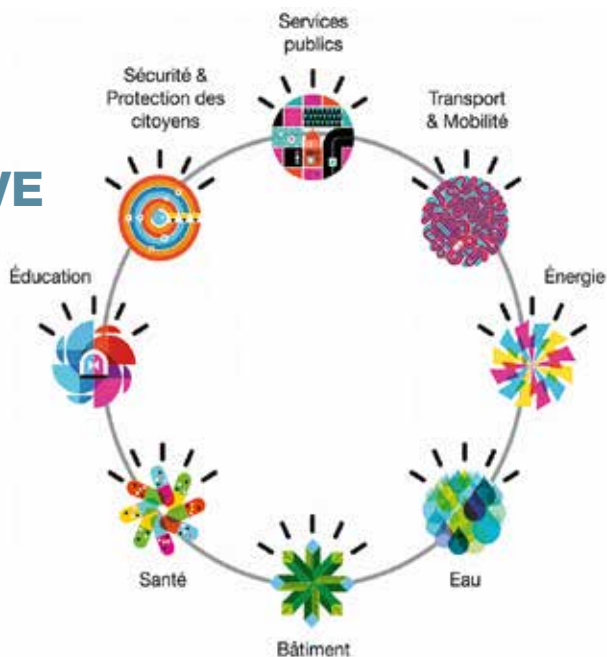
Une forte volonté politique semble nécessaire pour mettre en route ces mesures, lever les réticences des entreprises et décomplexer les échanges privé-public.

La transformation numérique engagée en France doit se faire en lien avec la Cybersécurité qui reste le gage de confiance dans l'usage du numérique. La crise sanitaire actuelle a confirmé cette impérieuse nécessité.

### L'AUTEUR

Cyril Bras remplit les fonctions de RSSI de la métropole grenobloise depuis mars 2018. Il est auditeur de la 2<sup>e</sup> session nationale Souveraineté numérique et Cybersécurité IHEDN & INHESJ. Il est par ailleurs enseignant vacataire auprès de l'université Grenoble Alpes et intervenant auprès du CNFPT.

# TERRITOIRES ET DÉMARCHE COLLABORATIVE



© Map, par BillionPhotos.com

## COLLECTIVITÉS TERRITORIALES : MAÎTRISE DES DONNÉES ET POLITIQUE PUBLIQUE PARTENARIALE

La question de la maîtrise du cycle de vie des données sensibles touche toutes les activités sociétales et place les collectivités territoriales devant une forte responsabilité.

Outre la cartographie des données et de leur usage, il importe de les sécuriser. Cela concerne le régime contractuel de leur stockage, via des prestataires privés et une vision collaborative des usages. Les administrations doivent ouvrir un accès régulé à leurs données sans pour autant renoncer au pilotage de leurs politiques publiques. Il importe donc que le pilotage des projets, dans le cadre de partenariats « Privés – Collectivités territoriales », s'inscrivent dans une vision d'intérêt général et d'adéquation aux besoins de la population. L'usage des données étant encadré juridiquement, les modèles de développement doivent être définis en conséquence pour servir de support aux projets innovants. La difficulté rencontrée dans la mise en œuvre des politiques publiques est d'en trouver les leviers d'action juridiques et financiers.

# Les données publiques

## territoriales

Par Jérôme Buzin

# A

Alors que la crise sanitaire met en avant l'importance du numérique, tant pour son influence sur le développement économique que pour son apport à la résilience de l'activité, les questions de souveraineté sont revenues au premier plan. Souveraineté alimentaire, médicale, des approvisionnements stratégiques, mais aussi numérique. Qui collecte, stocke ou traite nos données ? La question de la maîtrise de nos données sensibles et stratégiques touche l'ensemble des activités de notre vie



**JÉRÔME BUZIN**

Administrateur  
général des données  
Métropole  
européenne de Lille

quotidienne. Les collectivités territoriales gèrent tous les jours des quantités énormes de données relatives à l'environnement, la voirie, les transports, la gestion de l'eau, l'énergie, les déchets, l'habitat, le développement éco-

nomique, l'éducation, la recherche, etc. Afin de promouvoir et améliorer leurs politiques publiques, les collectivités territoriales ont donc la nécessité d'agir sur l'ensemble du cycle de vie de leurs données.

### Une culture du partage des données pour arriver à une efficience des traitements

Cela commence avec la connaissance de ces données, qu'elles soient produites directement par les services de la collectivité ou par d'autres acteurs. Cela implique de dresser et tenir à jour une cartographie et de mener une veille qui porterait également sur les usages. À ce stade, les premiers obstacles peuvent se dresser. Les services publics ont l'obligation de mettre à disposition leurs données gratuitement aux autres administrations mais les entreprises n'y sont pas soumises et peuvent s'avérer réfractaires, y compris dans le cadre de marchés publics

ou de délégations de services publics (DSP). La situation évolue, notamment

(1) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

grâce à la notion de données d'intérêt général introduite par la loi Lemaire<sup>1</sup>. Cependant,

la réalité est qu'aujourd'hui les collectivités doivent négocier et insister pour obtenir des données auprès de leurs partenaires privés.

Par ailleurs, les capteurs permettant de recueillir une partie des données sur le territoire sont d'une extrême diversité, tant dans leurs protocoles d'échanges que dans les réseaux de communication utilisés, et ils n'offrent pas toujours la possibilité de les administrer et les sécuriser.

### La question contractuelle au cœur du régime juridique de la gestion de la donnée

Le stockage des données collectées représente le second point d'achoppement pour les collectivités territoriales. En effet, si certaines ont les moyens d'opérer à partir de leur propre centre de traitement de données, la plupart doivent s'appuyer sur des partenaires privés. Cela n'est pas un mal en soi, au contraire, à condition que le contrat permette le respect de l'ensemble des contraintes réglementaires qui s'appliquent aux données stockées. Il faut également qu'il soit équitable et qu'il ne place pas la collectivité dans une situation d'impuissance. Cela implique en particulier de permettre la récupération ou

le transfert des données facilement vers un concurrent, ce qui est loin d'être le cas aujourd'hui. Ces aspects sont notamment au cœur du projet franco-allemand GAIA-X dont on ne peut que souhaiter la réussite.

Un autre aspect problématique lié à la situation de dépendance vis-à-vis de certains acteurs réside dans leurs conditions contractuelles et en particulier dans le fait que certains de ces acteurs s'arrogent le droit de les modifier unilatéralement comme l'a dénoncé le Contrôleur européen de la protection des données<sup>2</sup>.

(2) [https://edps.europa.eu/sites/edp/files/publication/20-07-02\\_edps\\_euis\\_micro-soft\\_contract\\_investigation\\_en.html](https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_micro-soft_contract_investigation_en.html)

Associée au point précédent qui place les collectivités dans une dépendance technique, cette pratique revient

dans les faits à vassaliser les clients qui ne peuvent que subir les nouvelles conditions contractuelles sans réelle capacité à sortir du contrat pour se tourner vers un concurrent.

### Une vision collaborative des usages

Le dernier volet de la stratégie des collectivités territoriales concerne la maîtrise des usages. Les grands acteurs du numérique se sont tous positionnés d'une façon ou d'une autre sur ce terrain du territoire connecté. En effet, selon

(3) <https://www.grandviewresearch.com/press-release/global-smart-cities-market>

*Grand View Research*, le marché de la Ville intelligente pourrait atteindre plus

de 460 milliards de dollars d'ici 2027<sup>3</sup>.





© Par metamonworks - Adobe stock

La sensibilité des données gérées par les collectivités territoriales et l'interaction de celles-ci avec les opérateurs privés nécessitent un cadre contractuel maîtrisé de leur stockage et usage en accord avec un cadre juridique national et européen.

La démarche de ces acteurs privés peut se faire en partenariat avec les collectivités territoriales, mais le plus souvent elle les ignorera voire visera à agir à leur place. En effet, nous l'avons vu précédemment, ces acteurs n'ont pas toujours à cœur le respect de la vision du client ou de l'utilisateur.

Imaginons une application mobile qui optimise votre trajet en voiture en s'appuyant sur des informations sur le trafic obtenues grâce à sa communauté d'utilisateurs. Imaginons qu'aux heures de pointe cette application oriente une partie importante du trafic vers des rues, non conçues pour accueillir un tel trafic, où de nombreux enfants entrent ou sortent des écoles. La collectivité territoriale pourrait alors

se tourner vers l'entreprise qui développe l'application pour exposer le problème et demander une adaptation des propositions faites aux automobilistes pour mieux s'accorder à la réalité du terrain, voire coconstruire des modèles de données qui incluraient l'information sur la capacité d'accueil de la voirie ou les heures d'entrée et de sortie des écoles.

Mais comment réagirions-nous si cette entreprise s'estimait porteuse d'une mission de service public et refusait de changer son modèle car cela pénaliserait le temps de trajet de ses utilisateurs ? Serions-nous amusés, choqués ou dans l'acceptation si cette entreprise proposait à la collectivité de modifier les jeux de données qu'elle met à disposition

et qui sont utilisés dans ce cadre pour fermer les rues concernées, en omettant que ces jeux de données sont utilisés pour d'autres usages ? Trouverions-nous acceptable que la situation soit figée parce que la décision se prend en Californie et non pas à l'échelon local ?

(4) <https://siecledigital.fr/2020/02/28/a-toronto-la-grogne-des-locaux-contre-alphabet/>

L'exemple du projet de *Sidewalk Labs* à Toronto<sup>4</sup>, qui a fini par être arrêté, est celui d'un projet

qui n'a pas réussi à concilier la vision de l'entreprise et les attentes des citoyens et de la collectivité.

Face à ces problématiques, les collectivités territoriales cherchent des leviers d'action pour défendre leurs politiques publiques.

Ainsi la métropole du Grand Lyon,

(5) Loi Lemaire, code des relations entre le public et les administrations (CRPA) et le règlement européen 2017/1926 de la Commission du 31 mai 2017, complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition dans l'ensemble de l'Union européenne de services d'informations sur les déplacements multimodaux.

pionnière en matière d'ouverture des données, avait lancé son service OpenData en 2013 avec une licence qui permettait la mise en œuvre d'une redevance modulable en fonction du succès économique de l'application réutilisant les données. Ce modèle était d'ailleurs l'un de ceux proposés par Mohammed

Adnène Trojette, Magistrat à la Cour des comptes, dans son rapport au Premier ministre en juillet 2013. Mais l'évolution du cadre législatif<sup>5</sup> a conduit le Conseil

de la métropole du Grand Lyon à remplacer, le 30 septembre 2019, cette licence par une « licence de réutilisation des données d'intérêt général » qui permet la

(6) [https://download.data.grandlyon.com/files/grandlyon/Licence\\_Reutilisation\\_Donnees\\_Interet\\_General.pdf](https://download.data.grandlyon.com/files/grandlyon/Licence_Reutilisation_Donnees_Interet_General.pdf)

mise à disposition gratuite de la donnée avec authentification du réutilisateur<sup>6</sup>. L'intérêt général est posé comme

principe de cette licence : le/la licencié(e) doit déclarer les utilisations du ou des jeux de données, la Métropole s'assurant qu'elles sont conformes aux politiques publiques.

Désormais, « les Données peuvent être utilisées par toute personne à toutes fins, internes ou externes, commerciales ou non, et notamment en vue :

- de l'information du public ;
- de la réutilisation des Données pour des services, applications ou produits ;
- du développement de services innovants ;
- de l'enseignement et de la recherche.

Sous réserve que :

- leur réutilisation soit compatible avec les politiques publiques mises en œuvre par le Concédant ou par le Producteur et ne porte pas atteinte à l'intérêt général,
- la mention soit faite de la paternité de la Donnée.

Les obligations du Licencié sont établies à l'article 8 de la présente Licence.

De plus, la réutilisation des Données mises à disposition est soumise, sauf accord du Concédant, à la condition que ces Données ne soient pas altérées, que leur sens ne soit pas dénaturé. »

De son côté, Nantes métropole fait le constat que « des données sont aujourd'hui produites en grand volume par la gestion des services publics, par des opérateurs de mobilité, des distributeurs d'énergie, des gestionnaires de déchets et bien d'autres. » et qu'il « est donc essentiel d'encadrer l'utilisation des données produites sur le territoire afin de protéger les citoyens. »

(7) <https://metropole.nantes.fr/charte-donnee>

Elle a donc créé la notion de « données d'intérêt métropolitain » et fédéré

plus de 40 acteurs privés, associatifs et publics pour faire appliquer les engagements et les principes de sa charte de la donnée métropolitaine<sup>7</sup>.

Ces démarches, qui vont dans le sens d'une réappropriation de l'usage des données par les administrations locales dans l'objectif de cohérence avec leur stratégie, sont isolées et peuvent se heurter aux dispositions réglementaires nationales ou européennes.

(8) <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte>

La mission confiée en juin 2020 par le Premier ministre au député Éric Bothorel<sup>8</sup>, dont les conclusions sont

attendues en décembre 2020<sup>9</sup> sera peut-être, il faut l'espérer, l'occasion de définir au niveau national et plus tard européen des outils pour permettre aux collectivités territoriales, et plus globalement aux administrations, d'ouvrir largement leurs données sans pour autant renoncer au pilotage de leurs politiques publiques.

## L'AUTEUR

Après un parcours dans l'administration centrale d'État (ANSSI, ministère de l'Intérieur, ministère de la Justice) et les institutions européennes, Jérôme Buzin est aujourd'hui administrateur général des données de la Métropole européenne de Lille. Sensibilisé à la gestion du risque et aux questions de sécurité, il est auditeur de la première session « Souveraineté numérique et cybersécurité » de l'IHEDN et l'INHESJ.

(9) Avant le FIC2021 mais après le bouclage de cet article.

# TERRITOIRES ET DÉMARCHE COLLABORATIVE



© F. Balsamo - SIRPA-Gendarmerie

## LA RÉSERVE NUMÉRIQUE : UN VIVIER D'EXPERTISES

La « Réserve numérique », ingénierie conçue par la mission numérique de la Gendarmerie nationale (MNGN), entre dans une logique de coordination des projets et de mutualisation des besoins des différents services, centraux comme déconcentrés. Elle associe des réservistes « citoyens », détenant de fortes expertises numériques, à des réservistes « opérationnels », ancrés dans une pratique de terrain, pour participer à des projets ou à leur conduite. À ce titre, les réservistes numériques renforcent les gendarmes d'active pour développer des logiciels ou apporter un conseil. Ils contribuent également à la sécurisation juridique, économique, technique et patrimoniale des projets, aidant ainsi à leur mise en production, à leur déploiement et à leur maintenance évolutive. Des plans d'action pour des besoins régionaux permettent d'élaborer collaborativement des supports de sensibilisation aux cybermenaces, notamment à destination des entreprises, et d'apporter une assistance aux TPE/PME pour qu'elles puissent diagnostiquer leurs vulnérabilités et mettre en place des partenariats.

La réserve numérique, vivier expérimental, est un des leviers du plan stratégique « Gend20.24 » pour faciliter la transformation numérique de la Gendarmerie nationale, accroître sa résilience aux cyber-attaques et la sécurité des « nouvelles frontières numériques ».

# La réserve numérique :

un réseau collaboratif d'experts au service de la transformation numérique de la gendarmerie

Questions à Florence Esselin, Alain Grandjean et David Toulotte

# L

Les réservistes renforcent depuis plusieurs années la Gendarmerie nationale dans le cadre du développement d'outils logiciels et participent ponctuellement à ses réflexions stratégiques en matière de transformation numérique. Avec la création du réseau des réservistes opérationnels et citoyens « numériques », la Gendarmerie nationale expérimente l'emploi

d'un vivier commun, sur site comme à distance et en fonction des compétences pour des missions ponctuelles ou promettant de devenir récurrentes.

L'approche disruptive de la « réserve numérique », qui mêle statuts et grades pour une pluralité et une complémentarité de vues, a déjà apporté de beaux résultats. C'est la raison pour laquelle

la Revue de la Gendarmerie a souhaité éclairer cette nouvelle approche de la cybersécurité avec des acteurs qui reflètent cette diversité et cette convergence d'expertise.



**FLORENCE ESSELIN**

Conseiller expert en numérique et sécurité du numérique. Cabinet du Directeur général de la Gendarmerie nationale.



**ALAIN GRANDJEAN**

Lieutenant-Colonel de Gendarmerie. Division des opérations. Région de gendarmerie des Hauts-de-France.



**DAVID TOULOTTE**

David Toulotte Directeur de projets informatiques Arcelor Mittal. Capitaine de gendarmerie (Réserve opérationnelle).

Florence Esselin, pourriez-vous nous dessiner le périmètre de la réserve numérique et nous expliquer ce

#### qui la différencie de la réserve cyber ?

La « réserve numérique » n'est pas une réserve de plus, c'est le nom d'un réseau qui s'appuie sur la « réserve opérationnelle » et la « réserve citoyenne de défense et de sécurité » (RCDS), définies par le code de la défense. Ce réseau a été initié en 2017 par la mission numérique de la Gendarmerie nationale (MNGN) en liaison avec le commandement des réserves gendarmerie ; il est composé de réservistes « opérationnels » et de réservistes « citoyens », partageant un même intérêt pour le numérique, ses impacts sur la société, ses atouts et ses faiblesses, et pour sa sécurité.

La « réserve cyber » est l'héritière de la « réserve de cyberdéfense » créée conjointement en 2012 par les armées et la gendarmerie ; elle regroupe des réservistes essentiellement intéressés par la cyberdéfense, la cybersécurité et la lutte contre la cybercriminalité. Notre réserve numérique embarque avec elle les réservistes cyber de la gendarmerie du fait d'une évidence : quelle transformation numérique peut-on prétendre mener sans cybersécurité ?

#### Florence Esselin, vous animez la « réserve numérique » depuis 2018. Pourquoi vous a-t-on confié cette mission ?

Quand, en juillet 2018, j'ai rejoint la MNGN au cabinet du directeur général de la Gendarmerie nationale, j'étais déjà membre

de ce réseau. J'étais lieutenant-colonel de la RCDS depuis 2012 et membre de la

(1) Article BEPA-Cyber, la Base d'estimation des potentiels d'attaques Cyber, Revue de la Gendarmerie Nationale N°248 4<sup>e</sup> trimestre 2013.

réserve cyber. Le colonel Éric Freyssinet, chef de la MNGN, connaissait mon travail sur l'échelle de dangerosité des cybermenaces BEPA-Cyber<sup>1</sup> et mon

approche résolument collaborative de la cybersécurité. Dans mon précédent poste (haut fonctionnaire adjoint de défense et de sécurité, fonctionnaire de sécurité des systèmes d'information au cabinet du ministre de la Culture), j'avais créé le réseau des acteurs de la sécurité du numérique de la Culture, à l'appui d'une démarche inédite de co-construction d'une politique de sécurité des systèmes d'information adaptée à la diversité de ce secteur.

Ma modeste connaissance de la Gendarmerie nationale a été heureusement complétée par une vision partielle de l'évolution de ses systèmes d'information. Depuis 2006, j'avais commencé à accompagner la Gendarmerie nationale dans quelques projets, en tant qu'inspecteur à la DCSSI. Cela a duré plus de dix ans, dans un contexte de pleine transformation tant par la création de l'ANSSI que par le rattachement de la Gendarmerie au ministère de l'Intérieur en 2009.

Aussi étais-je ravie et honorée de rejoindre

l'institution pour contribuer à l'élaboration de sa stratégie de transformation numérique et de lutte contre les cybermenaces, en collaboration avec toutes les ressources pertinentes, parmi lesquelles la réserve numérique de la gendarmerie.

### Dans quel esprit développez-vous la réserve numérique ?

Convaincue de l'importance du facteur humain dans la créativité comme dans la cybersécurité, c'est d'abord le lien avec chaque réserviste que j'ai cherché à renforcer, en m'appuyant en partie sur le travail d'animation des officiers d'active ou de réserve désignés comme « coordinateurs réserve cyber » en régions.

(2) La Gendarmerie nationale ne pouvant décemment pas convier ses réservistes à consommer de l'alcool, la grenadine est recommandée comme boisson issue de la transformation de la grenade, fruit mais aussi symbole de l'institution depuis 1795.

Chacun d'eux établit un plan d'action en fonction des effectifs et des profils des réservistes, pour des besoins régionaux et tisse des liens avec son groupe. Pour renforcer la cohésion nationale, j'ai notamment lancé les « rencontres grenadines<sup>2</sup> » - une réunion mensuelle

informelle en visio, pour « papoter » pendant une heure et demie autour d'un thème avec ceux qui sont disponibles en sortant du bureau : les idées fusent, les expériences sont échangées entre les régions, des contacts sont pris pour de nouveaux projets. C'est un forum où se retrouvent des experts juridiques,

des ingénieurs experts, des élèves ingénieurs, des élus locaux, des chefs d'entreprise, des professionnels de la communication, des anciens de l'arme de tous grades ainsi que des généraux en deuxième section, etc. Tous ont en commun leur attachement à la Gendarmerie nationale et la volonté de « Servir ».

### Quel est l'apport des réservistes numériques à la transformation numérique de la gendarmerie ?

Depuis plusieurs années les réservistes renforcent régulièrement les gendarmes d'active pour des développements logiciels ou des conseils techniques, par exemple.

Les réservistes citoyens, bénévoles du service public, généralement très expérimentés dans leur milieu professionnel, apportent un recul et un regard extérieur qui aident l'institution à se comparer à d'autres milieux et à progresser en cohérence avec la Société. Les réservistes opérationnels, qui sont formés à intervenir sur le terrain, ont une connaissance du quotidien des gendarmes qui en font d'excellents relais auprès des réservistes citoyens qui méconnaissent cet aspect de l'institution.

La rencontre des deux statuts, *a fortiori* en présence des gendarmes d'active, est d'une richesse phénoménale. Nous l'avons constaté notamment lors du séminaire national des réservistes





© Gendarmerie nationale - EOGN

Les ateliers du séminaire national 2019 des réservistes numériques ont permis des échanges intenses et de dégager des procédures collaboratives mobilisant des acteurs souhaitant mettre en commun leurs expertises au profit de projets innovants et disruptifs.

numériques, organisé à Melun en septembre 2019 avec le soutien de l'EOGN qui fêtait alors ses 100 ans, avec deux jours d'ateliers de recherche et de découverte de la gendarmerie d'hier, d'aujourd'hui et de projection dans la gendarmerie de demain. « Disruptif », « innovant », « engagement », « esprit de corps » ont été les mots les plus évocateurs de ces journées.

#### Pouvez-vous nous donner quelques exemples de cette contribution ?

@GendEtVous est une excellente illustration de la richesse de cette collaboration. C'est un service reposant sur une *applet* qui vous permet aujourd'hui, lorsque vous vous connectez à <https://lannuaire.service-public.fr> de prendre rendez-vous avec

la brigade la plus proche, en précisant le motif de votre rendez-vous, afin de faciliter votre accueil.

La création de ce service a été pilotée par la MNGN. Les réservistes numériques sont intervenus dès l'élaboration des spécifications générales. Une analyse des scénarios stratégiques, suivant la méthode EBIOS Risk Manager, a été menée par une équipe de réservistes citoyens de plusieurs régions, en une réunion « agile » en visioconférence avec les chefs de projet fonctionnels. Un réserviste opérationnel a participé au développement de l'*applet*. L'analyse des risques et le dossier d'homologation ont été complétés à distance par un réserviste opérationnel de la région



(3) [https://www.ssi.gouv.fr/uploads/2014/12/PASSI\\_referentiel-exigences\\_v2.1.pdf](https://www.ssi.gouv.fr/uploads/2014/12/PASSI_referentiel-exigences_v2.1.pdf)

Pays de Loire. Un audit de code a été mené par une équipe de réservistes opérationnels, familiers du référentiel d'audit PASSI

de l'ANSSI<sup>3</sup>, qui expérimentaient ainsi l'idée, née d'une « rencontre grenadine », de constituer un référentiel et une équipe

d'audit interne pour les homologations de sécurité des projets à petit budget. Des réservistes citoyens, juristes de profession, nous ont proposé leurs conseils pour la révision de quelques aspects juridiques. On a pu ainsi prononcer l'homologation de sécurité du système pour un coût modique et avec beaucoup d'agilité.



#### Adresse

34 Rue de Rennes  
35150 Janzé

#### Horaires d'ouverture

le Lundi : de 08h00 à 12h00, de 14h00 à 18h00  
le Mardi : de 08h00 à 12h00, de 14h00 à 18h00  
le Mercredi : de 08h00 à 12h00, de 14h00 à 18h00  
le Jeudi : de 08h00 à 12h00, de 14h00 à 18h00  
le Vendredi : de 08h00 à 12h00, de 14h00 à 18h00  
le Samedi : de 08h00 à 12h00, de 14h00 à 18h00  
le Dimanche : de 09h00 à 12h00, de 15h00 à 18h00  
les jours fériés : de 09h00 à 12h00, de 15h00 à 18h00



### BESOIN D'UN RENDEZ-VOUS ?

Veuillez décrire votre situation afin de répondre au mieux à votre demande.

FERMER



Pour signaler des faits en cours ou commis il y a moins de 24h



Pour signaler des faits passés de plus de 24h



Pour toute autre demande

Une application qui s'inscrit dans le souci de « répondre présent » à toutes les attentes du public par des moyens numériques entrés dans les usages quotidiens.

Ceci m'a convaincue que nous pouvions tenter de monter un collège de réservistes venant en appui des innovateurs de la gendarmerie, pour les aider à faire émerger leur projet en prenant en compte les contraintes techniques et réglementaires dont le respect est indispensable à une généralisation du produit et à son maintien en conditions opérationnelles et de sécurité. Ce processus complète les ateliers de la performance que pilote le service de la transformation, pour la valorisation de l'innovation participative. En liaison avec ce service et le service des technologies et des systèmes d'information de la sécurité intérieure notamment, j'ai pu monter un groupe de travail piloté par le CNE (R) David Toulotte, expert en chefferie de projet numérique.

En collaboration avec le service du traitement de l'information de la gendarmerie et la région de gendarmerie Ile-de-France, nous explorons également les missions qui peuvent être confiées aux réservistes en matière de gestion de crises numériques. Leur capacité de mobilisation a été illustrée au début du confinement en mars 2020, par le groupe des réservistes cyber d'Ile-de-France, qui a élaboré très vite un support de sensibilisation à destination des entreprises sur les cybermenaces dans ce contexte particulier, que toutes les régions de gendarmerie de France et le CGOM ont pu ensuite utiliser.

**David Toulotte, vous êtes directeur de projets informatiques, notamment de transformation Cloud pour Arcelor Mittal Europe. Vous avez actuellement une mission à la DGGN et une autre à la région de gendarmerie des Hauts-de-France. Qu'est-ce qui vous a motivé pour accepter ces missions ?**

Je travaille en effet avec Florence Esselin et trois réservistes citoyens, à établir un processus et à constituer une équipe de « coachs » afin d'accompagner les promoteurs d'outils numériques innovants. Il s'agit de sécuriser leurs projets quant aux aspects juridiques, économiques, techniques et patrimoniaux qui font peser une contrainte sur leur mise en production et leur déploiement à grande échelle, tout en soutenant leur innovation et en stimulant leur créativité. J'apporte mes compétences en termes de chefferie de projet.

Parallèlement, du fait de mon expérience professionnelle dans ce domaine, je participe aux actions de la réserve cyber en région Hauts-de-France pour la sensibilisation des entreprises TPE/PME à la cybersécurité. Notre but est d'apporter de l'expérience et de la connaissance aux TPE/PME déjà submergées par leur propre activité. Le profil idoine d'un chef d'entreprise TPE/PME est très large. Outre sa fonction, il doit maîtriser les règles comptables, les relations humaines sans oublier le domaine commercial. Il n'est pas évident d'absorber en plus toutes les

évolutions technologiques et leurs contraintes. Les actions de la réserve sont une façon de les soulager et de soutenir l'activité économique de la région. Le 15 octobre 2020, nous avons débuté une tournée régionale dans les CCI Hauts-de-France, une grande première qui fut un succès.

### **Vous animez un groupe de travail avec des réservistes citoyens. Comment se passe la collaboration ?**

Chacun apporte son propre domaine d'expertise, avec un fort engagement, en étant passionné et soucieux de soutenir la Gendarmerie nationale. Par ailleurs, les échanges d'expérience permettent à chacun de s'enrichir et de générer des partenariats ou des promesses de relations professionnelles.

### **Quelle est votre expérience de la réserve opérationnelle ?**

Je suis engagé dans la réserve opérationnelle de la gendarmerie depuis 1999. Depuis peu, la Gendarmerie nationale nous propose des missions en lien avec nos compétences professionnelles dans le domaine du numérique. C'est une véritable nouveauté qui me motive énormément.

Cependant, je suis aussi dans la réserve opérationnelle pour sortir du quotidien par des missions de terrain qui nous apportent autre chose, pour le bien commun. Cela permet de vivre une expérience

personnelle passionnante et enrichissante. C'est une véritable pratique professionnelle complémentaire qui permet d'acquérir de nouvelles compétences comme la gestion du stress, le dépassement de soi, la maîtrise de sa capacité physique mais aussi des expertises techniques et d'autres aptitudes (adaptabilité, encadrement, esprit d'équipe) qui peuvent être utiles au quotidien et dans son emploi. Cela peut aussi s'avérer un véritable atout pour la recherche d'emploi.

Il m'apparaît évident d'être aux côtés de mes camarades d'active et de réserve et je continuerai de les accompagner sur le terrain.

Mon profil me permet de travailler à divers échelons de l'organisation de la Gendarmerie nationale. C'est ainsi que j'ai pu travailler avec la Région de Gendarmerie nationale des Hauts-de-France et développer un outil de diagnostic des vulnérabilités des entreprises couvrant la cybersécurité et la sûreté. Après quelques années, cela a débouché sur un partenariat entre la région Hauts-de-France et la Région de Gendarmerie. Ce partenariat a été signé au FIC 2020, par le président du conseil régional, Xavier Bertrand, et le GCA Guy Cazenave-Lacrouiz, commandant de la région de gendarmerie des Hauts-de-France, en présence du Directeur général de la Gendarmerie nationale, le GAR Christian Rodriguez.

**Alain Grandjean, vous êtes officier à la division des opérations de la région de gendarmerie des Hauts-de-France, quel emploi faites-vous de la réserve numérique ?**

Dans le cadre du partenariat signé entre la région Hauts-de-France et la région de gendarmerie, la réserve numérique de la Gendarmerie nationale intervient depuis le 15 octobre 2020 sur le « pass cyber formation » organisé dans le cadre du plan cyber initié par le Président de la région Hauts-de-France. Il consiste en des journées de sensibilisation au profit des chefs d'entreprises et cadres des PME des Hauts de France. Ces journées sont financées par le Conseil régional (à hauteur de 50 %) et supportées par l'organisme de formation de la « CCI Hauts-de-France ». La « réserve numérique gendarmerie » a entièrement élaboré le programme de formation et le contenu des cours dispensés durant ces journées et travaille directement avec le chargé de formation de la CCI.

La « réserve numérique gendarmerie » de la région des Hauts-de-France est composée d'experts du domaine : cadres d'entreprises ou professeurs d'université. Lors de cette formation, ils abordent des thèmes très concrets : les différents types de cyber-malveillance, l'identité numérique, les mots de passe, le RGPD, les cyber-attaques les plus courantes (rançongiciels, phishing et Faux Ordres de Virement International). Ils expliquent également quels sont les

acteurs institutionnels et comment les saisir, que faire quand on est victime ou témoin et comment trouver les kits de sensibilisation sur [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr).

Enfin, la formation s'achève par l'enseignement des « bonnes pratiques » en matière de cybersécurité, car la meilleure des protections contre la cyber-malveillance demeure la mise en place d'une organisation au quotidien faisant appel au bon sens. Tout ce travail de sensibilisation en matière de cybersécurité pourra être partagé dans un deuxième temps avec les autres régions qui souhaitent mettre en place des démarches similaires.

**Florence Esselin, comment voyez-vous l'évolution de la réserve numérique ?**

La réserve numérique est un vivier expérimental. On ne s'interdit a priori aucune innovation. On imagine des transformations et on les teste à moindre coût, et si elles s'avèrent pertinentes, le fruit de nos recherches peut être intégré dans les processus existants.

En cela, c'est un levier du plan stratégique « Gend20.24 » pour faciliter la transformation numérique de la Gendarmerie nationale, accroître sa résilience aux cyber-attaques et la sécurité des « nouvelles frontières ». Il reste encore à renforcer son organisation et à formaliser sa feuille de route pour les années à venir, dans le cadre de son appui aux services centraux comme

aux unités sur le terrain. Signe positif, quelques groupements, régions de gendarmerie et services commencent déjà à s'approprier cet outil, afin de « Répondre présent, pour la population, par le gendarme ».

**Florence Esselin est conseiller expert en numérique et sécurité du numérique au cabinet du directeur général de la Gendarmerie nationale. Ingénieur en électronique, informatique, télécoms et réseaux, elle a plus de vingt ans d'expérience en transformation numérique et sécurité du numérique, en entreprise et en administration centrale (services du Premier ministre, ministère de la Culture et ministère de l'Intérieur) dont plus de dix ans au Secrétariat général de la Défense et de la sécurité nationale.**

**Issu de l'École de Militaire de l'Air de Salon-de-Provence (EMA 1992), le lieutenant-colonel Alain Granjean a intégré la gendarmerie en 1998. Expert en intelligence économique et protection des entreprises, diplômé de l'INHESJ, il est actuellement affecté à la division des opérations de la région de gendarmerie des Hauts-de-France. Il est à l'origine du partenariat cyber mis en place entre la Région de gendarmerie et le Conseil régional des Hauts-de-France.**

**David Toulotte est directeur de projets informatiques chez ArcelorMittal et capitaine de la réserve opérationnelle de la Gendarmerie nationale ; ancien auditeur de l'IHEDN et titulaire du MBAsp, Management de la sécurité de l'EOGN, il a été Référent sûreté multisites industriels, Data Protection Officer pour ArcelorMittal France, Coordinateur RGPD pour ArcelorMittal Europe. Référent en intelligence économique pour la réserve, il intervient également sur ce thème en université.**

# DOSSIER

## Hygiène des organisations et des systèmes



**Sécurité des données  
et transformation  
numérique**

**P.71**

par Ludovic Petit



**La CSPN, une certification  
en cybersécurité  
que l'Europe nous envie**

**P.131**

par Gérard Peliks



**SOC et IOC  
au travers  
de la Threat  
Intelligence**

**P.85**

par Robert  
Breedstraet  
et Matthieu Thuaire



**Blockchain, au service  
de la sécurité**

**P.137**

par Jacques Favier



**Des « faits alternatifs »  
à la « Deepfake reality »,  
vers la fin inéluctable de la vérité  
dans le cyberspace ?**

**P.95**

par Franck Decloquement



**« De la genèse de la loi  
informatique et libertés à l'éloge  
de la transdisciplinarité »**

**P.143**

par Alice Louis



**Cybersécurité et protection  
des données : Pourquoi les  
entreprises sont-elles plus  
exposées après la crise ?**

**P.105**

par Marie de Friminvill



**L'ingénierie sociale et du rôle  
de l'utilisateur en tant  
qu'acteur de la sécurité**

**P.149**

par Denise Gross



**Quelle cybersécurité face aux  
innovations numériques ?**

**P.111**

par Myriam Quemener



**La part humaine déterminante  
face aux crises majeures  
et son rôle  
dans la cybersécurité**

**P.155**

par Daniel Guinier



**Les IOT L'internet  
des objets**

**P.115**

par François Bouchaud



**Ce que  
l'expérience  
des Facteurs  
Humains  
Organisation-  
nels dans les  
domaines de**

**l'industrie et de l'aéronautique  
peut apporter à la notion  
de culture de cybersécurité**

**P.163**

par Marc-Xavier Joubert,  
Robert Breedstraet  
et Stéphane Deharvengt



**Cybermenaces :  
la transition numérique  
de la police**

**P.123**

par Thomas Souvignet



# Sécurité des données

## et transformation numérique

Par Ludovic Petit

# R

« Rien ne se perd, rien ne se crée, tout se transforme. »

À l'instar de cette citation prêtée à Antoine Lavoisier lors de l'élaboration de son « Traité élémentaire de chimie », l'omniprésence du monde numérique dans notre quotidien nous impose de reconsidérer notre perception relative à certains concepts, notamment liés à la cybersécurité. Ce changement de paradigme induit désormais une perspective collaborative et coopérative. La cybersécurité apparaît donc dès lors



**LUDOVIC PETIT**

Président de JADE  
Conseil en stratégie  
et cybersécurité

comme un véritable fil d'Ariane pour contribuer au succès de toute transformation numérique. Peut-on parler de maturité quand on parle de transformation numérique ? C'est tout l'objet de cet essai,

à travers quelques exemples concrets dans le cadre du Forum FIC dont le thème est « For a collective and collaborative cybersecurity ».

La transformation digitale est une histoire de stratégie, pas de technologie. Examinons tout d'abord un postulat relatif à la **sécurité collaborative** : « Tous connectés, tous solidaires, tous responsables ». L'hyper-connectivité, liée notamment au déploiement de la 5G, va renforcer l'interdépendance des acteurs et donc l'exigence de coopération pour éviter un risque systémique.

La **sécurité collaborative** peut être le fruit de la convergence de plusieurs approches :  
- D'un point de vue organisationnel, elle se traduit par la capacité de différents acteurs (individus, communautés d'individus, entreprises, États) à coopérer pour renforcer leur sécurité individuelle. Le concept sous-entend une dimension agile, voire une forme d'auto-organisation non centralisée,

- Sur le plan humain, elle rejoint le concept de « *crowd security* ».

- S'agissant des aspects techniques, enfin, la sécurité collaborative s'entend comme la possibilité pour plusieurs systèmes d'échanger de l'information et d'apprendre les uns des autres pour améliorer leurs propres capacités. Cette dimension collaborative est un défi mais aussi une véritable opportunité à l'heure de la multiplication des équipements connectés.

### Aux origines du mot « cyber »

Quel est donc le sens de ce préfixe *cyber*, que l'on entend partout de nos jours ? Les origines du mot aident à le comprendre. Il est né après la Deuxième Guerre mondiale dans la tête d'un chercheur américain nommé Norbert Wiener, théoricien et chercheur en mathématiques appliquées, surtout connu comme le père fondateur de la *cybernétique*.

Ce mathématicien fut engagé au Massachusetts Institute of Technology (MIT) dans un programme de recherche consacré à de nouvelles formes d'armements. On lui demanda de mettre au point des missiles capables d'atteindre les avions allemands V1 et les fusées V2, sans pilote, bourrés d'explosifs qui causaient tant de dégâts en Angleterre pendant la Deuxième Guerre mondiale. Pour ce faire, Wiener devait modéliser le comportement d'un pilote en situation de combat,

se sachant pourchassé, et donc mieux comprendre les mécanismes de décision de l'homme en général.

En 1948, Norbert Wiener baptisa *cybernétique* un nouveau domaine de la science où est étudié le concept de maîtrise des machines. L'idée du nom lui vint du grec ancien *kubernao* qui signifie '**piloter**'. *Cyber* a donc la même étymologie que gouvernail et que ... *gouvernement*.

En fondant la cybernétique, Wiener introduit en science la notion de *feedback* (rétroaction, dans son sens littéral de 'nourrir en retour'), qui a nombre d'implications dans des domaines tels que l'ingénierie, le contrôle de système, l'informatique, la biologie, la psychologie, la philosophie et l'organisation de la société. Il exposa ses théories sur la cybernétique dans son livre :

« **Cybernetics or Control and Communication in the Animal and the Machine** », dont le *New York Times* fit l'éloge en janvier 1949, en tant qu'un des livres les plus importants du XX<sup>e</sup> siècle, en lui prédisant un rôle de science phare dans le futur - et l'actualité lui donne raison. Un des concepts majeurs qui fondent cette nouvelle théorie est celui de « *régulation* », nous y reviendrons.

La cybernétique, omniprésente de nos jours, est en synthèse la science qui étudie comment un système peut poursuivre et atteindre un objectif malgré les perturbations imprévisibles de son environnement.



*Cyber* est devenu un préfixe à la mode à partir de la deuxième moitié du XX<sup>e</sup> siècle. Son usage est consécutif au développement exponentiel de l'informatique et de la robotique, plus généralement à l'avènement du réseau Internet et de la « révolution numérique » que nous connaissons depuis.

Force est de constater que la notion de sécurité a aussi subi une transformation assez radicale. À celle, classique, de défense fortifiée du système d'information, s'est ainsi depuis quelques années, substituée une autre approche, plus complexe, désignée sous le terme de « **cybersécurité** ».

Une des raisons premières est que l'évolution numérique technologique et fonctionnelle induit la disparition des périmètres logiques traditionnels (*on parle souvent de disparition des frontières*). L'entreprise orientée « client » doit donc adapter et développer l'interactivité, la fluidité et l'interconnectivité de ses échanges internes et externes via un système d'information nécessairement plus ouvert et connecté... donc plus vulnérable.

Ceci nous amène à un bref rappel de la signification de ce que l'on appelle « **cybersécurité** », véritable fil d'Ariane qui s'inscrit en filigrane de toute transformation numérique, pour une meilleure compréhension des quelques cas concrets mentionnés plus avant dans l'article.

La *cybersécurité* ou sécurité des technologies de l'information, s'apparente aux techniques de protection des ordinateurs, des systèmes d'information, des appareils mobiles, des réseaux, des applications et des données contre les accès non autorisés et les attaques malveillantes.

Le terme s'applique à des contextes divers et se décline en quelques catégories bien connues :

- **La sécurité de l'information** protège les informations et les systèmes d'information contre tout accès, utilisation, divulgation, perturbation, modification ou destruction non autorisés afin d'assurer la confidentialité, l'intégrité, la disponibilité et la non-répudiation des données, qu'elles soient stockées / hébergées ou en transit ;
- **La sécurité des réseaux** qui consiste à protéger un réseau informatique contre les intrus ;
- **La sécurité des applications** se concentre sur la protection des logiciels contre les menaces ;
- **La continuité d'activité et la reprise d'activité après un sinistre** qui définissent la manière dont une entreprise réagit à une cyber-attaque ou à tout autre événement qui entraînerait une interruption de service, un problème opérationnel ou une perte de données ;

- **La sensibilisation des utilisateurs**, relative au facteur le plus imprévisible : l'humain. Aider les utilisateurs à mieux comprendre et leur apprendre comment réagir est essentiel pour protéger l'activité d'une entreprise.

### Qu'est-ce que la sécurité des réseaux ?

Si vous considérez une entreprise comme un château fortifié contre les menaces extérieures, la sécurité des réseaux se préoccupe du maintien de la paix et du calme dans l'enceinte du château. Elle se concentre sur le maintien des fortifications, bien entendu, mais son objectif premier est de **se prémunir contre les problèmes de l'intérieur**, en se concentrant sur la protection des informations internes à l'entreprise, en surveillant le comportement des employés et du réseau de plusieurs façons. La cybersécurité est beaucoup plus **centrée sur les menaces venant de l'extérieur** du château.

Quand la sécurité du réseau s'inquiète de ce qui se passe à l'intérieur des murs du château, la cybersécurité consiste à surveiller ceux qui tentent de passer la porte ou de franchir les parapets et à analyser les techniques d'attaques. Il y a certes une forte intrication entre ces deux domaines mais leurs préoccupations sont très différentes. La cybersécurité vise à défendre le royaume et se concentre sur les attaquants à la porte et sur la façon dont le château communique avec le monde qui l'entoure.

Tenant compte du fait que nous vivons désormais dans un monde numérique, on considère de nos jours par extension - et par usage - la cybersécurité comme la sécurité de tout contexte lié à l'utilisation de l'informatique et du numérique, dans le cyberspace, notamment Internet.

### Vient alors LA question :

#### Contre quoi dois-je me protéger ?

#### Quelle est la menace ?

Dans certains contextes, par exemple militaires, on connaît les menaces. On agit donc en conséquence en effectuant des simulations et des exercices, en situation réelle, conformes aux scénarios. En informatique, une menace est une cause potentielle d'incidents pouvant créer un dommage au système ou à l'entreprise (selon la norme de sécurité des systèmes d'information ISO/CEI 27000).

La déstabilisation, l'espionnage, le sabotage et la cybercriminalité constituent les principales menaces pour une entreprise. L'atteinte à l'image, l'impact financier et les conséquences légales sont bien réels. C'est pourquoi il est impératif d'évaluer son niveau d'exposition à la menace cyber. Dans une perspective de sécurité des données et de transformation numérique, la cybersécurité induit naturellement et par essence la notion de travail collaboratif. En effet, la cybersécurité oblige à considérer tant l'élément à sécuriser que son contexte. En d'autres termes, raisonner cybersécurité ne peut se faire



© Metal Wheel Concept par EitAmmos

L'évolutivité des technologies, des mœurs des usagers et les contraintes économiques rendent impératives une vision collaborative pour promouvoir une cybersécurité normée et suscitant la confiance.

qu'en ayant une idée précise de ce qu'il y a à sécuriser (la vision *micro*) dans un contexte global (la vision *macro*). C'est accessoirement le sens de l'*Analyse de Risque*.

Un bon exercice est par exemple d'éteindre l'interrupteur du site de production, afin de tester ses processus de gestion de crise, de résilience de service(s) assurant la continuité d'activité et la reprise d'activité après un sinistre. Le coût d'une telle interruption de service(s) sera vite connu. Avez-vous déjà testé votre processus de gestion de crise en situation réelle ?...

La notion de collaboration (voire d'*hyper-collaboration* dans le cadre d'un contexte sensible) apparaît dès lors

comme essentielle. Nous le verrons dans quelques instants, les contraintes légales et réglementaires obligent les entreprises à sécuriser les données, donc leur système d'information. Par nature, cela nécessite une très forte interaction entre Direction Générale et Responsable de la Sécurité des Systèmes d'Information (RSSI) pour que les mesures opérationnelles mises en place répondent aux besoins métier(s) de l'entreprise.

Cette collaboration doit garantir la légitimité de la cybersécurité en entreprise, tant dans sa verticalité (Comité Exécutif / Direction Générale – RSSI) que dans sa transversalité (RSSI – entités Métiers et Direction des Systèmes d'Information). C'est ce qui conditionne une bonne vision d'ensemble

d'un écosystème. L'exercice est certes loin d'être trivial mais c'est le lot quotidien du RSSI, véritable chef d'orchestre de la sécurité des données de l'entreprise et protecteur du business.

Pour que cette collaboration pluridimensionnelle fonctionne, cela demande de sortir du carcan de la vision purement technique de la SSI. La transformation numérique introduit un **changement de perspective, centré sur la donnée et sur le potentiel de sa valorisation économique**. Ainsi s'explique l'engouement des entreprises pour l'Analytics et le Big Data. Ne dit-on pas de la *donnée* qu'elle est le « *pétrole* » du XXI<sup>e</sup> siècle ?

La valeur d'une information est conditionnée par sa disponibilité, son intégrité et sa finalité métier qui requièrent une confidentialité stricte. Les pratiques de la sécurité doivent donc dépasser la dimension purement technologique du SI pour embrasser la dimension métier(s). Là est le véritable challenge !

La sécurité ne peut donc se résumer à un arsenal technique de protection du système d'information. Elle est désormais intimement liée à tous les aspects de la vie des entreprises et des métiers, dans leurs relations avec les clients, les partenaires et les employés. Pour tirer profit de sa transformation numérique, il faut que l'entreprise dispose d'un système d'information de confiance et que cette confiance

soit partagée avec ses clients et partenaires.

La **cybersécurité** devient dès lors indispensable et constitue un catalyseur de développement économique, ce qui est aujourd'hui perçu comme un facteur différenciant essentiel. La démarche initiée par l'ANSSI concernant la certification de solutions est un exemple de ce qu'un **'facteur différenciant'** peut représenter en termes de solution de confiance. La cybersécurité est de nos jours devenue un véritable *business-enabler*.

De plus, cette synergie entre Exécutif et RSSI est « *bankable* » ; c'est à travers cette stratégie collaborative qu'une entreprise peut (doit !) être perçue comme un partenaire de confiance par ses clients et partenaires, socle indispensable pour contribuer à faire évoluer une notion de service.

La transformation numérique implique aussi une véritable **coopération entre Data Protection Officer (DPO, le Délégué à la Protection des Données personnelles - DPD en français) et RSSI**. Cette collaboration entre le DPO et le RSSI, primordiale de nos jours, est due à un **changement de paradigme**. Historiquement, et ce jusqu'aux prémices d'Internet de la fin des années 80, les émergences technologiques prenaient le pas sur le cadre légal de référence qui n'avait pas évolué en conséquence, ce qui posait

un problème majeur au législateur.

**Le droit évoluait alors en fonction des évolutions technologiques**, à l'image de la **Loi Godfrain du 5 janvier 1988**, ou de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, première loi française réprimant les actes de criminalité informatique et de piratage. Nommée d'après le député RPR *Jacques Godfrain*, c'est l'une des lois pionnières concernant le droit des nouvelles technologies de l'information et de la communication (NTIC), après, notamment, la **Loi Informatique et libertés**, de 1978, qui introduit la notion de système de traitement automatisé de données (STAD) et prévoit plusieurs dispositions corrélatives de la loi Godfrain (notamment concernant les obligations du responsable du traitement quant à la garantie de la sécurité des données - Art. 34, Loi de 1978).

### **Cette tendance s'est depuis inversée.**

La France a été un précurseur en matière d'évolutions légales relatives aux nouvelles technologies, faisant de nombreux émules de par le monde, par exemple avec le « *California Online Privacy Protection Act of 2003* » (CalOPPA), entré en vigueur le 1<sup>er</sup> juillet 2004 et modifié en 2013. C'est la première loi d'État des États-Unis à exiger que les sites commerciaux et les services en ligne sur Internet disposent d'une politique de confidentialité sur leur site web. De nos jours, et ce depuis maintenant une vingtaine d'années,

le cadre légal et réglementaire conditionne les moyens techniques à mettre en œuvre pour être conforme à la loi, à l'image du **règlement général sur la protection des données (RGPD)** entré en vigueur, le 25 mai 2018, pour toute société traitant des données personnelles de citoyens européens, avec une notion d'extra-territorialité.

L'article 37 du RGPD mentionne les cas dans lesquels il est obligatoire de nommer un DPO, ainsi que ses modalités de désignation. Les articles 38 et 39 définissent respectivement sa fonction et ses missions. Le DPO a la charge de recueillir les informations visant à connaître les opérations de traitement et d'apprécier leur conformité au cadre légal. Il doit informer, conseiller et émettre des recommandations au responsable de traitement et au sous-traitant.

Rappelons que, bien que le rôle de DPO fixé par le règlement européen soit très récent, la protection des données personnelles a toujours historiquement été au centre de la démarche du RSSI, sécurité de l'information oblige. Le RGPD vient néanmoins renforcer le fait que le RSSI doit travailler de concert avec la direction juridique et le DPO, afin que la sécurité de l'information soit appliquée à l'échelle de l'entreprise conformément au cadre légal en vigueur et aux besoins métier(s).

Cette synergie est aujourd'hui un plus indéniable pour toute entreprise souhaitant

valoriser la sécurité de son patrimoine informationnel auprès de ses clients. Lorsqu'on parle sécurité des données personnelles, cela implique de facto le principe de proportionnalité cher au RSSI de Disponibilité, Intégrité, Confidentialité et Preuve (DICP). Le travail conjoint du DPO et du RSSI est l'exemple type de ce que l'on doit concevoir comme cybersécurité collective et collaborative. Citons le Considérant 7 de l'introduction du RGPD qui image ce propos : « *Il importe de susciter la confiance qui permettra à l'économie numérique de se développer.* »

Au-delà de l'obligation légale, la coopération entre DPO et RSSI s'avère non seulement être une nécessité mais aussi une affaire de bon sens pour protéger le patrimoine de l'entreprise. Cette coopération majeure et essentielle permet à l'entreprise de pérenniser sa cybersécurité, contribuant ainsi à être perçue comme un partenaire de confiance par ses clients et partenaires.

### Anonymat, pseudonymat, un vrai-faux débat ?

La définition d'une donnée à caractère personnel existe, certes, tout comme celle de l'anonymisation et de la pseudonymisation. En fait, il faudrait que le législateur crée un **label** certifiant que le processus technique d'anonymisation a été bien appliqué conformément aux standards technologiques nécessaires, sur les données caractérisées à caractère personnel dans

le label. Dans cette perspective, le processus appliqué par l'entreprise est audité et certifié conforme au label ou pas. Il n'y a pas de demi-mesure. Dans le cadre du RGPD, le principe de finalité du traitement de données à caractère personnel régit le processus opérationnel à appliquer. Pas de débat, il faut rester pragmatique et matriciel dans une approche qui dépend du contexte. La CNIL est très claire sur ce point.

**L'anonymisation** est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible toute identification de la personne par quelque moyen que ce soit et de manière **irréversible**. L'anonymisation ne doit pas être confondue avec la pseudonymisation.

La **pseudonymisation** est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire. La pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) d'un jeu de données par des données *indirectement* identifiantes (alias, numéro séquentiel, etc.). La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. En pratique, il est toutefois bien souvent possible de retrouver l'identité de ceux-ci grâce à des données tierces : les données concernées conservent donc un caractère

personnel. L'opération de pseudonymisation est également réversible, contrairement à l'anonymisation. La pseudonymisation constitue une des mesures recommandées par le RGPD pour limiter les risques liés au traitement de données personnelles.

À noter qu'il est important que la démarche d'anonymisation / pseudonymisation soit gérée en mode projet, afin de documenter la stratégie et la procédure appliquée (données concernées, méthode technique choisie et appliquée, description du processus de modification, *etc.*), d'être en mesure d'appliquer le même processus dans le temps, suivant les mêmes règles, de pouvoir trouver une éventuelle faiblesse dans le processus, ou de le faire évoluer en cas de besoin.

Quid en revanche de l'anonymat / du pseudonymat lors de la navigation sur Internet ? De façon native, la connexion à Internet par un fournisseur d'accès ne fournit pas d'information sur l'utilisateur, mais en revanche référence une adresse IP correspondante. Techniquement, même si le nom/prénom de la personne qui surfe sur le Net n'est pas divulgué lors de la connexion, l'anonymat n'est pas garanti. On considère donc en ce cas qu'il y a pseudonymat, en ce sens que le fournisseur d'accès à internet peut lui, très simplement corréler cette adresse IP à une personne physique (ne serait-ce que par les références de souscription initiale au service).

Exemple par excellence de transformation numérique, **Internet** est un média électronique dont l'utilisation - quelle qu'elle soit - ne permet PAS l'anonymat. Afin d'étayer mon propos je vais citer ici une personne remarquable, **Edmond Locard**, père de la police scientifique qui, alors que Georges Clemenceau venait de créer ses Brigades régionales de police mobile (dites « Brigades du Tigre », et ancêtre de l'actuelle police judiciaire française), posait en 1910 les fondamentaux de la criminalistique : « *Nul ne peut agir avec l'intensité que suppose l'action criminelle sans laisser des marques multiples de son passage. Par une action inverse, il a emporté sur son corps ou sur ses vêtements les indices de son séjour ou de son geste.* »

En substance et si on transpose le postulat émis par Edmond Locard au contexte de transformation numérique qui régit notre quotidien, les technologies utilisées par le réseau des réseaux pour son fonctionnement intrinsèque conditionnent ceci : *tout individu laisse une trace*. Techniquement, quand bien-même nous utiliserions des technologies de chiffrement et autres VPNs, l'anonymat – au sens strict du terme – est presque impossible sur internet car la technologie permet la plupart du temps de corréler les faits (mon propos ne concerne pas le cas des États-Nations dans le cadre de leur souveraineté nationale disposant de moyens *ad hoc*). J'ajoute que, bien souvent, la complexification des technologies

utilisées à dessein rend - presque - impossible l'identification d'une personne, mais d'un point de vue technique perdure, quoi qu'il en soit, la notion dite de bout-en-bout. En telle circonstance donc, il s'agit d'un vrai-faux débat.

### Vaste débat que celui de l'Internet des objets (IoT, pour Internet of Things)

Le sujet de l'Internet des objets a brièvement été évoqué, qu'en est-il des **objets connectés et quid de la cybersécurité collaborative** ?

#### Des solutions mal sécurisées

Force est de constater que les solutions IoT développées de nos jours ont, pour la plupart, échoué d'un point de vue sécurité. Les raisons sont variées mais trois axes majeurs s'en dégagent : manque de support matériel pour la sécurité, des solutions disparates nécessitant des mises à jour systématiques et un manque de compréhension de l'environnement de la menace.

Beaucoup d'entreprises, qui n'étaient pas connectées auparavant, ont cherché à numériser leurs produits et services sans réellement disposer de la connaissance préalable de la cybersécurité. Elles ont sous-traité le problème à des sociétés qui ne comprennent pas non plus les risques cyber ou qui n'ont qu'une vision partielle du système dans son ensemble. Les hackers profitent bien évidemment de cette situation pour perpétrer des attaques DDoS (Deni de Service Distribué), causer

des pertes de revenus, des vols de données et d'autres atteintes à la vie privée.

On peut dès lors légitimement se poser la question : pourquoi ces sociétés développent-elles des objets connectés non sécurisés ? Comme bien souvent, des décisions fondées sur les coûts ont conduit les développeurs et les entreprises à choisir des plateformes IoT peu sécurisées. Les entreprises évitent souvent de fournir des mises à jour logicielles sécurisées en raison du coût de déploiement et de gestion du cycle de vie des produits qui y est associé. Les ingénieurs de ces plates-formes ont souvent abordé le problème à partir de leur propre base de connaissances, qui ne comprend généralement pas une bonne compréhension des considérations de sécurité. De fait, même inconsciemment, des décisions ont été prises qui portent atteinte à la sécurité du système à long terme. C'est le challenge à relever concernant le sujet des objets connectés. À noter qu'un produit perçu comme peu sûr peut non seulement entraîner son rejet par les consommateurs (avec une potentialité d'impact économique certain) mais aussi d'éventuelles enquêtes judiciaires, ne l'oublions pas.

#### Une conception des réseaux datée

Le *pragmatisme* est de rigueur avec un tel sujet. D'un point de vue personnel, je ne pense pas que l'on puisse disposer, à date, d'une tendance crédible du nombre



d'objets qui seront connectés dans les années à venir, ceci pour une raison simple qui bien souvent est passé sous silence : les réseaux de communication actuels ne sont pas, à date, conçus pour supporter une charge de trafic aussi conséquente relative à xxx milliards d'objets à interconnecter en temps réel (Fin de la statistique probabiliste précitée). Ce n'est pas un postulat intangible de ma part, encore moins une critique, mais un fait. Les réseaux de télécommunications, tels que nous les connaissons aujourd'hui, ont initialement été conçus pour nous permettre de communiquer plus facilement, évolutions technologiques aidant, et ont évolué à travers le temps (tout relatif) pour passer du stade de réseaux voix à celui de voix-data par l'adoption massive de la technologie en mode paquet, notamment IP. En fait, on a voulu avec les télécoms (fixe et mobile) migrer de technologies initialement dédiées à transporter de la voix, à faire de la voix sur IP, alors que le protocole IP n'est pas du tout conçu pour embarquer des échantillonnages voix en paquets qui doivent eux-mêmes être resynchronisés sans fin dans les réseaux hétérogènes... Qualité de Service quand tu nous tiens (QoS). En clair, on a voulu faire moins bien avec IP que ce qui marchait à peu près bien avec les réseaux voix. Peu importe, l'évolution technologique va de pair avec l'évolution humaine, c'est dans la logique des choses.

Le fonctionnement du réseau Internet repose sur les protocoles TCP (Transmission Control Protocol) et IP

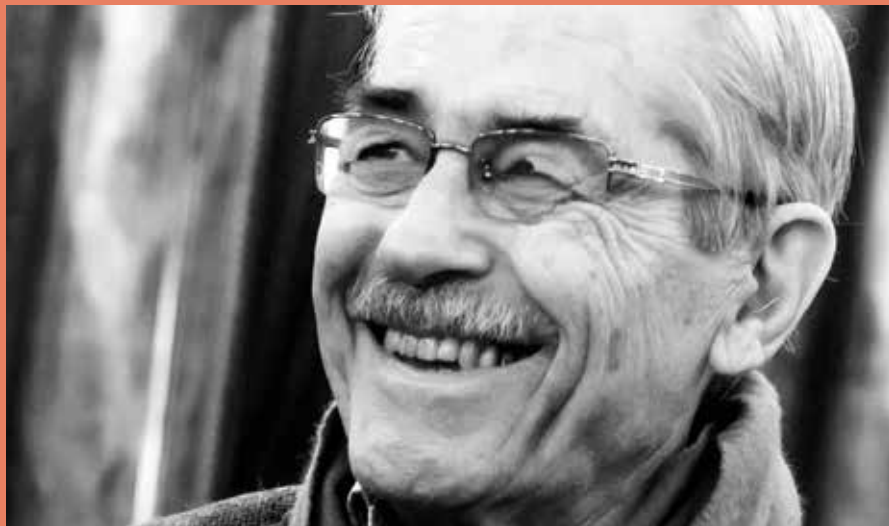
(Internet Protocol) qui n'ont pas changé depuis leur développement dans les années 1970 et leur utilisation à partir des années 1980, notamment par le réseau Arpanet qui préfigurerait le réseau internet.

Or, de quelques centaines d'utilisateurs au départ, le réseau des réseaux accueille quarante ans plus tard plus de 4,5 milliards d'utilisateurs à travers une kyrielle de services inimaginables à l'époque : développement du haut débit, téléphonie sur IP, télévision sur IP, explosion des usages internet en situation de mobilité, **essor de l'Internet des objets**, etc.

Les protocoles TCP et IP n'ont pas été pensés, dans les années 1980, pour supporter une telle diversité d'applications : « *IP n'a pas été optimisé pour prendre en charge les flux de données tels que la voix, la diffusion audio et la vidéo. Il a été conçu pour ne pas être le réseau téléphonique* », expliquait en 2011 John Day, co-concepteur d'Arpanet.

La technologie 4G a apporté un plus dans le cadre de cette transformation numérique, et la 5G - pour faire simple - va semble-t-il apporter la pervasivité, l'omniprésence, le tout connecté « de partout », n'importe quand et quelle que soit la technologie. En conséquence et avec une telle perspective technologique, la **cybersécurité** ne peut qu'être **collaborative**.

Brève incise à propos de l'un des nombreux projets visant à inventer l'Internet du futur, appelé RINA (Recursive InterNetwork Architecture), auquel participe le chercheur français Louis Pouzin (que je salue ici avec respect et reconnaissance), l'un des pionniers de l'Internet.



RINA propose une nouvelle architecture de réseau capable de résoudre les lacunes de l'internet actuel. La France a tout à gagner à supporter et valoriser un tel projet !

© CC BY-SA 3.0 Photo Jérémie Bernard

La technologie 4G a apporté un plus dans le cadre de cette transformation numérique, et la 5G - pour faire simple – va semble-t-il apporter la pervasivité, l'omniprésence, le tout connecté « de partout », n'importe quand et quelle que soit la technologie. En conséquence et avec une telle perspective technologique, la **cybersécurité** ne peut qu'être **collaborative**.

Comment en effet espérer, en de telles circonstances, pouvoir gérer une quelconque cybersécurité contextuelle s'il n'y a pas

d'harmonisation des normes, de partage d'informations, voire de transfert de compétences, de consensus et d'actions coordonnées entre les acteurs, tant publics que privés ?

Si le champ des possibles est considérable avec la 5G, c'est loin de n'être qu'un sujet technique. On est là au cœur de la notion de collaboration nécessaire entre acteurs, car la complexification technologique est telle que les business-models restent à créer, tout comme celui de la Cybersécurité qui devra nécessairement évoluer

pour s'adapter en conséquence.

### Véhicule autonome et sécurité collaborative

Comment, avant de terminer cet essai, ne pas parler des **véhicules connectés**, tant il y a de préoccupations inhérentes à la **cybersécurité** et à la **sûreté**.

Un exemple pour s'en convaincre ? Sautons ensemble dans l'arène. Une vidéo publiée par *Wired* en 2015 montre un des journalistes du magazine spécialisé, Andy Greenberg, rouler à plus de 100 Km/h sur une autoroute du Missouri, dans une Jeep Cherokee récente.

Sans qu'il n'actionne aucun bouton, la climatisation s'active au maximum. Il poursuit sa conduite, tandis que sa radio se met en route avec le son lui aussi au maximum. Une minute plus tard, son réservoir de liquide lave-vitres se vide et ses essuie-glaces battent la mesure. Il ne voit plus grand-chose. Les portes se verrouillent et se déverrouillent automatiquement. Mais un problème plus important survient. La transmission de son véhicule est coupée, la Jeep ralentit. Pendant une longue minute, durant laquelle il craint de se faire emboutir par un camion semi-remorque, Andy Greenberg ne peut rien faire. Grosse panique à bord ! En fait, deux chercheurs en sécurité informatique, Charlie Miller et Chris Valasek, ont piraté à distance la Jeep Cherokee d'Andy Greenberg. Ils ont exploité une faille

qui touche le système reliant la voiture à Internet, en l'occurrence, *Uconnect*. *(Le lien pour visualiser la vidéo est disponible dans les sources et références, en fin d'article).*

Il y a quelques décennies, une voiture n'était qu'une mécanique de métal dans une carcasse de tôle. Aujourd'hui, c'est aussi un ordinateur...Puissant... Et connecté. La part des voitures connectées sur le nombre total de voitures neuves vendues dans le monde en 2015 était de 35%, avec une prévision de 90% pour 2020 et de 100% en 2025. (Voir Ref.) Ainsi, en 2025, toutes les voitures neuves vendues chez les concessionnaires devraient être connectées à Internet et équipées de services d'information et de communication : *Connecto*, *ergo sum*.

Une projection du nombre de voitures connectées en circulation en France était de 3,1 millions en 2017, 8,6 millions cette année en 2020, 10,7 millions en 2021, avec une prévision de 12,8 millions en 2022. D'une évaluation effectuée en 2015 par des entreprises européennes du secteur automobile relative aux défis du marché des voitures connectées, il ressort que près de 40 % des entreprises ont considéré l'absence de normes entre les fabricants et les fournisseurs comme un défi majeur à cette période. Ce « simple » fait concourt à complexifier la mise en place d'une cybersécurité efficace

et adaptée au secteur des véhicules connectés. Le défi est réel, car on constate que la cybersécurité peut sauver des vies ! Il ne viendrait à l'esprit de personne d'acheter un véhicule sans freins ou en option, ce serait un non-sens. C'est pareil avec le cyber pour les véhicules connectés, **la sécurité n'est PAS une option !** Il est une évidence que cela méritera considération dans la perspective des **véhicules autonomes** qui nécessitent une cybersécurité collaborative.

Je sais les engagements, les talents qui œuvrent au quotidien, tout comme j'ignore certainement bien des développements en cours. Je les salue ici avec respect car le sujet est loin d'être simple. Comme nous avons pu le voir, nous vivons dans un *Work in progress*, un monde en perpétuelle mutation dont la transformation numérique n'en est qu'à ses prémices. L'Intelligence Artificielle, le Machine Learning ? Je ne les oublie pas : nous en discuterons au FIC 2021. À vous y rencontrer avec plaisir !

#### Sources et Références

- Aux origines du mot « cyber », Luc de Brabrandere
- Cybernetics, or Control and Communication in the Animal and the Machine (1948) publié en anglais par la Librairie Hermann & Cie (Paris), The MIT Press (Cambridge, Mass.) et Wiley (New York) ; traduit sous le titre La cybernétique. Information et régulation dans le vivant et la machine, par R. Le Roux, R. Vallée et N. Vallée-Lévi, éd. Seuil, Coll. Sources du Savoir, 2014.
- Notions de « données personnelles », « d'anonymisation », de « finalité » et de « traitement », CNIL
- Edmond Locard, le père de la police scientifique
- Règlement général sur la protection des données (RGPD)  
<https://www.cnil.fr/fr/reglement-europeen-protection-donnees>
- Louis Pouzin, RINA (Recursive InterNetwork Architecture)  
<https://la-rem.eu/2019/09/rina-un-projet-pour-linter-net-de-nouvelle-generation/>  
<http://pouzinsociety.org/>
- Hackers Remotely Kill a Jeep on a Highway - With me in it  
<https://www.youtube.com/watch?v=MK0SrxBC1xs>  
<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- Securing IoT Solutions By Design - A Guide to Securing IoT Devices and Services at Scale  
<https://www.copperhorse.co.uk/copper-horse-and-arm-launch-white-paper-on-iot-security-by-design/>
- Les voitures connectées - Faits et chiffres, juin 2020  
<https://fr.statista.com/themes/3695/les-voitures-connectees/>

#### L'AUTEUR

**Président de JADE, cabinet de conseil en stratégie et cybersécurité, Ludovic Petit a été Directeur Cybersécurité du Groupe Altran. Expert en cybersécurité et protection des données, il est également chercheur associé au Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale, Commandant de Réserve Citoyenne Cyberdéfense et membre du Conseil d'Administration de Cyberlex, l'Association du droit et des nouvelles technologies.**

# La Threat Intelligence

Par Robert Breedstraet et Mathieu Thuaire

# L

La crise sanitaire mondiale que nous traversons actuellement rappelle que le coronavirus COVID-19 tout comme les virus informatiques n'est pas soumis à la notion de frontières. Par ailleurs, il nous rappelle la nécessité de travailler ensemble pour obtenir au plus vite le traitement et surtout signaler les clusters afin de préserver la population. En matière de cybersécurité cela revient à disposer de la capacité de détecter le signaux des attaques, même faibles, de bâtir une stratégie sur des bases techniques et organisationnelles et de partager, en sûreté, les informations récoltées par les systèmes dans un mode collaboratif.



**ROBERT BREEDSTRAET**

Division information security officer.  
Adjoint au Corporate CISO d'Amadeus IT Group.



**MATHIEU THUAIRE**

RSSI  
Secrétariat Général de la Défense et de la Sécurité Nationale

(1) SOC : « Security Operation Center », le SOC est un département de sécurité qui est en charge de superviser et protéger les systèmes d'information des entreprises contre les cyber attaques.

(2) APT : « Advance Persistent Threat » menace avancée persistante, c'est-à-dire une attaque cyber précise, ciblée, souvent complexe et furtive. L'acronyme APT est aussi utilisé pour décrire les groupes responsables de ces attaques (exemple : APT 1, présumé chinois et supposé troisième département de l'état major de l'Armée Populaire de Libération, connu sous le code Unité 61398).

Fort de cette actualité « pandémie », dans le cadre de la cybersécurité et de ses moyens déployés par les entités qu'elles soient privées ou publiques, un des outils qui intègre la boîte à outil du RSSI est constitué du SOC (Security Operating Center)<sup>1</sup>. La détection des empreintes ou des signaux faibles - constituant notamment les APT<sup>2</sup> (Advanced Persistent Threat) – est assurée par les mécanismes de corrélation des logs concentrés par le SOC, et restituée au travers du SIEM<sup>3</sup> (Security Information and Event Management) aux analystes. Bien évidemment, malgré

l'automatisation possible, ainsi que le machine learning implémenté dans cet outil, tout signal qui se glisserait dans un compor-

tement normal défini par les métiers de l'entité considérée risquerait de passer inaperçu. Cela souligne ainsi la nécessité et la difficulté de corréler l'ensemble des signaux

(3) SIEM : « Security Information and Event Management » les SIEM sont des outils de gestion de l'information de sécurité qui aident les organisations et les entreprises à gérer tous leurs événements de sécurité (les logs ou journaux systèmes) afin d'en extraire les alertes et, potentiellement, de remonter à la source de l'attaque.

(4) IOC : « Indicator of Compromise » on pourrait traduire par indicateur de compromission, les IOCs classiques sont les signatures de virus, les signatures de trafic réseau, les « hashes » (MD5) de malwares, les URL et les noms de domaine des serveurs de commande et de contrôle...

de manière globale afin d'identifier une attaque potentielle. La notion d'indicateur, que nous retrouvons plus régulièrement sous le terme d'IOC : Indicator Of Compromise, est ici primordiale<sup>4</sup>.

Nous pressentons ici la limite de l'exercice si chaque entité travaille de manière isolée. En effet, afin de couvrir le spectre le plus large possible, il est nécessaire de détenir les IOC les plus pertinents couvrant les risques des SI considérés de l'entité, ce qui nécessite donc de

maîtriser son infrastructure et sa configuration, et surtout de les *partager* au plus vite pour limiter l'impact des attaques.

### L'état de la menace

Ce qui se cache derrière les menaces aujourd'hui peut prendre plusieurs formes : les attaquants peuvent avoir des visées purement économiques, des groupes criminels parfois multinationaux vont extorquer votre argent, voler vos cartes

de crédit et vider vos comptes en banque. Le but des attaquants peut aussi être de capturer de nombreuses informations sensibles tels des secrets de fabrication ou même des données personnelles et de voyage. D'autres attaques ont comme finalité de réduire les moyens de communication ou même de complètement détruire les moyens informatiques de grands groupes industriels ou d'États ennemis. Les tactiques, les techniques et les procédures utilisées diffèrent car une attaque persistante pour le vol des

(5) EBIOS RM : « Risk manager » méthode française d'identification et de compréhension des risques numériques au sein d'une entreprise.

(6) Script kiddie ou lamer désigne des néophytes, ne disposant pas de compétences sérieuses en sécurité informatique, qui tentent de forcer des systèmes au moyens de scripts dont ils ne maîtrisent qu'imparfaitement les ressorts.

données se construit différemment d'une attaque purement destructrice. Ces éléments sont notamment identifiés dans la méthode EBIOS RM<sup>5</sup>, éditée et préconisée par l'ANSSI, dans le cadre des analyses de risques servant de base à l'homologation des systèmes d'informations.

Toutefois, la stratégie est commune pour certaines phases de ces différentes attaques (dans le scénario décrit ci-dessous les trois premières phases se retrouvent dans les attaques citées plus haut). Bien évidemment nous parlons ici d'attaques élaborées et non pas de simples scan de ports ou d'attaques de script kiddies<sup>6</sup>.

- Une première phase dite de **reconnais-**

**sance**, où se mêle de l'ingénierie sociale pour apprendre à connaître ses victimes,

(7) Identifiants de connexion à un espace à accès restreint.

du phishing avec des pièces jointes ciblées et piégées, ou le vol de credentials<sup>7</sup>.

- Une seconde phase dite d'**exécution**, où l'attaquant s'installe dans le système en utilisant des chevaux de Troie (appelés aussi Trojan) à accès distant.

- Une troisième phase de **persistance** qui caractérise le fait de rester caché au fond des systèmes informatiques de la victime. Cette phase est réalisée quand l'attaquant a pris le contrôle de comptes dit à privilège, comme des comptes « administrateurs ».

- Une quatrième phase dite de **collection** où les informations sensibles de la victime sont capturées : données sensibles, identifiants et mots de passe, courriels.

- Une étape finale d'**extraction**, où les données sont compressées, chiffrées et envoyées sur le réseau à un ou des serveurs externes.

Sans préjuger d'un ordre de criticité de ces différentes phases, intéressons-nous à la troisième phase qui est l'objet de beaucoup d'attention de la part d'attaquants que nous qualifierons d'experts. En effet, la capacité à se dissimuler dans un réseau et à exploiter le plus longtemps

possible une attaque relève souvent de capacités techniques élevées. Par ailleurs, cette phase est souvent la plus difficile à identifier, d'où la nécessité d'indicateurs pertinents et un besoin de corrélation prégnant.

Afin de définir une stratégie de sécurité pertinente, il est nécessaire de se baser sur une approche multi-factorielle : technique, organisationnel ou encore métier.

Sans décrire ici l'ensemble des briques nécessaires à l'exploitation d'une bonne politique de sécurité des systèmes d'information (PSSI), quelques bases sont à respecter :

### Les bases techniques (liste non exhaustive) :

- La maîtrise de la configuration de ses systèmes (version logicielle, équipements installés, politique de gestion du changement, politique de maintien en condition opérationnelle et de sécurité, ...) ;
- La politique de journalisation des logs de tous les équipements du proxy au serveur métier (les équipements dits de sécurité ne sont pas les seuls à pouvoir fournir des logs pertinents, d'autant plus dans le cadre d'une surveillance comportementale) ;
- La maîtrise de ses annuaires (AD<sup>8</sup>, LDAP<sup>9</sup>, ... toutes ces briques doivent être maîtrisées et respecter un cloisonnement fort) ;

### - Une architecture suffisamment cloisonnée

(8) AD et GAD : « Active Directory et Global Active Directory » ce sont des annuaires qui fournissent des fonctionnalités d'authentification, de gestion des identités, de gestion des groupes et des services d'administration des services d'annuaire de l'entreprise.

(9) LDAP : « Lightweight Directory Access Protocol » Si LDAP était à l'origine un protocole standard pour accéder à des services d'annuaire (« AD »), c'est surtout maintenant une norme pour ces services.

pour garantir le service métier et assurer une protection contre les mouvements latéraux, tout en mélangeant des technologies issues de fournisseurs différents ;

- Une maîtrise forte des comptes à hauts privilèges (PAM - Privileged Account Management, bastion d'administration, coffre fort à mots de passe, réseau d'administration dédié...) ;

- La capacité à faire ressortir les bonnes informations parmi ces quantités de données (d'où le besoin de règles de corrélation pertinentes en prenant en compte les comportements dits « normaux » de son entité).

### Les bases organisationnelles (liste non exhaustive) :

- Connaître, identifier et responsabiliser les acteurs des équipes réseaux, systèmes et sécurité, et garantir que ces derniers sont bien informés de leur rôle dans le cadre de la gestion de la sécurité et des incidents ;
- Disposer d'un RSSI (Responsable

de la Sécurité des Systèmes d'Information), capable d'assurer en gestion de crise le management transverse des équipes, mais aussi, en temps calme la sensibilisation et le respect des politiques de sécurité (ce poste peut couvrir bien plus de responsabilité en fonction des entreprises, par exemple : pilotage des audits, management des équipes SOC, ... ) ;

- Disposer d'une organisation claire des responsabilités d'un point de vue SSI, ayant une certaine indépendance par rapport à la DSI et à ses contraintes budgétaires.

### Les bases métiers (liste non exhaustive) :

- Maîtriser les comportements métiers normaux et tenir informé les équipes techniques des changements potentiels dans les activités ;
- Assurer la sensibilisation à l'outil informatique des équipes, ainsi qu'à la bonne gestion de la sécurité des comportements utilisateurs (un grand nombre de guide existent, notamment ceux de l'ANSSI permettant d'obtenir un socle solide sur les bons comportements) ;
- Restreindre au juste nécessaire les accès des utilisateurs (mise en place d'une politique de gestion des accès et des identités basée sur chacun des rôles des membres de l'entreprise).



Ces éléments permettent ainsi de réduire considérablement le périmètre d'attaque, et optimisent les travaux des équipes de sécurité. Toutefois, ils ne garantissent aucunement un risque zéro des attaques informatiques. Il est donc nécessaire d'anticiper les scénarios de crise, et surtout de maintenir une politique de veille de sécurité.

### L'identification de la menace

Face à une cyber menace si bien organisée, comment doit-on réagir ? La communauté cyber a ainsi commencé à partager l'ensemble de ses indicateurs, permettant d'informer la communauté au plus tôt des chemins d'attaques rencontrés. À l'instar des tests de robustesse des algorithmes confiés à l'ensemble des acteurs du monde cyber, il est illusoire de pouvoir imaginer bénéficier uniquement de ses propres indicateurs de compromission (IOC « Indicator Of Compromise ») et de vivre en autarcie.

Ces initiatives sont donc vitales à la maturité de la sécurité des systèmes d'information à plusieurs titres :

- Informer la communauté pour anticiper et freiner la diffusion de la menace ;
- Circonscrire, voir rendre inopérant les codes ou attaques malveillantes.

Quelles sont ces communautés ou organisations en capacité de fournir ces indicateurs :

- Les entreprises ou les administrations qui se sont dotées des technologies nécessaires pour détecter les attaques dont elles sont ou pourraient être les victimes. Certaines d'entre elles, surtout celles dont les comités exécutifs ont pris la mesure du risque cyber, se sont équipées d'un CERT, une équipe de veille et surveillance de la menace et de réponse rapide à incident (« Computer Emergency Response Team ») et ont la possibilité de conserver et de trier leurs propres indicateurs ;
- Les CERT nationaux, comme le CERT-FR dont le rôle au sein de l'ANSSI (Agence nationale de la sécurité des Systèmes d'information) est notamment de corréler les informations sur les incidents, de traiter les alertes et d'échanger avec les autres CERT nationaux et privés. Certains gouvernements, comme celui du Royaume-Uni, favorisent ces échanges dans le cadre de partenariat privé-public comme le CISP (« Cyber-security Information Sharing Partnership ») initié par le NCSC (« National Cyber Security Center »).
- Des regroupements internationaux indépendants de CERT, comme l'organisation FIRST (siège basé à Cary en Caroline du Nord - USA), dont l'objectif est de mutualiser les informations de CERT issus de toutes les cultures et régions du monde. Les menaces étant globales, la réponse elle aussi doit l'être. FIRST regroupe plus de 500 CERT,

(10) SIRP : « Security Resonse incident platform » est une plateforme dédiée à la gestion des incidents de sécurité qui avec le SIEM réalise la corrélation des « logs » (journaux systèmes) pour en extraire les alertes de sécurité. Le SIRP aide les CERT et les équipes de sécurité à gérer leurs incidents.

(11) <https://www.ivation.fr/>  
NDLR : On définit par l'acronyme SOAR ces technologies logicielles qui permettent d'automatiser certaines tâches liées à la gestion de la sécurité informatique, et notamment, à la détection des incidents. Le terme SOAR (Security Orchestration, Automation and Response, qui signifie en français « Orchestration, automatisation et réponse aux incidents de sécurité informatique ») a été utilisé pour la première fois par le cabinet Gartner, en 2018.

dont 16 en France. En sont membres pour la plupart des grandes institutions bancaires françaises comme la Banque de France, le Crédit Agricole, La Société Générale, BNP Paribas, la Poste mais aussi le CERT-FR, le SIRP<sup>10</sup> d'Interpol et quelques autres.

- Les acteurs privés spécialisés dans l'orchestration, de l'automatisation et des solutions de réponses aux incidents de cyber sécurité<sup>11</sup>. Toutes ne fournissent pas exactement les mêmes services mais leur utilisation est bien sûr payante ;

- Les organisations sectorielles qui regroupent des acteurs d'un même type d'industrie (comme Aviation-ISAC pour le secteur aérien ou RH-ISAC pour les secteurs grande distribution et chaînes d'hôtels) afin d'échanger des informations sur les cybermenaces. Ces organisations favorisent aussi les échanges entre acteurs publics et privé, surtout aux US.

Ces organisations issues des US sont très fortement orientées pour défendre les actifs Américains.

### Comment s'organiser face à la menace et anticiper pour être prêt, par exemple en cas de pandémie mondiale

En effet, reprenant ainsi l'analogie de la pandémie, il est nécessaire de veiller à alerter l'ensemble de la chaîne dès l'apparition des premiers « clusters » de diffusion afin de se prémunir de la pandémie. L'étape suivante est de fournir l'antidote ou le vaccin afin de rendre cette menace mineure et être ainsi capable de vivre avec.

Ces éléments sont devenus vitaux, notamment du fait d'un marché parallèle au sein duquel sont vendus ces malwares, trojans ou concepts d'attaques. Il n'est pas rare de voir ressurgir des versions mutantes des malwares quelques années après la diffusion de ces « zero day ».

Compte tenu de la rapidité de mutation de ces malwares, il est donc indispensable d'agir sur la rapidité de diffusion des symptômes permettant de déceler ces attaques informatiques.

Une fois les informations collectées, le problème est souvent dans la détermination de leur pertinence. L'idée d'organiser ces IOCs a émergé et certaines plateformes ont ainsi pris naissance notamment en open source tel que OPENCTI

(12) MISP : « Malware Information Sharing Platform » une plateforme "open-source" pour rassembler, stocker, partager et corréler les informations sur les attaques cyber, les informations sur les vulnérabilités, et même de l'information liée au contre-terrorisme.

ou MISP<sup>12</sup>. Par exemple, le projet OpenCTI (Open Cyber Threat Intelligence) est développé par l'ANSSI en partenariat avec le CERT-EU. C'est un outil de gestion et de partage de la connaissance en matière d'analyse de la cybermenace (Threat

Intelligence). Initialement conçue pour structurer les informations de l'agence relatives à la menace informatique, la plateforme facilite aussi les interactions entre l'ANSSI et ses partenaires. L'outil, intégralement libre, est aujourd'hui disponible pour l'usage de l'ensemble des acteurs de la « threat intelligence ».

Un éco système complémentaire de logiciel libre est disponible, permettant ensuite de centraliser la gestion et le suivi de la réponse (The Hive), et Cortex x permettent d'utiliser des données MISP (Malware Information Sharing Platform) ainsi que des données provenant d'autres sources pour enrichir le contexte.

### **Le besoin de protéger les acteurs qui échangent des informations sur les menaces**

Cependant, malgré cette volonté et nécessité de partage de l'information, des réticences sont encore nombreuses. En effet, la collaboration atteint ses limites quant à la diffusion d'une information permettant de déduire qu'une grande

entreprise ou administration a été victime d'une cyber attaque. Qui n'a jamais pensé qu'une entité victime de cyber attaque n'était donc pas de confiance ?

Quel impact pour sa santé financière, non pas à cause de l'attaque elle-même mais à cause de la notoriété impactée par cette attaque ? Autant de questions qui soulignent les réserves potentielles à partager ces informations.

Il est donc nécessaire de se pencher sérieusement sur la protection des entités qui consentent à partager leurs indicateurs de compromission. Beaucoup hésitent encore même si tout le monde s'accorde à dire qu'ensemble face à une menace toujours plus variée et toujours plus sophistiquée, nous serons plus forts. En Europe et en France en particulier, il n'existe pas de garantie légale que ce partage de l'information ne se retournera pas contre ceux qui ont eu l'honnêteté et le courage de partager leurs IOC et ce dans le but même d'aider et renforcer nos défenses face à des ennemis de mieux en mieux organisés et financés alors qu'elle existe bien aux États-Unis. L'administration Obama a, en effet, fait adopter par le Congrès Américain une loi : le CISA (« Cyber Security Information Sharing Act ») dont le but est de fournir une protection juridique aux acteurs qui échangent des informations sur les menaces de cyber sécurité pour peu que ces échanges



soient conformes aux règles stipulées dans la loi. La question est donc posée : comment favoriser l'adhésion du plus grand nombre et protéger les sources d'informations ?

### Conclusion

Fort de ces éléments, plusieurs constats sont donc à synthétiser :

A l'instar des US, n'est-il pas souhaitable de fédérer la communauté européenne pour le partage des indicateurs. Pourquoi ne pas imaginer une réponse

commune aux attaques cyber ; cela n'aurait-il pas limité les impacts de Wannacry ?

En complément de ces partages d'informations, et toujours dans l'optique d'une amélioration de la circulation de l'information, n'est-il pas nécessaire de protéger les contributeurs afin de défendre des intérêts communs ?

Bien sûr, il est facile d'opposer à ces propositions la souveraineté nationale des différents États,

mais n'est-il pas envisageable de distinguer les actifs primordiaux d'un État et de ne pas exposer ces derniers lors du partage d'IOC. Par ailleurs, un grand nombre de systèmes d'informations sont basés sur des technologies communes. Le partage d'indicateurs ne met donc pas en exergue les architectures des États membres, sauf usage de technologies spécifiques.

Enfin, un volet légal ne permettrait-il pas un partage accru des bonnes pratiques et ne renforcerait-il pas une réaction commune de l'Europe face à des menaces étatiques fortes ?

Ainsi, soutenons ce vœu pieu d'une réponse européenne à la fois technique, organisationnelle et juridique.

f. <https://www.congress.gov/bill/114th-congress/senate-bill/754>

g. <https://www.fireeye.fr/current-threats/apt-groups.html>

h. <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/>

i. <https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager>

## Bibliographie

a. <https://www.ssi.gouv.fr/administration/bonnes-pratiques/>

b. <https://www.misp-project.org/>

c. <https://thehive-project.org/>

d. <https://www.cert.ssi.gouv.fr/>

e. <https://www.first.org/>

## L'AUTEUR

Robert Breedstraet - Division information security officer, adjoint au Corporate CISO d'Amadeus IT Group.

Robert Breedstraet dirige le département gouvernance et contrôle, le management de projets de cyber sécurité comme la gestion des identités et des accès, la protection de la marque Amadeus.

Il a aussi sous son autorité les responsables régionaux de sécurité informatique (Amériques, Inde, Asie-Pacifique, Europe et Moyen Orient). Robert a une expérience de plusieurs dizaines d'années en informatique et en particulier dans le domaine de la réservation aérienne.

Il est également représentant d'Amadeus dans différents groupes internationaux, informaticien et titulaire d'une maîtrise en politique économique, il est auditeur IHEDN - INHESJ de la première session nationale Souveraineté Numérique et Cyber-sécurité.

## L'AUTEUR

Mathieu Thuaiere exerce la fonction de RSSI au sein du SGDSN. Dans le cadre de ses activités, il a en charge la politique de sécurité et ses aspects réglementaires au sein de son entité, la réalisation de la politique d'audit et sa mise en application, et enfin la responsabilité du SOC et le management des programmes cyber.

Mathieu Thuaiere a une expérience de plusieurs années dans la cyber sécurité, et plus particulièrement dans l'administration, avec notamment un passage en tant que manager programme à la DGA, puis au SGDSN. Il est également auditeur IHEDN - INHESJ de la première session nationale Souveraineté Numérique et Cyber-sécurité.

# La « Deepfake reality » : vers la fin de la vérité dans le cyberspace ?

Questions à **Franck DeCloquement**

# D

ans cette nouvelle fabrique du sens qu'est devenu l'internet, une vigilance accrue des pouvoirs publics se fait jour face aux nouvelles « menaces à la vérité ». La question fondamentale est la crédibilité des informations que nous percevons demain à travers le cyberspace. Franck Decloquement s'entretient avec nous de cette problématique qui intéresse, outre notre entendement et les libertés associées, le fondement de nos sociétés médiatisées.



**FRANCK DECLOQUEMENT**

Professeur à l'IRIS  
MBA « Gééconomie  
et gestion des  
risques »

**La Revue : « Actions sur les perceptions », « guerre du sens », « faits alternatifs » et « menaces à la vérité » ? Quoi de neuf dans le champ des opérations de propagande, à l'ère des réseaux sociaux et du web 2.0 ?**

Franck DeCloquement :

Dans nos démocraties occidentales en proie au doute, au séparatisme communautaire et à la tentation illibérale, la liberté d'expression qui circule sur les réseaux dits « sociaux » est à la fois un formidable mécanisme de contre-pouvoir mais aussi une promesse de déstabilisation massive pour nos démocraties représentatives, avec l'émergence de ces « vérités alternatives » qui y font florès. L'affaire des gilets jaunes en a été le démonstrateur évident. Parce qu'elle est cette nouvelle « forge » de l'opinion publique et de ses revendications tues, la vie des réseaux sociaux suscite la convoitise des influenceurs politiques et des législateurs qui cherchent naturellement à la mettre au pas ou à l'endiguer. Cependant, la vie trouve toujours son chemin ! Ce quadrillage de l'opinion publique, qu'il vienne des grandes plateformes elles-mêmes ou des pouvoirs publics, ne doit pas oblitérer le fait qu'à l'individu seul incombe en définitive le soin et la responsabilité de choisir ses informations, afin de juger au mieux de la compétence de ses édiles.

Sur le plan international et intérieur, les pays occidentaux sont impliqués depuis plus d'une trentaine d'années, dans des « foires d'empoigne » où les communautés s'affrontent au nom de leurs valeurs propres et revendiquent une légitimité politique ou idéologique qui justifierait leur combat. Dans ce véritable malström pour la « guerre du sens », qui s'opère par médias interposés, rien de véritablement neuf sous le soleil en matière d'accaparement de la réalité si ce n'est la puissance accrue de ces opérations de falsification, augmentée cette fois par l'apport déterminant des nouvelles technologies digitales opérant au sein du Web 2.0. En conséquence, dans ces nouveaux espaces de conflictualités délétères et de luttes sémantiques, les fausses nouvelles à des fins de propagande ou les deepfakes à visée parodique s'y multiplient tout naturellement à un rythme exponentiel. Cela représente évidemment un risque accru de désinformation pour les populations.

Le courage, la haine, le jusqu'aboutisme, la tromperie, l'assujettissement des consciences et le brouillage des faits en constituent indubitablement le moteur. Des discours trafiqués aux images truquées, les fausses nouvelles se propagent à toute vitesse à travers les réseaux digitaux. Les fameuses deepfakes, par exemple, se basent pour l'essentiel sur les avancées de l'intelligence artificielle. Elles consistent, très schématiquement, à fusionner des vidéos, dans un but

de substitution notamment de visages et de sons afin de réaliser des trucages pour orienter le sens de la compréhension ou tout simplement pour faire sourire la multitude. Parfois pour une noble cause, la fausse vidéo de Donald Trump réalisée par « Solidarité sida » en est un exemple type.

Toutefois, dans la majeure partie des cas, il s'agira de diffuser des informations erronées afin de discréditer une personnalité pour manipuler l'opinion publique à des fins idéologiques. Cette tendance lourde ne devrait pas s'éroder dans les prochaines années, dans ces espaces d'affrontement virtuels qui sont plus que jamais devenus le reflet de nos turpitudes collectives, à l'approche d'élections présidentielles déterminantes, par exemple.

(1) Yves Citton est professeur de littérature à l'Université Paris-VIII. Il est l'auteur de livres et d'articles consacrés à l'imaginaire politique de la modernité occidentale. Il est directeur de l'École universitaire de recherche ArTeC depuis 2018. [https://fr.wikipedia.org/wiki/Yves\\_Citton](https://fr.wikipedia.org/wiki/Yves_Citton)

Au sein de l'écosystème attentionnel dans lequel nous sommes peu ou prou plongés, selon le chercheur Yves Citton<sup>1</sup>, s'accumulent irrémédiablement dans nos cerveaux des informations parfaitement disparates qui finissent tôt ou tard par converger et se combiner

entre elles pour faire sens. Or, l'art de faire adhérer, de faire croire ou de faire penser dans le champ psychologique, prend désormais le pas sur l'art de manœuvrer la force brute pour soumettre autrui à sa





Efficace, cette vidéo a été critiquée. L'incrustation qui spécifiait qu'il s'agissait d'une fake news n'apparaissait que 50 secondes après son début. Le plus faible temps consacré par les internautes à l'examen de documents médias l'occultait et accréditait la véracité du document. Le directeur de campagne a spécifié avoir privilégié la densité de l'information.

© Solidarité SIDA

volonté dans le champ du réel. L'objectif fondamental vise, en définitive, à produire ces opérations d'influence offensives afin d'orienter la compréhension de l'adversaire, jusqu'à le faire œuvrer parfois contre ses propres intérêts.

**La Revue : À quoi devons-nous faire face au juste, quand on parle de « deepfake reality » ou de « faits alternatifs » ?**

**Franck DeCloquement :** Cette petite fabrique de l'opinion publique 2.0 ne cesse d'innover dans ses modalités d'actions subversives. La créativité sémantique et l'imagination des attaquants dans ce nouvel écosystème digital apparaissent

sans limites. À titre d'exemple, les faits alternatifs ont fait irruption dans notre espace perceptif commun voilà quatre ans lorsque Kelly-Anne Conway, conseillère spéciale du président Trump, évoqua ce terme, courant 2017, pour justifier les dires du porte-parole de la Maison-Blanche, Sean Spicer. Au lendemain de la cérémonie d'investiture du 45<sup>e</sup> président des États-Unis, celui-ci accusait en effet les médias d'opinion américains d'avoir volontairement sous-estimé les chiffres de la foule qui y assistait, autrement dit, de remettre en cause l'importance de la participation publique lors de l'investiture du président Trump. Or les données disponibles d'alors montraient bien qu'il n'y avait pas eu autant de participants que cela aux



réjouissances, en tout cas, bien moins que pour celle de Barack Obama. Sean Spicer a depuis admis que certains des chiffres qu'il avait mobilisés pour son argumentaire étaient incorrects, même s'il les avait crus pourtant exacts sur le moment.

Très concrètement, les « faits alternatifs » sont des mensonges ou des « *bullshit* » (bobards, sottises, stupidités, balivernes, conneries, affabulations, mensonges, crâneries), ayant pour intention principale de plier la réalité à des objectifs prédéfinis, en la manipulant ou en la « façonnant » en fonction d'un « état final recherché » (EFR), selon une terminologie bien connue dans le champ de l'action psychologique à

visées militaires. Ce qui change et interpelle dans l'exemple américain évoqué précédemment, c'est cette capacité indubitable pour les parties prenantes à assumer le mensonge et à faire mine de le considérer comme un élément quasi factuel. Nous sommes ici dans le registre du bobard pur et simple, utilisé sciemment comme matériau de construction d'une argumentation indubitablement falsificatrice, soit une « construction de la réalité ».

Cela diffère grandement, avouons-le, d'une manipulation de masse classique à la sauce Orwellienne, usant d'une *novlangue* limitant le langage, pour mystifier le discernement d'une population. On était habitués à ce

que l'histoire soit réécrite par les vainqueurs dans les périodes post-confliktuelles mais, dorénavant, c'est le passé immédiat et les événements de la veille qui sont susceptibles d'être instantanément réécrits et revus en quasi-temps réel alors que tout le monde a pourtant encore les faits de la veille en mémoire.

Concernant les *deepfakes*, les avancées vertigineuses en matière d'intelligence artificielle (IA) et de *deep learning* permettent aujourd'hui de façonner ou de contrefaire le réel pour lui faire dire ce que l'on veut, ou presque ! Grâce à la puissance croissante des algorithmes « apprenants », les *deepfakes* gagnent constamment en sophistication, obligeant les chercheurs en génie logiciel à perfectionner leurs outils de détection. Mais de quoi s'agit-il au fond ? Le terme récent de « *deepfakes* » est une expression forgée en ajoutant au terme « *fake* » le terme « *deep* », pour « *deep learning* » ou apprentissage profond. Ce néologisme anglophone désigne en somme un ensemble de procédés techniques permettant aux intelligences artificielles d'apprendre à reconnaître des formes, des structures, des motifs, des objets ou des personnes. Les anglophones parlent ici de « *Patterns* » : un terme polysémique ayant moult traductions en langue française. La « *deepfake reality* », quant à elle, découle en droite ligne de cet usage délétère et intensif par certains États ou groupes d'acteurs des outils du faux,

pour convaincre un auditoire-cible.

Ce sont des actions d'intelligence menées dans le but d'orienter la réalité perçue par autrui, en jouant sur le filtre de ses perceptions ou de ses biais cognitifs. Une forme de « guerre sans la faire » en somme, mais qui se livre dans le champ psychologique de l'adversaire.

**La Revue : Quand la prolifération de ces « armes du faux », selon l'expression consacrée du chercheur François-Bernard Huygues, augure dangereusement d'une possible désintégration du ciment de nos sociétés démocratiques, pourrions-nous encore croire demain tout ce que nous verrons sur la toile, et ses plateformes sociales ?**

**Franck DeCloquement :** Rien n'est moins sûr en effet, si on considère l'arsenal digital et les outils de falsification qui sont aux mains des prédateurs. Du fait de la promesse tenue d'une « réalité augmentée », il se pourrait bien que nous nous dirigions à grands pas – compte tenu des avatars de la « *Deepfake reality* » – vers une « réalité diminuée » ou une version très « rabougrie » de celle-ci ! Dans l'analyse classique qui est faite du cyberspace en trois couches, la composante sémantique ou informationnelle du cyber, recèle l'ensemble des informations qui transitent sur la toile. Les enjeux stratégiques actuels se portent indéniablement vers la maîtrise de cette 3<sup>e</sup> dimension informationnelle où s'opère justement la conflictualité, la contrefaçon

(2) <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/manipulations-de-l-information/rapport-conjoint-caps-irsem-les-manipulations-de-l-information-un-defi-pour-nos/>  
[https://www.diplomatie.gouv.fr/IMG/pdf/les\\_manipulations\\_de\\_l\\_information\\_2\\_cle04b2b6.pdf](https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2_cle04b2b6.pdf)

des faits n'y étant pas le moindre mal à gérer par les Etats occidentaux. Pour preuve, les constats du document produit en 2018 par l'IRSEM et le CAPS<sup>2</sup>, sur les manipulations de l'information envisagées sans ambages comme « un défi absolu pour nos démocraties ».

À titre d'illustration, le grand classique de la littérature de George Orwell, « 1984 » que nous évoquions plus haut ne disait pas autre chose. Il figure toujours parmi les meilleures ventes de livres à travers le monde ! L'auteur y préfigurait déjà ? en 1949, comment le pouvoir politique fictif, qu'il dépeignait à travers son œuvre, contrôlait drastiquement les esprits et les cœurs de ses citoyens en manipulant sans vergogne la vérité des faits. Dans son chapitre IX, Orwell y avait rédigé cette injonction parfaitement annonciatrice des périls qui nous guettent : « Pour diriger et continuer à diriger, il faut être capable de modifier le sens de la réalité ». C'est en somme ce que sont en capacité de produire aujourd'hui tous ces moyens digitaux sur nos psychés. C'est entre autres le jeu auquel s'adonnent les régimes autoritaires et populistes à travers la planète, à l'ère du Web 2.0. C'est aussi ce que font de grandes plateformes sociales américaines, en croissance constante partout dans le

monde. Cette année « 1984 » fictive promise par Orwell au siècle dernier, n'est-elle pas définitivement devenue notre réalité, avec ce présent aux relents de guerre froide que nous sert quotidiennement l'Amérique de Donald Trump à travers ses « faits alternatifs » et sa « post-vérité » mais aussi la Russie de Vladimir Poutine, en pointe sur la désinformation comme au bon vieux temps recouvré de l'Union Soviétique ? L'avenir glorieux que nous réserve la Chine de Xi Jinping n'est pas en reste, empreint de cette propagande communiste d'antan, mais aujourd'hui mâtinée de technologies intelligentes dernier cri... Ne sommes-nous pas en train de basculer subrepticement dans une ère de « post-vérité intégrale », au risque de briser irrémédiablement sur ces récifs le socle de nos sociétés occidentales ? La question se pose indubitablement, un peu plus chaque jour.

**La Revue : Est-ce que les attentes des différents Etats en matière d'implication des GAFAM dans la régulation des contenus ne rencontrent pas un frein dans les modèles économiques que ces derniers ont choisi ?**

**Franck DeCloquement :** Le paradoxe n'est pas mince. Si Mark Zuckerberg, le fondateur emblématique de la multinationale Facebook, accepte aujourd'hui l'augure d'un meilleur contrôle d'Internet par les Etats occidentaux, sa posture affable peine à cacher la réalité de son emprise croissante

sur nos vies et notre modèle de démocratie. Ravir nos attentions collectives, les monétiser sans relâche et maintenir nos cognitions individuelles captives de leurs dédales digitaux, via l'usage de *Dark Patterns*, est bien in fine le grand jeu des plateformes dites « sociales » dans leur ensemble. Le principe de ces *Dark Patterns* repose sur un précepte assez simple en définitive : inciter l'utilisateur lambda à faire une action qu'il n'aurait pas eu l'intention d'effectuer de lui-même sans être influencé, si possible sans qu'il s'en rende compte... Le but recherché est, par exemple, de collecter ses données personnelles plus aisément, de lui faire ajouter des produits dans son panier utilisateur ou encore de lui faire passer plus de temps sur une interface spécifique afin d'améliorer le trafic du site. L'une des plus célèbres formes de *Dark Pattern* connues est le « *Privacy Zuckering* », en référence à Mark Zuckerberg justement ! Celle-ci s'opère principalement en coulisses, quand vous êtes très progressivement invité par la plateforme de réseautage social à partager publiquement beaucoup plus d'informations sur vous-même, que vous ne le souhaitiez initialement... Le sobriquet « *Privacy Zuckering* » a d'ailleurs fini par s'imposer aux États-Unis pour qualifier ce type de procédé qui repose pour l'essentiel sur un « élément de design douteux » qui vise à orienter ou manipuler le choix de l'utilisateur en ligne. Il s'oppose en cela à « l'UX éthique » (ou design éthique), qui consiste

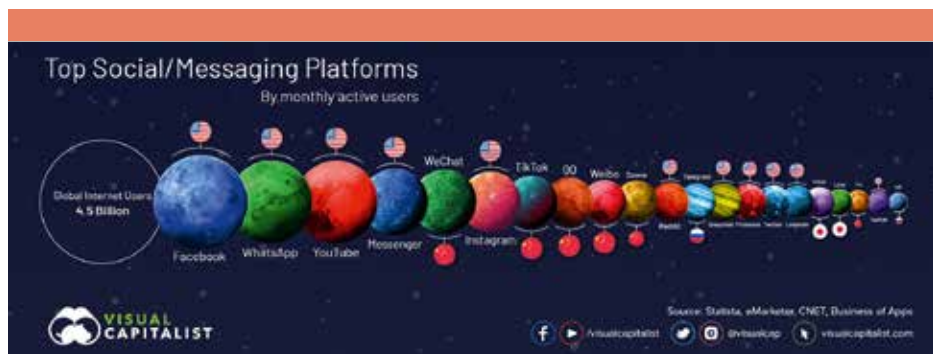
à penser et à concevoir un site web de manière à ce que l'expérience utilisateur soit privilégiée, et demeure la meilleure possible.

La commercialisation de nos données personnelles assure de gigantesques profits aux firmes géantes de la Tech, essentiellement américaines et toutes sous contrat avec le Pentagone. En réclamant en mars 2019 une intervention plus musclée des États dans la régulation du web, récidivant le 10 mai 2019 à l'Élysée aux côtés d'Emmanuel Macron, et prônant pour la France et l'Europe « un nouveau modèle de régulation d'internet », Mark Zuckerberg approuvait dans la foulée l'appel de Christchurch contre les contenus terroristes, extrémistes et haineux, à l'initiative concertée de plusieurs dirigeants occidentaux, outre celle de la Première ministre néo-zélandaise Jacinda Ardern et celle du président français. Trompe l'œil que tout cela ! Derrière les bonnes intentions affichées, l'essayiste Bruno Patio résume impeccablement cette affaire « d'encerclement cognitif » mis en œuvre par les plateformes sociales dans son ouvrage à succès, « la civilisation du poisson rouge » : « Les empires économiques ont créé une nouvelle servitude avec une détermination implacable. Au cœur du système, et au cœur de notre vie quotidienne, un projet caché : l'économie de l'attention. Augmenter la productivité du temps pour en extraire encore plus de valeur... ». Sur la durée, on évalue

encore mal les conséquences exactes de ces technologies de rupture sur la fragile trame du tissu social de nos systèmes démocratiques, la bonne tenue de leur cohésion générale face à la production de contenus hautement déstabilisants mais aussi leur impact général sur le développement de l'esprit critique des populations. L'accroissement de la crédulité générale est bien entendu en ligne de mire des falsificateurs de tous poils, et autres promoteurs de « faux ». Ne nous voilons évidemment pas la face : la diffusion des *deepfakes* n'est pas seulement un problème technologique qui pourra être résolu par un surcroît de technologie. A contrario, les explications technophiles très orientées « business » d'un Mark Zuckerberg, qui promettait déjà l'an dernier – et pour cause – de résoudre ce problème grâce à l'usage intensif d'une « IA plus performante », occultent en réalité un problème structurel crucial bien plus prosaïque. La croisade

de Zuckerberg cache l'emprise indéniable des GAFAM sur nos vies. Le modèle économique initialement adopté par les plateformes sociales, comme Facebook, exploite en réalité ardemment ce type de contenus contrefaits pour mieux prospérer. En la matière, le bon sens commanderait évidemment de ne pas confier les clefs du poulailler à « Maître Renard » en espérant qu'il assurera loyalement et en toute quiétude la surveillance des gallinacés ! Gageons que Jean de La Fontaine aurait aussi trouvé à y redire...

La nouvelle puissance des réseaux sociaux assume indéniablement une sorte de cinquième pouvoir, à côté de celui des médias audiovisuels et de la presse écrite traditionnelle. Elle oblige aussi à la responsabilité accrue et à la vigilance extrême de nos élus. Sans filtrage éditorial apparent, les faits et les opinions se bousculent dans les groupes *Facebook*, les *threads*



Le classement des plateformes révèle immédiatement l'enjeu économique, sociétal et géostratégique qu'elles génèrent par leur business-modèle ou leur contrôle par certains États.

de *Twitter*, les vidéos *YouTube* ou *TikTok*. Cette révolution silencieuse qui imprègne désormais nos perceptions, oblige lourdement nos élites politiques à de nombreux examens de conscience.

**La Revue : En n'envisageant la lutte contre les effets de la Deepfake Reality qu'à l'aune d'une remédiation technique, les géants de la Silicon Valley ne s'exonèrent-ils pas de leurs relations symbiotiques avec ces contenus profitables et consubstantiels de leur business-modèle ?**

**Franck DeCloquement :** C'est indéniable. Cette posture ambiguë leur est en effet consubstantielle et incluse, pourrait-on dire, au cœur même de leur ADN industriel, compte tenu du choix de leur business-modèle. La conflictualité, les propos haineux, rageurs et complotistes génèrent du trafic en très grande quantité et alimentent la machine. Le volume des audiences-cibles s'en trouve naturellement augmenté et les recettes publicitaires nécessairement boostées. Pour résumer à grands traits nos propos précédents et enfoncer le clou, les médias sociaux et les grandes plateformes du web sont cyniques par nature. La relation très ambiguë qu'entretiennent ces multinationales géantes de la Silicon Valley, avec la diffusion d'informations alternativement « factices » ou « factuelles », s'explique en grande partie par la poursuite implacable de leurs intérêts commerciaux bien compris. Lorsque le business-modèle d'une

plate-forme consiste à maximiser le temps d'engagement de ses audiences (certains parleraient ici de « temps de cerveaux disponible »), afin de s'octroyer des revenus publicitaires astronomiques, des contenus controversés, choquants, complotistes ou parfaitement complaisants sont tout naturellement poussés jusqu'au sommet de la « chaîne alimentaire » pourrait-on dire.

C'est bien là que réside la véritable ambiguïté de fond car en le formulant indubitablement sous le seul prisme des errements de la technologie, ces puissantes plates-formes technologiques américaines distraient en réalité opportunément leur public – ainsi que certains pouvoirs publics – de l'idée qu'il pourrait y avoir des liens de connivences et d'intérêts croisés bien plus fondamentaux, en deçà de notre appréhension des véritables enjeux géopolitiques et financiers pour l'essentiel. Ainsi peut-on résumer très schématiquement la chaîne de valeur qui les meut.

Pour les spécialistes avertis de l'association militante « la quadrature du Net », la régulation des contenus haineux ou contrefaits par les seuls géants du Web est clairement vouée à l'échec. Cette petite équipe d'experts et de juristes, d'inspiration libertaire, mène d'ailleurs une campagne de lobbying musclée contre les GAFAM depuis quelques années, accusés de beaucoup trop s'immiscer dans nos vies privées. En lutte contre les faux dilemmes et les fausses évidences nourries



par les cabinets de lobbying inféodés aux GAFAM, elle préconise en outre deux autres options possibles, mais non suivies jusqu'alors par les gouvernements : renforcer le rôle de la justice sur le plan numérique, en musclant ses effectifs dédiés mais aussi développer des formations d'aguerrissement, ayant toutes une vocation à édifier les « esprits et les cœurs ». En somme, il s'agirait de vacciner individuellement les internautes contre les méfaits cognitifs d'un usage irréfléchi et intensif des plateformes sociales, mais aussi des réalités frelatées qu'elles véhiculent, conformément en cela aux impératifs de leur business-modèle. Pour l'heure, leurs nombreuses recommandations n'emportent pas la conviction des décideurs politiques successifs, plus adeptes d'imposer un filtrage et une centralisation accrue du Web, mais opérés par ces plateformes elles-mêmes... Une alliance impossible par nature, tel le mariage de la carpe et du lapin, confinant véritablement à un syndrome de Stockholm vis-à-vis des GAFAM, de l'avis général des plus fins spécialistes de la toile.

## L'AUTEUR

**Franck DeCloquement est praticien et expert en intelligence économique et stratégique. Ancien de l'École de Guerre Économique de Paris (EGE), membre du CEPS (Centre d'Etude et de Prospective Stratégique), de la CyberTaskForce, membre fondateur du Cercle K2, il est professeur à l'IRIS (MBA « Géoéconomie et gestion des risques »). Il enseigne à l'IHEDN les actions d'influence et de contre-ingérence économique, les stratégies d'attaques subversives adverses contre les entreprises. Il a également enseigné la géopolitique des médias et de l'Internet en Master 2 recherche « Médias et mondialisation », à l'IFP (Institut français de presse) de l'université de Paris II Panthéon-Assas.**



# Cybersécurité et protection

## des données : pourquoi les entreprises sont-elles plus exposées après la crise ?

Par Marie de Freminville

# D

Diverses raisons expliquent l'exposition aux risques cyber de l'ensemble des organisations : le contexte imprévu et anxiogène, la désorganisation du cadre de travail et des comportements inadaptés, et des dispositifs de cyber sécurité insuffisants (outils, gouvernance, processus, ressources, formation). Il est temps de définir une stratégie de cybersécurité. La prochaine crise sera numérique !



**MARIE DE FREMINVILLE**

Présidente de  
Starboard Advisory

Il n'a échappé à personne que la crise Covid-19 a été un accélérateur exceptionnel de transformation numérique : de nombreuses initiatives ont été prises dans l'urgence pour réaliser des opérations à distance (vente, administration, communication interne, gestion de projets...) qui n'avaient pas

encore vu le jour pour des raisons politiques ou culturelles, de résistance au changement ou de cyber risques. Nous avons assisté au développement du télétravail, de la signature électronique, à la création de nouveaux sites e-commerce, et à l'utilisation croissante d'outils collaboratifs (partage de fichiers ou réunion en visio-conférence).

La crise COVID-19 a forcé les entreprises (même les grandes entreprises qui n'avaient pas anticipé une telle situation) à prendre les dispositions nécessaires pour une grande partie des effectifs et sur une durée inconnue : achat de PC portables, transport de PC fixes au domicile ou encore utilisation de PC privés à des fins professionnelles...

Revers de la médaille : cette période a considérablement augmenté la surface d'attaque et l'exposition au risque de vol de données, de fraude ou de demandes de rançons. Elle a aussi été la révélatrice de la dépendance des entreprises au numérique,

qui permet de faire fonctionner l'économie et de maintenir le lien social. Le SI est devenu, pour la plupart des entreprises, des collectivités locales ou des hôpitaux, un organe vital sans lequel l'organisation peut être paralysée ! Une fuite de données stratégiques ou personnelles peut avoir des conséquences mortelles ou fragiliser durablement l'entreprise, mais aussi ses parties prenantes.

Faire la cyber autruche et attendre l'attaque pour intervenir n'est pas recommandé !

Certaines entreprises en ont en effet déjà subi les conséquences : la mutuelle MMA a demandé aux collaborateurs de rapporter leur matériel informatique, pour le sécuriser. Par ailleurs, les salariés ont été priés de revenir sur site, sauf cas particulier. D'autres organisations, telles que Rabot Dutilleul, Bolloré Transport & Logistics, Faro Technologies, ou encore le Conseil départemental d'Eure-et-Loir, ont été attaquées récemment...

### **Pourquoi les entreprises sont-elles plus exposées après la crise ?**

**Première raison : le contexte de crise sanitaire** a en effet facilité la tâche des cybercriminels, qui n'attendent pas longtemps avant de saisir une nouvelle occasion d'attaquer. Créatifs et rapides, ils profitent du fait que la surface d'attaque a naturellement augmenté pendant la crise : utilisation accrue d'Internet,

navigation sur le Web, achats en ligne et utilisation des réseaux sociaux.

La crise sanitaire est anxiogène et les internautes sont vulnérables. Les cybercriminels le savent très bien. L'état de confusion et d'anxiété des collaborateurs engendrent de mauvaises manipulations et la pandémie est donc une excellente opportunité pour tromper la vigilance des utilisateurs.

Les nouvelles attaques liées au Covid-19 (malwares, attaques DNS, noms de domaines frauduleux, faux sites, spams, phishing, faux installateurs) sont nombreuses et ne sont pas identifiées par les systèmes de sécurité. Entre le 9 mars et le 23 mars, 316 523 nouveaux sites factices relatifs au Coronavirus ont été repérés, ayant pour objectif de voler des identifiants et d'adresser des malwares sur les postes de travail qui n'ont pas été mis à jour.

Les mobiles sont aussi des vecteurs d'attaque. De fausses applications exploitent la crise du Coronavirus et accèdent aux photos, vidéos, fichiers, à la localisation du terminal, ainsi qu'à l'autorisation de prendre des photos et d'enregistrer des vidéos. Des courriels et SMS usurpant la marque de grandes enseignes (de la vente en ligne, de sociétés de transport, de banques, d'administrations ou d'ONG) ont permis de récupérer les identifiants et les mots de passe de leurs utilisateurs.



© Par metamorworks - Base adobe stoc

Le télétravail a modifié la perception des menaces du fait de la confusion des outils privés et professionnel, de la redistribution des systèmes d'authentification et des logiciels « métiers ». Cela oblige à adopter une stratégie pérenne qui mobilise les décideurs, les usagers et les responsables de SI.

Enfin, des campagnes de phishing prenant l'apparence d'outil de visioconférences récoltent ainsi les informations d'identification des utilisateurs via des courriels ou encore un lien qui invitent le destinataire à cliquer pour activer son compte en le redirigeant vers une page web frauduleuse afin qu'il y saisisse ses identifiants. Un autre type de mail prétexte une réunion manquée, comprenant un lien vers une fausse page d'identification. Les niveaux de sécurité de ces plateformes sont divers (des études ont été publiées à ce sujet).

**Deuxième raison : le cadre de travail est désorganisé** à la fois pour les utilisateurs et pour les équipes informatiques et de sécurité.

(1) [https://www.trendmicro.com/fr\\_fr/about/newsroom/press-re](https://www.trendmicro.com/fr_fr/about/newsroom/press-re)

(2) <https://www.tessian.com/research/the-state-of-data-loss-prevention-2020/>

Selon l'étude Trend Micro<sup>1</sup>, les salariés prennent des libertés avec les règles de l'entreprise : 56% reconnaissent utiliser au moins une application personnelle sur leur outil

de bureau, et 64% ont déjà téléchargé des données de l'entreprise vers cette application. 80% admettent utiliser leur PC professionnel pour un usage personnel sur Internet.

Selon une étude publiée par Tessian<sup>2</sup>, la moitié des employés admettent qu'ils prennent des raccourcis en télétravail en matière de cybersécurité, comme le partage de fichiers confidentiels par courrier

électronique au lieu de recourir à des mécanismes plus fiables.

Les télétravailleurs mélangent leurs usages personnels et professionnels sur leur poste de travail (soit personnel, soit fourni par l'entreprise) et l'utilisation d'applications non-sécurisées se développe.

(3) <http://www.revue-banque.fr/management-fonctions-supports/breve/les-dirigeants-mailon-faible-securite-mobile>

Les dirigeants s'estiment souvent au-dessus des règles ! «Trouble at the Top» selon une étude publiée par MobileIron<sup>3</sup> : bien que visés par

les cybercriminels, 74% d'entre eux demandent de relâcher les mesures de sécurité mobile, 45% d'entre eux estiment qu'elles freinent l'utilisation de leur appareil. 37 % ont voulu accéder à des données professionnelles à partir d'une application non reconnue.

Les usages évoluent : la tendance est de passer d'un SI central à un modèle cloud. Les utilisateurs organisent les espaces partagés et en sécurisent les accès, alors que la gestion des accès est traditionnellement mise en œuvre par l'équipe informatique.

Enfin, la charge de travail des équipes informatiques augmente : achat d'ordinateurs, installation de logiciels de sécurité, formation aux outils et aux bonnes pratiques de télétravail, surveillance des activités à distance (les comportements

changent comme les horaires de travail par exemple ce qui crée de fausses anomalies dans les systèmes de détection).

Elles sont moins disponibles, par exemple, pour :

- Former les collaborateurs, les intérimaires et les prestataires aux nouveaux usages et outils, les sensibiliser aux risques de sécurité liés au télétravail et adresser des instructions claires sur ce qu'ils peuvent faire ou ne pas faire.
- Informer les utilisateurs des nouvelles menaces et attirer leur attention sur les tentatives des cyber attaquants, qui utilisent le COVID ou les outils de visio-conférence pour piéger les utilisateurs.
- Compléter la liste des sites ou mots-clés en "liste noire" et monitorer les accès distants.

### **Troisième raison : un manque d'outils et des processus techniques inadaptés**

sont apparus pendant cette période de confinement, certes pas dans toutes les organisations ! Ces carences ont donné lieu à de nouvelles situations et à des compromis avec la sécurité.

## LES MAUVAISES PRATIQUES

Au-delà de la mise en place d'outils<sup>4</sup> empêchant le téléchargement d'applications non autorisées et la connexion à des sites web frauduleux), les processus techniques peuvent ne pas être mis en place ou ne pas être adaptés à une nouvelle situation.

- Pour améliorer la performance, les filtrages VPN sont diminués, ou le « split tunneling<sup>5</sup> » est désactivé.
- Les procédures de patch sur tous les équipements du SI (postes nomades, fixes, tablettes, smartphones, serveurs, équipements réseaux ou de sécurité, logiciels exposés sur Internet, tels que le VPN, le bureau distant, la solution de messagerie) n'ont pas été modifiées. Les VPN sont par ailleurs incapables de transporter de gros volumes de mises à jour.
- Des privilèges ont pu être donnés aux collaborateurs pour installer un VPN par exemple (en cas d'infection par un virus ou malware, un programme malveillant pourra être installé avec des droits étendus et augmentera fortement le risque d'intrusion).
- Le chiffrement et la tokenisation par défaut ne sont pas encore la norme. Selon le « 2020 Data Threat Report » publié par Thales<sup>6</sup>, le multicloud progresse, mais insuffisamment : 57% des données sensibles stockées dans des environnements cloud sont protégées par le chiffrement et 48% le sont par tokenisation.
- Les équipements utilisés ne sont pas configurés correctement ou le wifi domestique n'est pas sécurisé.
- La politique de mots de passe n'est pas assez robuste.
- Les fonctionnalités de sécurité (par exemple sur les outils de visio-conférence : admission dans les « salles de réunion », partage de documents avec les participants, mots de passe, authentification...) ne sont pas connues ou pas respectées.
- Le filtrage applicatif au niveau des pare-feu n'est pas ajusté, ce qui génère des risques de rebond vers les réseaux internes depuis un poste de télétravail.
- La classification des données, la gestion des autorisations (interne et externe !), le contrôle des accès et des flux, la sécurisation des transferts de données ne sont pas toujours en place.
- L'annuaire et le serveur d'authentification dédiés aux télétravailleurs ne sont pas placés en DMZ (zone « démilitarisée » entre Internet et les réseaux internes), ce qui augmente les risques de compromission.
- Des sessions utilisateurs restent trop longtemps inactives et ouvertes (réduire les délais d'expiration automatique).
- L'activité des accès externes, des systèmes sensibles et équipements d'infrastructure (serveurs, pare-feu, proxy...), des API, voire des postes de travail, 'est pas surveillée via un SOC (Security Operation Center), ce qui permettrait de pouvoir détecter les connexions suspectes ou un volume inhabituel de téléchargement d'information. L'état du parc de machines via des outils d'inventaire, les opérations de partage de fichiers, en fonction de leur classification, ne sont pas suffisamment supervisés.
- Les données sont éparpillées, les sauvegardes ne sont pas assurées selon les processus habituels ! Le niveau de sauvegarde des hébergements externes (cloud, site Internet d'entreprise, service de messagerie...) est également à contrôler.

(4) Dispositifs de DLP-Data Loss Prevention, barrières de type CASB-Cloud access security broker, environnements VDI, solutions antivrals complémentaires pour protéger des infrastructures et des terminaux.

(5) Le split tunneling VPN (Virtual Private Network) permet de diriger une partie du trafic à travers un tunnel VPN chiffré, tandis que les autres appareils ou applis conservent un accès direct à Internet.

(6) <https://www.thalesgroup.com/fr/group/journaliste/press-release/securite-du-cloud-moment-charniere-le-rapport-2020-thales-menaces>

### **En conclusion, il faut développer une stratégie pérenne**

Le télétravail a créé des failles qui ont déjà été exploitées ou le seront (il faut donc se préparer à une crise numérique, après cette crise sanitaire !). En conséquence, il exige à la fois :

À court terme, une vigilance accrue lors du retour dans l'entreprise : les postes de travail ont pu être infectés pendant le confinement. Avant de les reconnecter au SI de l'entreprise, il faudra contrôler les postes, auditer les systèmes, faire les mises à jour, changer les mots de passe, effacer les données stockées sur des supports personnels, supprimer des dérogations de sécurité, auditer la sécurité des fournisseurs et sous-traitants critiques !

À moyen terme, le lancement d'un programme qui permettra le développement de ces nouveaux modes de travail de façon pérenne.

À long terme, notamment pour des raisons de développement durable, les entreprises mettront en place des dispositifs qui permettent de limiter les déplacements et de gagner en productivité. Les dirigeants devront mettre en place une stratégie cyber, ce qui implique de comprendre les enjeux et les priorités, basés sur un audit et une cartographie des risques, et de transférer une partie des risques à l'assurance. L'objectif est de trouver le bon équilibre entre les outils et la technologie,

les processus, la gouvernance des données tout en prenant en compte les contraintes juridiques !

### **L'AUTEURE**

**Marie de Freminville est l'auteure de l'ouvrage : « La cybersécurité et les décideurs », publié en 2020 par Isté. Le Prix du « livre cybersécurité 2020 » lui a été décerné par le FIC. Elle est Associée-fondatrice de Starboard Advisory, société de conseil en gouvernance, finance et cyber risques : audits de gouvernance, pilotage de filiales, organisation de conférences et ateliers pour dirigeants et administrateurs sur les bonnes pratiques de gouvernance, la responsabilité numérique des dirigeants et administrateurs, la cartographie des risques cyber, la protection des données, et la conformité RGPD. Elle est diplômée d'HEC, membre de l'IFA (Institut Français des Administrateurs), du bureau HEC Gouvernance et du comité du Cercle Suisse des Administratrices. Elle a été administratrice de filiales d'Airbus Group (EADS Singapour, Airbus Group France et IT services), et de Fonds d'Investissement dans l'Aéronautique, d'une ETI (Construction) et d'une PME de promotion et commercialisation Immobilière.**

# Quelle cybersécurité

collective face aux innovations numériques ?

Par Myriam Quéméner

**L**

La période que nous vivons après le déconfinement est propice à faire le point sur la mobilisation des acteurs pour renforcer la cybersécurité dans un esprit à la fois collectif et collaboratif désormais indispensable. En effet, il apparaît très clairement une montée en puissance des cyberattaques amplifiée par un climat anxigène et d'improvisation numérique qui nécessite une mobilisation sans faille de tous les acteurs, publics et privés. L'exemple du domaine de la e- santé est à cet égard très parlant.



**MYRIAM QUÉMÉNER**

Avocat général  
près la Cour d'appel  
de Paris.  
Docteur en droit

## Le cyberconstat

La crise mondiale, qui a émergé à la suite de la pandémie de COVID-19, a touché tous les secteurs d'activités économiques et humaines de nos sociétés. Durant cette période, la digitalisation a permis à des

secteurs entiers d'assurer la continuité de leur activité. La crise sanitaire liée à la covid 19 a conduit à de nouveaux comportements numériques avec notamment un recours accru au télétravail, souvent développé de façon empirique voire risquée.

En outre, les innovations numériques exploitant massivement les données, allant des cryptoactifs à l'intelligence artificielle,

ne sont souvent pas ou imparfaitement réglementées ce qui n'échappe pas aux cybercriminels<sup>1</sup> tant l'écosystème numérique est disruptif<sup>2</sup>. Si le numérique apparaît plus que jamais incontournable, tant pour le secteur privé que

public, il soulève également de nombreuses interrogations au niveau de la cybersécurité, notamment à l'heure où les données représentent une valeur essentielle pour les entreprises.

(1) M. Quéméner, C. Wierre, F. Dalle, quels droits face aux innovations numériques ? Lextenso 2020.

(2) M. Quéméner, le droit face à la disruption numérique, Lextenso 2018.

(3) L'humain au cœur de la cybersécurité, Revue de la gendarmerie nationale n°266.

<https://www.gendarmerie.interieur.gouv.fr/crgn/publications/revue-de-la-gendarmerie-nationale/revue-n-266>.

(4) Au croisement du conseil en management et du conseil en digital, Wavestone accompagne les grandes entreprises et organisations dans leurs transformations les plus critiques en combinant 3 natures d'expertises différentes : sectorielle, fonctionnelle et technologique. <https://fr.wavestone.com/fr/>

De plus, la masse d'informations et de nouveaux systèmes liés à la transformation numérique s'accompagnent d'attaques qui démontrent un niveau d'expertise de plus en plus élevé. Les cyberattaques se manifestent sous des formes évolutives et il ne s'agit plus de se protéger seulement par des moyens techniques. Il convient également de faire intervenir l'humain<sup>3</sup>, de mobiliser l'ensemble des forces de l'entreprise. Au-delà des conseils d'organisation et de prise en compte de la menace, il s'agit d'impulser

de nouvelles collaborations à tous les niveaux et de vérifier le bon fonctionnement et la solidité de leurs systèmes de sauvegarde, qui pèchent très régulièrement comme le constatent les experts de Wavestone<sup>4</sup> lorsqu'ils interviennent pour aider des entreprises touchées par des cyberattaques.

La défense et la sécurité sont plus que jamais d'actualité dans le contexte mondial de la crise de la COVID-19 et de ses effets économiques et sécuritaires. Les leçons tirées de cette crise renvoient toutes à la question de l'autonomie stratégique, rendant nécessaire l'adaptation de ce qui fonde la sécurité du pays.

### La coopération public/privé à renforcer

Il convient de développer les initiatives associant acteurs publics et privés qui peuvent permettre de mieux accompagner les cybervictimes. Par exemple, on peut citer le dispositif d'assistance aux victimes de cyberattaques cybermalveillance.gouv.fr, incubé par l'Anssi et copiloté avec le ministère de l'Intérieur. La plate-forme a reçu 25 000 demandes en un an, survenant surtout de particuliers, et permis de mobiliser près de 1 600 prestataires référencés pour assister les victimes. Ces partenariats donnent l'occasion à deux cultures différentes, publique et privée, de se rencontrer, de se connaître et d'ap-prendre à travailler ensemble. Ils posent les bases d'une relation de confiance, indispensable à la lutte contre des cybercriminels qui savent profiter des failles des organisations. Cela permet, en outre, à de grands acteurs internationaux de démontrer qu'ils sont prêts à être transparents et à travailler avec les États. C'est un acte indispensable de responsabilité sociale des entreprises en faveur d'une véritable stratégie de cybersécurité.

Face à la nécessité de rassembler toutes les forces et les compétences pour juguler les cyberattaques, les partenariats public/privé apparaissent comme une voie à encourager. L'Agence Nationale de la Sécurité Informatique a mis en place des visas de sécurité, une initiative qui permettent à la fois aux entreprises de disposer de produits et services conformes aux niveaux exigés et aux start-ups de mieux vendre leurs produits aux grands groupes industriels. Parallèlement,



(5) <https://www.ssi.gouv.fr/entreprise/reglementation/cybersecurity-act-2/>

à l'échelle européenne le *Cyber Security Act*<sup>5</sup> devient le cadre législatif qui permettra d'homogénéiser

le niveau de certification des systèmes informatiques au sens large.

L'État est un acteur très important mais les acteurs économiques doivent aussi mutualiser leur savoir-faire en la matière afin de mieux contrer les attaquants qui, par exemple, mettent en commun leurs informations sur les failles à exploiter. Désormais, les acteurs économiques doivent mettre en place des stratégies de défense face aux attaquants.

La coopération « public-privé » en matière de cybersécurité est cruciale et doit être au cœur de toute politique menée à l'échelle de l'Union. C'est l'idée maîtresse qui irrigue et structure l'émergence d'un « État régulateur », via la prise en compte politique et l'organisation progressive du secteur de la cybersécurité au sein de l'Union.

Ce renforcement de la collaboration entre acteurs se réalise aussi au niveau des institutions elles-mêmes, par exemple entre le ministère de la Justice et l'ANSSI,

(6) [https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques\\_par\\_ranconciels\\_tous\\_concernes-v1.0.pdf](https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_ranconciels_tous_concernes-v1.0.pdf)

ainsi qu'en témoigne le guide récent de bonnes pratiques préventives et réactives face aux rançongiciels<sup>6</sup>. Dans ce guide, trois victimes d'un rançongiciel

en 2019, livrent un témoignage éclairant à destination des entreprises et des collectivités.



© DACG – ANSSI

Les enjeux induits par une telle attaque vont bien au-delà de la perte de données ou du paiement d'une rançon. En effet, les organisations victimes doivent faire face à de nombreuses autres conséquences. C'est pourquoi il est recommandé de mettre en place une cellule de crise au plus haut niveau de l'organisation, indépendante des groupes opérationnels de travail qui auront des responsabilités de pilotage et d'exécution. Les attaques par rançongiciels connaissent une augmentation sans précédent.

### L'exemple de l'e-santé

Le champ de la santé est particulièrement concerné par la cybersécurité car les données numériques de ce domaine sont particulièrement sensibles et convoitées par les cybercriminels et le sujet défie les frontières<sup>7</sup>. À cet égard,

(7) <https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services>

(8) [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/2019-11-20\\_Dossier\\_Information\\_Campagne\\_Cybersecurite.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/2019-11-20_Dossier_Information_Campagne_Cybersecurite.pdf)

le ministère des solidarités et de la santé a réalisé une campagne d'information : « santé 2022, un engagement collectif ». Il est souligné que la cybersécurité est une condition préalable et continue de la confiance et de la transformation du système de santé<sup>8</sup>.

Pour se saisir plus rapidement des opportunités et appréhender les risques spécifiques du numérique, la ministre des Solidarités et de la Santé a présenté la feuille de route : « Accélérer le virage numérique en santé », le 25 avril 2019, qui est le résultat d'une convergence de l'ensemble des acteurs de l'écosystème de la e-Santé.

### Cybersécurité collective sur le plan international

Depuis 2017, la multiplication de cyberattaques de grande ampleur et médiatisées, comme Wannacry et NotPetya, ont marqué la nécessité d'un cadre normatif commun dans un nombre croissant de domaines.

L'Europe constitue l'échelon naturel et souhaitable pour promouvoir une vision souveraine de la cybersécurité et exprimer ses valeurs sur la scène internationale. En plaidant pour une approche ambitieuse de la cybersécurité tournée vers l'économie et la société, la France apporte sa pierre à la construction d'un édifice législatif en matière de cybersécurité et développe une politique d'échange au sein de l'écosystème numérique. La cybersécurité est un sujet par es-

sence international qui devrait aussi être évoqué dans le cadre du G7.

(9) <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/actualites-et-evenements-lies-a-la-cybersecurite/article/troisieme-dialogue-strate>

Le troisième dialogue stratégique « France-États-Unis » en matière de cybersécurité<sup>9</sup> s'est tenu à Paris le 2 janvier 2020. Ces deux puissances ont évoqué les discussions et les projets portés à l'ONU dans les enceintes multilatérales relatives à la paix et à la sécurité dans le cyberspace,

les initiatives multi-acteurs, notamment l'Appel de Paris, ainsi que les enjeux de souveraineté numérique.

Par le biais de l'European Union Agency for Cybersecurity (ENISA), l'Union prône un cyberspace de « *libertés, commun et ouvert* ». Ces valeurs sont partagées par Paris, qui, au travers de l'ANSSI, a appelé, en janvier 2020, à l'approfondissement de la souveraineté européenne dans le domaine cybernétique. Les enjeux liés au domaine cyber conduisent à agir sur plusieurs fronts simultanément : l'Europe et l'international. Cet engagement, tous azimuts, est visible également dans nombre d'institutions au sein desquelles le pays s'investit. Par exemple, les délégations françaises ont été les premières à s'être rendues au Centre d'Excellence de Cyberdéfense Coopérative de l'OTAN depuis le début de la pandémie. La France voit également en l'OSCE une instance tout à fait apte à accompagner le développement normatif en matière cyber.

# L'Internet des objets

## à l'épreuve de la criminalistique numérique

Par François Bouchaud

**L**

La criminalistique numérique a été popularisée avec le développement et la diffusion des séries télévisées telles que NCIS ou « Les experts ». À ses débuts, elle résulte de demandes opérationnelles des Forces de Sécurité Intérieure (FSI), dans le cadre d'une enquête sur un crime impliquant l'appropriation du système informatique, généralement un ordinateur personnel, un téléphone portable ou un

serveur. Cependant, les enquêtes médico-légales numériques ne se limitent pas aux affaires de cybercriminalité telles que l'accès ou sa tentative non autorisés à un système de traitement automatisé de données ou la diffusion de contenus d'exploitation sexuelle de mineurs. De plus en plus, elles sont

également présentes dans des activités criminelles impliquant l'utilisation d'un appareil informatique ou numérique, comme dans les cas de trafic ou de blanchiment d'argent dans lesquels l'appareil numérique constitue le vecteur de l'infraction.

À cette diversification du périmètre infractionnel et des usages s'ajoutent de nouveaux défis techniques. Le développement des écosystèmes connectés à Internet confronte la médecine légale à des dispositifs et des environnements hétérogènes, étendus et interconnectés avec de fortes dépendances. La donnée probante se retrouve fragmentée et dispersée au gré de la politique de gestion de la donnée, tant au niveau du stockage que de la synchronisation dans le réseau. Cette structuration de l'espace numérique et physique constitue donc un tournant dans l'analyse et la compréhension des phénomènes, nécessitant une contextualisation de la donnée et de sa diffusion.



**FRANÇOIS BOUCHAUD**

Capitaine de Gendarmerie. Chef du département coordination du Centre de lutte contre les criminalités numériques (C3N).

Cependant, elle est gage d'opportunités inédites dans le recueil de données probantes par son fort ancrage dans l'environnement de l'utilisateur, tant dans la digitalisation de ses habitudes que dans le monitoring des systèmes.

### 1- Présentation d'une scène de crime connectée

Classiquement, les matériels étudiés sont des ordinateurs, des appareils mobiles, des passerelles, des équipements de stockage ou des serveurs. L'Internet des objets ouvre de nouvelles perspectives en introduisant des sources qui diffèrent par leur nature, leur nombre, leur format et les protocoles utilisés. Ainsi, les données pro-

bantes sont extraites ou proviennent des appareils ménagers, de systèmes domotiques, des équipements médicaux pour le vivant « homme ou animal », des voitures, des lecteurs RFID, *etc.* Par conséquence, les données sont plurielles et varient en fonction des interactions avec l'environnement et des services fournis. Pour illustrer ces propos et répondre aux multiples défis que génère la criminalistique dans l'Internet des objets, nous vous proposons d'étudier une scène de crime contenant des dispositifs intelligents et communicants.

Le 10 avril 2018, à 8 heures, le CORG<sup>1</sup> est alerté pour le cambriolage d'un

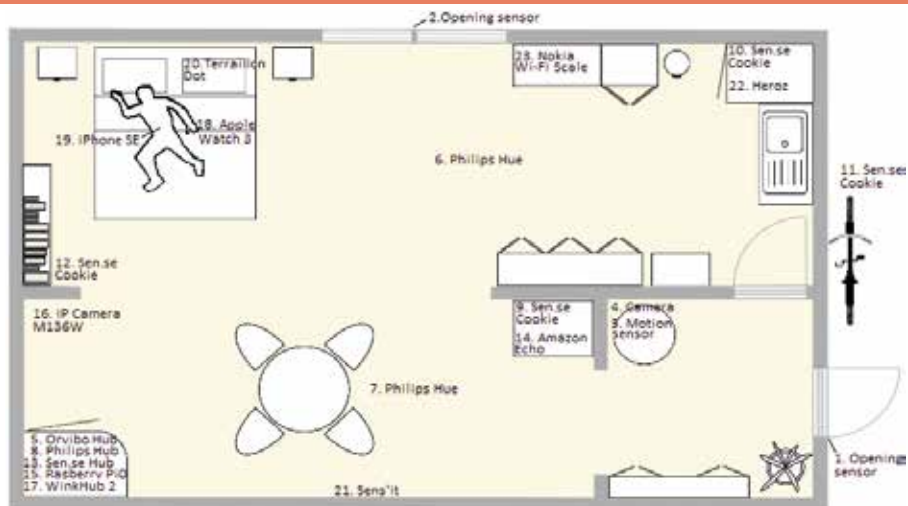


Figure 1 : croquis de l'appartement avec les équipements connectés.

(1) Centre d'opérations et de renseignement de la gendarmerie, niveau départemental.

appartement. Une patrouille de gendarmerie arrive à 8h15 sur le lieu des faits. Lors de la reconnaissance, elle

découvre la porte d'entrée de l'appartement fracturée. Les premières constatations font ressortir de nombreuses traces de lutte et de violence avec des objets renversés et brisés sur le sol. Dans une pièce, une personne décédée est retrouvée gisant sur un lit. La patrouille met donc en œuvre les premières mesures de protection de la scène de crime et demande un appui auprès des unités compétentes. Une équipe médico-légale, dont un technicien en nouvelles technologies, prend en charge la scène de crime à 9 heures. Il procède à l'appréhension de l'environnement en identifiant les différents objets connectés (figure 1) et en traçant la cartographie des interactions (figure 2).

L'appartement s'étend sur une surface de 45 m<sup>2</sup>. Il comprend trois pièces distinctes : une entrée (pièce 1), une chambre (pièce 2) et un salon (pièce 3). Il est équipé d'un système domotique issu d'un kit *Orvibo*, avec deux capteurs d'ouverture (1 et 2) et un capteur de mouvement (3) couplé à une caméra Wi-Fi (4). Cette solution contrôle les deux ouvertures extérieures. Elle communique par le protocole *ZigBee* au travers d'une passerelle dédiée (5). Le système domotique est complété d'une ampoule Philips (6 et 7) connectée à sa passerelle (8). Par ailleurs, quatre capteurs *Sen.se Cookies* sont cachés dans les différentes pièces. Ils transforment les objets ménagers en objets connectés. Dans cette situation, ils surveillent la température ambiante de l'appartement (9), le niveau d'eau de la machine à café (10), la position du vélo en extérieur (11) et la gestion de la bibliothèque (12).

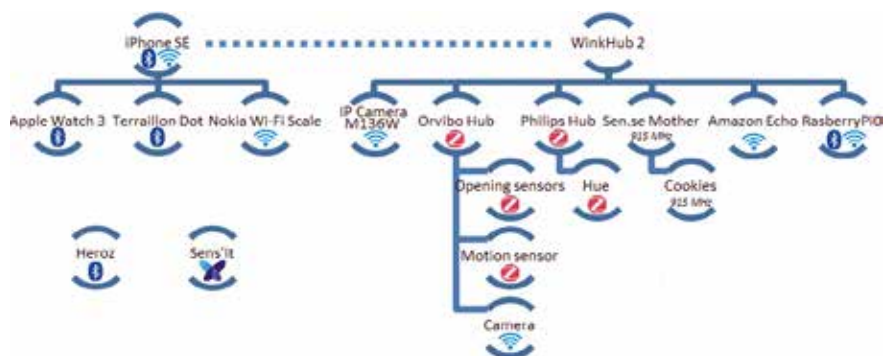


Figure 2 : cartographie globale de l'environnement local [1].

Tous ces équipements sont reliés à une base centrale *Sen.se Mother* et communiquent avec un protocole propriétaire (13). Les différentes passerelles *Orvibo*, *Philips et Sen.se*, l'*Amazon Echo* (14), le *RaspberryPi0* (15) et la caméra IP M136W (16) sont connectées à Internet au travers d'un *WinkHub 2* (17).

La victime est allongée sur le lit de la chambre. Elle porte à son poignet droit une *Apple Watch 3* (18) et a un *iPhone SE* (19) dans sa poche. Un capteur de sommeil *Terraillon Dot* (20) est caché dans le lit. D'autres objets hétéroclites sont disposés dans l'appartement : un *Sens'it* (21), un bracelet *Heroz* (22) et une balance *Nokia* (23).

## 2- Appréhension de l'environnement connecté dans sa globalité

Dans une démarche analytique de l'environnement, l'écosystème se découpe en trois zones complémentaires (figure 3) [2] : un environnement local composé des objets connectés et des passerelles (1), une infrastructure externalisée construite autour de plateformes Cloud (2) et un interfaçage avec l'utilisateur ou avec un autre système connecté (3). L'appréhension de la scène de crime se focalise sur l'environnement local, soit les zones 1 et 3. Seules les données de ces zones demeurent directement accessibles aux enquêteurs. L'acquisition des données de la zone 2 nécessite l'intervention d'un tiers, initiée par une réquisition judiciaire. Cependant, les demandes auprès des opérateurs de plateforme doivent

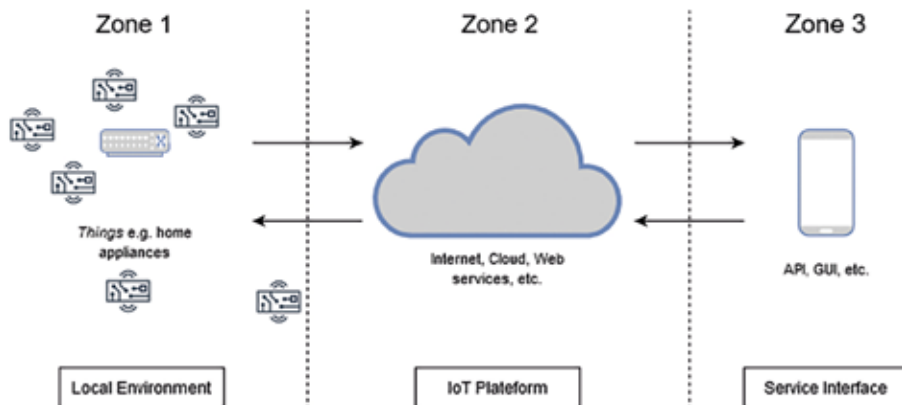


Figure 3 : découpage par zones de l'environnement connecté.

être orientées et motivées en fonction des informations recueillies localement, en particulier dans l'identification de l'équipement et des données remontées.

Chaque infrastructure est caractérisée par une politique de gestion de la donnée unique. Par exemple, le *Terraillon Dot* est synchronisé manuellement alors que l'*Apple Watch* utilise une synchronisation automatique. De même, la caméra *Orvibo* utilise un stockage externe comme mémoire tampon dans la communication avec le réseau. La donnée remontée se retrouve alors dispersée au sein du réseau au gré des configurations et des services proposés. Un équipement est susceptible d'être contrôlé ou accessible à partir d'un autre appareil du système, selon une structure de lien caché. La donnée se propage dans les équipements du réseau, concourant ou non à l'objet cible [3]. Cette problématique soulève plusieurs questions pour la criminalistique moderne sur le partage et le recoupement des informations afin de reconstituer la chronologie des événements. Elle met à mal une approche statique et unitaire des éléments de la scène de crime, en s'inscrivant dans une approche plus globale de la chose.

### 3- Exploitation et analyse des données recueillies

La littérature scientifique est riche de nombreux travaux dans l'étude des solutions connectées et de leurs artefacts, que ce soit au travers des montres, des

bracelets connectés [4], des assistants vocaux [5] et plus globalement de tout dispositif connecté de la vie quotidienne [6]. Cependant, les traces obtenues résident en de nombreux fragments contenus dans une pluralité de supports d'un même réseau, susceptibles d'évoluer à travers le temps et l'espace. Afin qu'elle ne soit pas parcellaire, l'analyse ne doit pas se focaliser sur l'étude d'un unique objet mais sur l'infrastructure connectée dans son intégralité. Elle consiste donc à étudier la donnée selon trois axes : **le temps** en définissant la chronologie des événements et des phénomènes itératifs, **l'espace** en positionnant la donnée dans l'infrastructure et au regard de l'environnement local et **le contexte** de l'évènement au regard des rôles et des actions des équipements face au phénomène. Par cette approche ternaire, l'enquêteur cherche à déterminer le cycle de vie de la donnée retrouvée, afin de la qualifier, et établir sa cohérence. Dans le but de procéder à une analyse pertinente des événements, il est nécessaire d'étudier l'information au regard d'un horodatage commun, défini à partir des caractéristiques techniques des appareils étudiés.

Par exemple, en étudiant les journaux d'événements contenus dans la passerelle et l'application *Philips*, l'évènement «lampe allumée» est horodaté. Cependant, il doit être caractérisé plus précisément. S'agit-il d'une action de l'utilisateur par le biais de l'application téléphonique, d'un interrupteur

externe, du signal d'un capteur ou d'une commande vocale au travers de l'*Amazon Echo* ? A-t-elle été effectuée par un utilisateur connu ? S'agit-il d'une action programmée ? Pour chaque question, une donnée unique est associée. Cette approche analytique est généralisable à tous les objets de l'infrastructure connectée. Ces informations déterminent les acteurs étant intervenus sur et dans l'événement, leurs positions en fonction des objets, les actions effectuées ou détectées et la réponse des objets aux différentes sollicitations.

Ainsi, les équipements regroupent des données de contexte (une configuration physique et logique d'un lieu, une habitude de vie, un enregistrement sonore ou vidéo, *etc.*) et des données à caractère personnel (une identité du consommateur de service, des informations numériques et de biométrie, *etc.*). Ces informations offrent aux enquêteurs la possibilité de reconstituer la succession des événements avant et après l'incident. Ainsi, à partir des premiers éléments numériques, l'enquêteur est en mesure de dater l'intrusion dans le domicile de la victime avec le capteur de la porte d'entrée, le parcours du mis en cause avec le système domotique *Orvibo* corroboré par le mouvement du *Sen.se Cookie* (9), ainsi que l'heure du décès de la victime. Il peut constater l'absence de modification de la scène de crime comme un déplacement du corps de la victime post-mortem, émettre des

hypothèses sur le lieu du meurtre et les circonstances. Ces informations doivent être mises en perspective avec les données médico-légales recueillies sur la scène de crime et sur la victime. Par ailleurs, les données numériques sont en mesure d'orienter certaines investigations comme des relevés de traces biologiques sur la scène de crime en fonction du parcours criminel du mis en cause. Sur une habitation de plus grande taille, ces informations aident à délimiter et à discriminer une zone d'étude en définissant une stratégie d'investigation en cohérence avec les données relevées. Les objets connectés donnent la possibilité de vérifier des hypothèses de travail en apportant de nouveaux éléments matériels, comme par exemple un mobile incohérent avec un mode opératoire. L'étude de la chronologie des événements peut également renseigner sur une éventuelle préméditation dans la logique criminelle.



| Date                | Description                                                                                                                                               | Source locale                                                                                         | Faits                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| T0                  | Lampes Philips Hue éteintes (6 et 7)<br>Porte et fenêtre fermées (1 et 2)<br>Etat repos : activité cardiaque de l'Apple Watch (18) et Terraillon Dot (20) | Hub Philips Hue, Hub Orvibo, iPhone (Backup Apple Watch et applications domotiques) et Terraillon Dot | Présence d'une personne en pièce 2 (connue) et aucun mouvement détecté.                                                     |
| 10/04/2020 06:43:17 | Ouverture de porte détectée (1)                                                                                                                           | Hub Orvibo et iPhone (Application domotique)                                                          | Présence d'une personne en pièce 2 (connue) et d'une personne en pièce 1 (non reconnue). Mouvements en pièce 1.             |
| 10/04/2020 06:44:03 | Détection du mouvement (3)                                                                                                                                |                                                                                                       |                                                                                                                             |
| 10/04/2020 06:44:12 | Lancement de la Camera Orvibo (4)                                                                                                                         | Camera Orvibo (carte SD), Hub Philips Hue et iPhone (Application domotique)                           | Présence d'une personne en pièce 2 (connue) et d'une personne en pièce 3 (non reconnue). Mouvements en pièce 3.             |
| 10/04/2020 06:52:46 | Déplacement Sen.se Cookie (9)                                                                                                                             | Sen.se Mother et iPhone (Application Sen.se)                                                          |                                                                                                                             |
| 10/04/2020 06:54:16 | Déclenchement IP Camera M136W                                                                                                                             | iPhone (Application IP Camera)                                                                        |                                                                                                                             |
| 10/04/2020 06:57:11 | Mesure d'un mouvement Terraillon Dot (20)                                                                                                                 | Terraillon Dot                                                                                        |                                                                                                                             |
| 10/04/2020 07:01:04 | Mesure d'une accélération du rythme cardiaque Apple Watch (18)                                                                                            | iPhone (Backup Apple Watch)                                                                           |                                                                                                                             |
| 10/04/2020 07:03:39 | Allumage de la Philips Hue (6) déclenchement à partir du téléphone portable iPhone SE                                                                     | Hub Philips Hue et iPhone (Application domotique)                                                     | Présence d'une personne en pièce 2 (connue).                                                                                |
| 10/04/2020 07:07:01 | Mesure de l'arrêt cardiaque (8)                                                                                                                           | iPhone (Backup Apple Watch)                                                                           |                                                                                                                             |
| 10/04/2020 07:07:54 | Fin de la mesure du mouvement Terraillon Dot (20)                                                                                                         | Terraillon Dot                                                                                        |                                                                                                                             |
| 10/04/2020 07:11:44 | Détection du mouvement (3)                                                                                                                                | Hub Orvibo et iPhone (Application domotique)                                                          | Présence d'une personne en pièce 2 (connue) et d'une personne en pièce 3 puis 1 (non reconnue). Mouvements en pièce 3 et 1. |
| 10/04/2020 08:17:21 | Détection du mouvement (3) : arrivée de la patrouille                                                                                                     |                                                                                                       |                                                                                                                             |
| 10/04/2020 08:24:56 | Détection du mouvement (3)                                                                                                                                |                                                                                                       |                                                                                                                             |
| 10/04/2020 09:12:00 | Détection du mouvement (3) : arrivée enquêteur en nouvelles technologies                                                                                  |                                                                                                       |                                                                                                                             |
| T1                  | Lampes Philips Hue allumée (6) éteinte (7)<br>Porte ouverte (1) et fenêtre fermée (2)                                                                     | Hub Philips Hue, Hub Orvibo et iPhone (Backup Apple Watch et applications domotiques)                 |                                                                                                                             |

#### 4- En Bref...

L'Internet des objets contribue à l'apport subséquent d'éléments de preuves confortant un procès au pénal. Il s'avère, dans certains cas, que cette structuration étendue de l'environnement connecté peut présenter des difficultés en termes de réponse criminalistique. Les traces sont dispersées localement ou également au travers des ramifications de l'infrastructure et des espaces de traitement en ligne. Ainsi, la donnée est susceptible d'être partielle dans l'objet connecté mais devient un ensemble cohérent dans l'arborescence numérique. Cette détermination de la présence et du positionnement de l'information demeure unique à chaque écosystème. Elle est en particulier liée à la politique de la gestion de la donnée, tant au niveau du stockage que de sa synchronisation au travers du réseau. L'analyse des traces est donc beaucoup plus complexe que dans le cadre de la criminalistique numérique traditionnelle, en raison de son caractère multidimensionnel et pluridisciplinaire. Elle s'accompagne également d'un travail de contextualisation de la donnée et de compréhension de sa diffusion, selon les facteurs espace et temps. Identifier et comprendre les sources précieuses de traces est donc un défi majeur. L'ensemble de l'enquête dépend de la nature de l'appareil connecté et de l'intelligence mise en place pour sa gestion.

#### Références bibliographiques :

- [1] Bouchaud, F., Vantrois, T., Grimaud, G.: Evidence gathering in IoT criminal investigation. In: 11th EAI International Conference on Digital

Forensics and Cyber Crime. Springer (Oct 2020).

- [2] Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P.: Internet of things forensics: Challenges and approaches. In: 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. IEEE (Oct 2013).
- [3] Attwood, A., Merabti, M., Fergus, P., Abuelmaat-ti, O.: SCCIR: Smart cities critical infrastructure response framework. In 2011 Developments in E-systems Engineering. IEEE (Dec 2011).
- [4] Baggili, I., Oduro, J., Anthony, K., Breiting, F., McGee, G.: Watch what you wear: preliminary forensic analysis of smart watches. In 2015 10th International Conference on Availability, Reliability and Security. IEEE (2015, August).
- [5] Chung H, Park J, Lee S.: Digital forensic approaches for Amazon Alexa ecosystem. Digital Investigation (Aug 2017).
- [6] Bharadwaj, N. K., Singh, U.: Acquisition and analysis of forensic artifacts from Raspberry Pi an Internet of Things prototype platform. In Recent Findings in Intelligent Computing Techniques. Springer (Nov 2019).

#### L'AUTEUR

**Officier de la Gendarmerie nationale, le Capitaine François Bouchaud dirige le département coordination du Centre de lutte contre les criminalités numériques (C3N). Doctorant en informatique à l'Institut de recherche sur les composants logiciels et matériels pour l'informatique et la communication avancée, il est diplômé de l'École supérieure d'électronique de l'Ouest et de l'École centrale Paris.**

# Cybermenaces :

## la transition numérique de la police

Par **Olivier Ribaux** et **Thomas Souvignet**

L

(1) <https://third.digital/>

**NDLR** : cet article a été initialement publié dans la revue *Third*<sup>1</sup> en novembre 2020.

Les transformations numériques de nos activités quotidiennes se sont inévitablement accompagnées d'une évolution de la criminalité et des menaces qui pèsent sur la société. Les cybermalveillances sont devenues quasi banales et nous



**OLIVIER RIBAU**

Directeur de l'École des Sciences Criminelles de l'Université de Lausanne, Suisse.



**THOMAS SOUVIGNET**

Lieutenant-colonel de Gendarmerie (En disponibilité). Professeur à l'École des Sciences Criminelles de l'Université de Lausanne, Suisse.

ne prêtons même plus attention aux tentatives d'hameçonnage qui pullulent dans nos boîtes de « spam » (pourriels).

Il devient alors indispensable de se demander comment les victimes ressentent ces attaques et y réagissent, et comment les pratiques policières évoluent pour s'adapter à ces transformations. Nous exprimerons ces enjeux et présenterons des développements opérationnels en illustrant nos propos par une fraude en ligne, typique, dont notre École a été la cible.

### L'omniprésence des crimes numériques

Les transformations numériques de notre société engendrent toute sorte de nouveaux dangers qui perturbent concrètement notre quotidien. Ils sont mis en évidence dans l'étude menée en juin 2019 par l'Institut National de la Consommation pour Cybermalveillance.gouv.fr<sup>2</sup>, le dispositif français d'assistance aux victimes, de prévention des

(2) <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/plus-de-9-francais-sur-10-ont-deja-ete-confrontes-a-un-acte-de-cybermalveillance>.

(3) <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/chiffres-et-tendances-des-cybermenaces-cybermalveillance-gouv-fr-de-voile-son-premier-rapport-dacti-vite-2019>.

risques numériques et d'observation de la menace en France : plus de 9 français sur 10 admettent avoir déjà été confrontés à un acte de malveillance sur Internet.

Le nombre et la variété des événements pour lesquels ce même organisme est sollicité<sup>3</sup> (Figure 1), indiquent le polymorphisme de ces dangers.

### Répartition des menaces par types de publics

Recherches d'assistance / particuliers

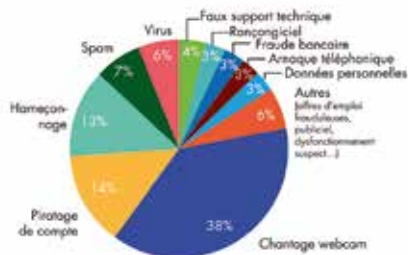


Figure 1 - Répartition des menaces lors des recherches d'assistance provenant de particuliers (source : [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)).

Ces formes omniprésentes de criminalité en ligne, confirmées par d'autres entités comme l'association Signal Spam (Figure

2), sont souvent faussement considérées comme banales et bénignes. Elles sont néanmoins susceptibles de causer des dommages financiers et psychologiques parfois dramatiques pour les victimes.

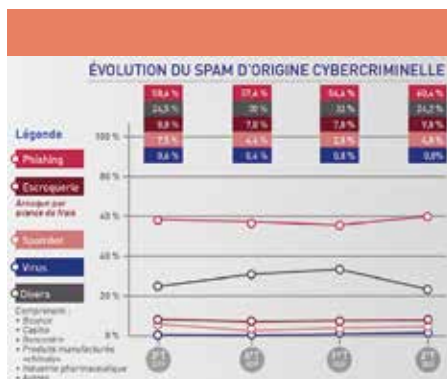


Figure 2 - Évolution du spam d'origine cybercriminelle entre 3ème trimestre 2019 et 2e trimestre 2020 (source : [www.signal-spam.fr](http://www.signal-spam.fr)).

(4) <https://www.europol.europa.eu/activites-services/main-reports/internet>

Dans son évaluation annuelle du paysage des cybermenaces pour l'année 2019 (IOCTA 2019<sup>4</sup>), Europol met notamment en avant les formes plus organisées et graves, telles que l'exploitation sexuelle de mineur en ligne, la fraude aux paiements, l'atteinte aux systèmes numériques (ransomiciel, compromission de données, etc.) ou encore les espaces numériques sur lesquels s'appuient des activités terroristes.

Nombre de ces cybermenaces ont toutefois un angle d'attaque commun :

les vulnérabilités de l'humain. En effet, une action et une inattention de l'utilisateur sont très souvent nécessaires pour qu'une attaque puisse avoir l'effet escompté.

### Au-delà des chiffres, comment réagir ?

Les réponses apportées jusqu'ici résultent d'une multitude d'initiatives souvent prometteuses, mais encore très fragmentées. Elles se confrontent à de nouvelles questions : qui doit prendre en charge les problèmes (institutions privées, publiques, responsabilité individuelle), quand (modes d'intervention) et comment (quelle représentation ? quelles méthodes de prévention ?). Les questions éthiques (par ex. les libertés individuelles), comme le reste, doivent s'envisager à une nouvelle échelle.

Une attaque dont notre École a été victime durant l'été 2019, permet d'illustrer une partie de ces difficultés.

(5) <https://www.sciencedirect.com/science/article>

Nous prenons conscience qu'une attaque (détaillée dans un article publié dans

*Forensic Science International : Digital Investigation*) par harponnage (ou *spear phishing*) est en cours lorsque le premier auteur de cet article (professeur spécialisé en criminalistique numérique) reçoit, sur son adresse professionnelle, un courriel de son directeur (deuxième auteur de cet article) dont le sujet est « Hello are you available? ». Le tout est envoyé d'une adresse Gmail et non de celle de l'université. Tous deux sur nos lieux de vacances,

nous arrivons toutefois à nous contacter et débute alors une gestion commune de l'incident.

Professionnels avertis en la matière, nous comprenons rapidement qu'il s'agit d'une usurpation d'identité (faux directeur) visant à demander de l'argent aux destinataires des courriels. Nous devons découvrir quels sont les destinataires de ceux-ci. Deux hypothèses se dessinent rapidement : soit le carnet d'adresse du Directeur a été piraté, soit l'attaquant a récupéré une liste de cibles de choix en exploitant des données publiées par exemple par le site web institutionnel de l'École.

Le mode opératoire étant défini, vient ensuite l'étape visant à endiguer l'attaque et, de manière pragmatique, éviter tout paiement. Nous comprenons que la fraude est synchrone (l'auteur dialogue en temps réel avec les personnes contactées). Notre réaction doit être immédiate.

Les messages étant envoyé d'une adresse Gmail créée par l'attaquant, la première idée consiste à s'appuyer sur Google. Un formulaire disponible sur le site support de Google semble pouvoir répondre au besoin. Mais, en restant réaliste, nous comprenons que le temps de réaction du géant américain n'est pas compatible avec l'évolution de la fraude.

L'identification des destinataires n'étant toujours pas possible, le directeur prend la décision :

- d'envoyer un courriel à l'ensemble des collaborateurs de l'École,
- d'informer le support informatique de l'université,
- de prendre contact individuellement avec quelques adresses de sa propre liste de contacts, en dehors de l'École, pour tester l'hypothèse du piratage de son compte.

Enfin, le directeur contacte officiellement quelques responsables de la police locale, spécialisés en numérique, afin de connaître la démarche à suivre.

Les actions menées ont eu l'effet escompté puisque certains collaborateurs en discussion avec l'attaquant ont stoppé net à réception du courriel adressé aux collaborateurs de l'École. De même, le service informatique de l'université a été en mesure d'intercepter immédiatement le flux continu de messages provenant de l'attaquant. Par les retours obtenus des collaborateurs et les réponses des contacts hors de l'université, il apparaît maintenant clairement que le cercle des personnes ciblées se restreint aux membres de l'École.

Dans une seconde phase d'analyse à froid, cette hypothèse a été confirmée par l'examen des journaux d'événement (logs) du site internet de l'École : des accès aux adresses électroniques des collaborateurs par le site internet

étaient synchronisés avec l'émission des courriels d'harponnage.

Finalement, seule une cible sur une centaine ira jusqu'à la phase de paiement, mais ce paiement sera annulé à la dernière minute.

Dans cette situation assez simple, de nombreuses décisions et démarches, à des niveaux différents ont été nécessaires pour endiguer la fraude.

Ces démarches, pas forcément simples ou accessibles, même pour des utilisateurs avertis, montrent la difficulté de faire face à une attaque technologiquement simple. On peut aisément imaginer la grande difficulté d'une victime âgée face à un rançongiciel (eg. *cryptolocker*) ou une prise en main à distance lors d'une fraude au faux support technique.

### Une évolution nécessaire de la réponse policière

Cet exemple met en exergue un paradoxe quant à la manière dont la Police aborde la criminalité sur Internet et aux attentes que nous avons à l'égard de cette institution.

En effet, si nous n'avions pas été victime d'une attaque en ligne mais d'une rixe ou d'un cambriolage, nous aurions immédiatement appelé la Police et lui aurions laissé entièrement gérer la crise engendrée. Dans son rôle régalien, celle-ci aurait sans doute réalisé des opérations de police

technique et scientifique, effectué une enquête de voisinage et saisi les images de vidéoprotection disponibles. Quand bien même nous enseignons à nos étudiants ces pratiques, nous aurions entièrement « confié » ces opérations à la Police.

Dès lors, pourquoi n'avons-nous pas agi de la même manière avec cette cyberattaque dont nous avons été victimes ? Parce que nous n'avions pas « confiance » en la réponse que pourrait apporter

la Police dans un délai aussi court. Même dans un contexte de confiance Police-Nation aussi fort qu'en Suisse, où la Police est régulièrement sollicitée pour des renseignements de toutes natures, nous considérons tacitement qu'elle n'aurait pas les ressources pour traiter immédiatement notre petite attaque. N'aurait-elle pas agi immédiatement si l'on tentait de s'en prendre à nos biens dans le monde physique ?

England and Wales, year ending December 1981 to year ending March 2020



Source: Office for National Statistics – Crime Survey for England and Wales

Figure 3 – Estimation de la délinquance en Angleterre et Pays de Galle (source : Office nationale de la statistique du Royaume-Uni).

Cela pose ainsi la nécessité et la capacité des forces de l'ordre à traiter individuellement toutes les cyberattaques.

Une enquête doit-elle et peut-elle être menée dès la réception d'une tentative d'hameçonnage ? Si ce n'est pas le cas, à partir de quel niveau d'intensité une réponse policière doit-elle être apportée ?

Pour comprendre l'éventuelle difficulté à faire face à ces cyberattaques, il suffit de consulter les statistiques de la délinquance de l'Angleterre et du Pays de Galles (Figure 3). En effet, la prise en compte des crimes et délits liés au numérique depuis 2007 a pour effet de quasiment doubler la délinquance estimée.

(6) <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearending-march2020>.

(7) <https://www.gov.uk/government/collections/police-workforce-england-and-wales>

(8) <https://online-library.wiley.com/doi/abs/10.1111/1556-4029.13849>.

Au vu de la criminalité dans les années 1990-2000, on pourrait se dire, qu'à effectif du même ordre de grandeur<sup>7</sup>, la moitié serait dédiée à cette nouvelle délinquance et qu'une réponse à la hauteur de la criminalité traditionnelle serait produite. Ceci n'est bien sûr pas le cas.

Dès lors, les polices sont-elles atteintes du « syndrome Kodak » qui semble frap-

per les laboratoires forensiques<sup>8</sup> ?

En d'autres termes, est-ce que les forces de police ont su prendre le virage numérique, adapter leurs pratiques aux cybermenaces ? Faute de prendre en compte ces nouvelles menaces, et campant sur des pratiques du siècle dernier, ne risquent-elles pas, à l'image de Kodak qui misait tout sur la vente de pellicules, de ne pas se remettre de ces évolutions numériques ?

Tout d'abord, il est possible d'argumenter à ceux qui voient un « syndrome Kodak » dans l'adaptation des forces de police aux cybermenaces, qu'un « syndrome Polaroid » peut également être mis en avant. En effet, même avec l'avènement du numérique les pratiques traditionnelles restent d'actualité. Le succès du Polaroid ne se dément pas, comme celui de la criminalité traditionnelle.

(9) Technicien en Identification Criminelle – TIC – en Gendarmerie et Agent spécialisé de Police Technique et Scientifique – ASPTS – en Police.

(10) Enquêteur spécialisé en technologie numérique – NTech – en Gendarmerie et Investigateurs en cybercriminalité – ICC – en Police.

Ensuite, les forces de l'ordre s'attachent à réaliser leurs transformations numériques. En France, dès la fin du XX<sup>e</sup> siècle, les spécialistes en scène de crime<sup>9</sup> ont été rejoints par des spécialistes en analyse de supports et en enquêtes numériques<sup>10</sup>.



(11) <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte>

Depuis 2009<sup>11</sup>, la Plateforme d'Harmonisation, d'Analyse, de Recoupement

et d'Orientation des Signalements (PHAROS) a quant-à-elle pour mission de recueillir, de manière centralisée, l'ensemble des signalements de nombreux faits commis en ligne, dont les escroqueries et arnaques financières utilisant internet. Enfin des unités spécialisées détiennent les compétences techniques nécessaires

(12) <https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe>

à la lutte contre les fraudes mettant en œuvre des technologies évoluées, comme le montre le démantèlement d'un réseau de *Darkphone* (téléphones hautement sécurisés utilisés

par des groupes criminels) par la Gendarmerie Nationale<sup>12</sup>.

Reste tout de même la prise en compte de l'utilisateur qui doit faire face à une cyberattaque, telle que nous l'avons vécue. Là encore, les agences gouvernementales françaises prennent en compte le virage numérique avec esprit d'innovation.

La Gendarmerie a ouvert une brigade en ligne, accessible 24h/24 en créant la « brigade numérique ». La coproduction de sécurité est ainsi régulièrement

utilisée dans les mécanismes mis en place. Nous noterons ainsi la participation des forces de l'ordre dans des associations de lutte contre la criminalité numérique (Signal Spam, CECyF, etc.) ou encore la création de Groupes d'Intérêt Public (GIP) comme le GIP Action contre la Cybermalveillance (GIP ACYMA) derrière « [cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) » préalablement cité.

### Une marge de manœuvre encore grande

Malgré cette prise en compte des nouvelles menaces portées par le numérique et la transformation de leurs pratiques, les forces de Police ont quand même du chemin à parcourir pour prendre en compte la criminalité numérique comme elles prennent en compte la criminalité traditionnelle. En dehors d'une meilleure prise en charge des victimes, l'exploitation systématique du renseignement judiciaire pourrait être un moyen efficace de rattraper ce retard. C'est du moins ce qu'essaie de faire la Suisse en développant la Plateforme d'Information de la Criminalité Sérielle en Ligne (PICSEL). Cette plateforme exige déjà des policiers qui saisissent les plaintes et qui alimentent le dispositif, une attention particulière à ces formes de criminalité jusqu'ici ignorées. Ils doivent s'entretenir avec le plaignant et s'appuyer

sur les brigades spécialisées pour exprimer clairement le mode opératoire et en identifier des traits pertinents. Les traces accessibles sont aussi susceptibles d'aider à détecter des problèmes répétitifs et à suivre leur évolution. L'analyse des informations, ainsi réunies et organisées, offre les moyens d'adapter les stratégies préventives et répressives, de mieux communiquer avec les partenaires et avec le public, de prioriser les efforts et d'orienter les enquêtes. En moins de deux ans de fonctionnement et bien qu'en état encore embryonnaire, ces nouveaux processus ont déjà modifié profondément l'approche policière des crimes transformés numériquement.

## L'AUTEUR

**Lieutenant-Colonel de gendarmerie en position de disponibilité, Thomas Souvignet est professeur spécialisé en traces numériques à l'École des Sciences Criminelles de l'Université de Lausanne. Titulaire de différents masters (Sécurité des Systèmes d'Information — Information Security and Computer Crime — Systèmes embarqués et mobiles), il détient un doctorat en Informatique (sujet relatif à la lutte contre la fraude aux moyens de paiement). Après avoir œuvré au développement du département informatique-électronique de l'IRCGN pendant une douzaine d'années, il se consacre actuellement à élargir la recherche, l'expertise et l'enseignement du numérique au sein de la plus ancienne école de police scientifique au monde.**

# Critères Communs, CSPN

et Qualification, pour une confiance objective dans un produit de sécurité

Par Gérard Peliks

# L

La confiance en un produit de cybersécurité ne se décrète pas. Si on parle de confiance objective, elle s'obtient en faisant certifier ou qualifier le produit. Des standards et des normes existent et sont élaborés par une coopération entre pays comme les standards ITSEC pour l'Europe et les Critères Communs pour l'international.



**GÉRARD PELIKS**

Association des Réservistes du Chiffre et de la Sécurité de l'Information. Réserve citoyenne cyberdéfense. Gendarmerie nationale.

De l'Orange Book à la qualification, en passant par l'ITSEC, les Critères Communs et la CSPN, cet article explore ces différentes préconisations.

**Vers une confiance objective et internationale pour un produit de cybersécurité**

Les solutions de sécurité, comme les pare-feux,

les Réseaux Privés Virtuels (VPN), les antimalwares, l'authentification forte, le chiffrement, concourent à diminuer les risques, les effets des cyberattaques et à réduire l'incertitude sur la qualité des produits. Elles augmentent ainsi la confiance que les utilisateurs peuvent éprouver vis-à-vis de leur système d'information. Elles peuvent garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des process et des data, surtout quand celles-ci sont sensibles. Cependant, le problème des logiciels de sécurité est que ce sont des logiciels ou des solutions qui reposent sur des logiciels, or tout logiciel comporte des vulnérabilités. Les plus dangereuses sont celles qui sont encore peu connues et qui n'ont donc pas de correctifs largement distribués. Un outil de cybersécurité est-il adapté pour contrer les cyberattaques auxquelles il est censé faire face ? Les fonctionnalités prétendues sont-elles réelles et efficaces ? Le logiciel comporte-t-il des fonctionnalités cachées ? Le développe-

ment du produit est-il compatible avec la sécurité attendue ?

Quelle confiance objective peut-on accorder aux solutions de sécurité ? Qui est garant de la confiance que ces solutions feront ce pour quoi elles sont installées et tout ce qu'elles doivent faire dans des conditions réelles de telle ou telle attaque ?

On pourrait penser qu'un produit de sécurité est lui-même sécurisé et assume bien son rôle si une organisation, dont la sécurité repose sur le même produit, n'a jamais exprimé un avis négatif. On pourrait penser que, si un produit de sécurité est développé ou commercialisé par une organisation qui a bonne réputation, ce produit est sûr. On pourrait penser que, plutôt que de comparer deux produits, il est préférable de comparer la réputation de leurs concepteurs. Cette confiance n'est que de la confiance « **subjective** ».

On peut considérer qu'un produit de sécurité assure sa fonction, n'assure que sa fonction et toute sa fonction, que s'il est passé au travers d'une batterie de tests menés par des experts et validés par un organisme officiel. Bien sûr, ce sont les mêmes tests pour tous les produits de la même famille, qui poussent à un niveau suffisant les contrôles sur toute la surface des fonctionnalités attendues de ce produit et avec une profondeur suffisante. On peut vouloir vérifier, **par une certification**

**validée** par un diplôme, que ces tests ont été réalisés par un organisme indépendant et que le résultat a reçu l'aval d'un organisme d'état. On veut être persuadé que deux produits, qui assurent les mêmes fonctionnalités, ont passé les mêmes tests, avec le même degré d'exigence, sur une surface équivalente des produits. On obtient alors une **assurance de sécurité objective** qui, de plus, permet de comparer deux produits de la même famille.

Pour que cette confiance en un produit puisse être formalisée, elle doit reposer sur des méthodes d'évaluation de risque et sur la fourniture de preuves qualifiées et infalsifiables, mais elle doit s'appuyer aussi sur une **autorité de confiance**, universellement reconnue. Ces méthodes et ces preuves peuvent apporter une **confiance objective** en la sécurité d'un produit.

### De l'Orange Book à la CSPN, des alliances se dessinent

Dans les années 80, les USA ont adopté l'Orange Book (ou TCSEC), certification américaine fruit d'un appel d'offre émis par le NIST<sup>1</sup>. L'*Orange Book* définissait des niveaux de sécurité allant du niveau D (le moins exigeant) au niveau A, mais qui ne permettaient pas d'avoir des critères de comparaison entre plusieurs produits de la même famille. Ces certifications américaines définies par l'*Orange Book* allaient-elles être reconnues en Europe ?

Trois pays européens, un bel exemple de coopération multilatérale dans le domaine de la certification de sécurité : France, Grande-Bretagne et Allemagne, auxquelles

(2) Information Technologies Security Evaluation Criteria.

(3) Anadrian Trusted Computer Product Evaluation Criteria.

se sont joints les Pays Bas, ont écrit les **ITSEC**<sup>2</sup> qui établissaient des niveaux de confiance de E1 à E6, pendant que le Canada écrivait ses

propres critères d'évaluation, le **CTCPEC**<sup>3</sup>. Pourtant la certification ITSEC E3, par exemple d'un pare-feu, allait-elle être reconnue par les États-Unis, ou même par les pays d'Europe qui n'avaient pas participé à l'élaboration des ITSEC ? Nous avons là plusieurs organismes de certification, qui ont défini leurs niveaux de confiance et qui, avec les ITSEC, ont montré qu'une certification commune entre pays était possible.

Au début des années 2000, tous ces pays unissent leurs travaux pour définir une nouvelle méthodologie pour s'assurer qu'un produit de sécurité remplit ses fonctions, pas plus et pas moins, avec un niveau d'assurance quantifié, face à des menaces bien définies. Cette coopération internationale allait aboutir aux « **Critères Communs** ». Ce n'étaient encore que des standards industriels, qui n'avaient pas force de loi, mais la version 2.1 des Critères Communs devint une norme internationale (ISO/IEC 15408) publiée en 2009 et modifiée en 2014.

## Les Critères Communs, un standard international devenu une norme ISO

(4) Common Criteria for Information technology Security Evaluation» <https://www.commoncriteriaportal.org/>

(5) Common Criteria Recognition Arrangement.

(6) Agence Nationale de la Sécurité des Systèmes d'Information <https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/criteres-et-methodologies-devaluation/>

Les Critères Communs<sup>4</sup> sont des spécifications qui évoluent grâce aux travaux d'un groupe d'experts, avec des accords de reconnaissance mutuelle, le CCRA<sup>5</sup>. La version actuelle 3.1 se compose de quatre volumes : Le premier porte sur le sujet « *Introduction et modèle général* », le deuxième sur les « *exigences*

*fonctionnelles* » qui sont essentiellement une bibliothèque d'éléments qui décrivent les fonctionnalités de sécurité pouvant être mises en œuvre par le produit. Le troisième volume décrit les « *exigences et les niveaux d'assurance* » relatifs aux mesures de sécurité conformes aux spécifications et assortis d'une efficacité, en accord avec le niveau de certification visé. Un quatrième volume traite des méthodologies d'évaluation. Il existe une version en français de ces spécifications, à télécharger sur le web de l'ANSSI<sup>6</sup>.

Un produit est évalué « Critères Communs », non pas pour l'ensemble de ses fonctionnalités et de son code, ce ne serait que trop difficilement atteint, mais sur un espace restreint appelé une « **cible de sécurité** ». Pour éviter qu'un éditeur ne se lance dans un jeu subtil de

découpage de sa cible de sécurité pour ne proposer de soumettre aux tests qu'une fine dentelle du produit dont il est persuadé qu'elle passera les tests sans problème, il a été prévu la notion de « **Profil de Protection** » (PP : *Protection Profile*).

Un profil de protection est une cible de sécurité générique propre à un type d'équipement ou à une communauté d'utilisateurs comme, par exemple les Firewalls. Si un commanditaire veut faire certifier un produit, qui présente des fonctionnalités couvertes par un profil de protection, il doit l'inclure dans sa cible. Ainsi la certification « Critères Communs » gagne en crédibilité, surtout que, d'un standard international, elle est devenue une norme (ISO/IEC 15408).



Le caractère normé de la cible et la profondeur des tests permet de donner au client une assurance objective de l'adéquation du produit commercialisé à ses besoins et à la sécurité de son activité.

Le commanditaire soumet, à l'autorité de certification, sa cible de sécurité qui définit la surface du produit qui va subir les tests.

Cette cible de sécurité doit être

(7) Secrétariat  
Général de la  
Défense et de la  
Sécurité Nationale.

(8) Centre d'Évaluation  
de la Sécurité  
des Technologies  
de l'Information.

acceptée par l'organisme signataire de la certification, en France l'**ANSSI**, rattachée au SGDSN<sup>7</sup>, organisme interministériel qui dépend du Premier ministre. La cible

acceptée, les tests de certification peuvent commencer. Cette évaluation est menée par un cabinet privé, le CESTI<sup>8</sup>, choisi par le commanditaire.

Dans la cible de sécurité sont définies les menaces auxquelles le produit doit faire face et comment il se comporte pour les contrer. Le soumissionnaire définit la surface d'évaluation en choisissant parmi les **éléments fonctionnels** des Critères Communs, ceux qui correspondent aux fonctionnalités à tester. Il décide du niveau de certification qu'il souhaite que son produit atteigne, ce qui implique la fourniture des **éléments d'assurance** qui prouveront que la cible peut obtenir ce niveau de certification. Un produit

(9) EAL : Evaluation  
Assurance Level

peut être certifié « Critères Communs » sur l'un des sept niveaux d'évaluation allant de EAL1 à EAL7<sup>9</sup>.

EAL1 est le plus bas niveau des Critères Communs et définit des tests de fonctionnement en boîte noire : on s'assure que le produit se comporte conformément à ce qui est écrit dans sa documentation. Avec EAL4, on commence à vérifier

des parties du code source du produit.

Au-delà commence le domaine de la certification par des technologies mettant en œuvre des méthodes de développement plus spécifiques et rigoureuses. On commence alors à parler de spécifications semi-formelles. Le plus haut niveau, EAL7, impose des spécifications formelles exprimées dans un langage syntaxique basé sur des concepts mathématiques.

S'engager dans une démarche de certification « Critères Communs », c'est emprunter un chemin long, sinueux et coûteux. Cela suppose un travail important qui peut s'étaler sur plus d'un an. Le coût d'une certification EAL4 peut s'élever à plus de 100 000 euros qui seront versés à un CESTI, l'organisme d'experts qui va effectuer les tests et monter le dossier d'évaluation qu'il remettra à l'organisme officiel de certification. Il faut aussi compter les ressources que le commanditaire de la certification doit mettre en œuvre en interne. Bien entendu plus le niveau de certification à atteindre est élevé, plus la surface de la cible de sécurité est étendue, plus le travail et le budget à prévoir sont conséquents. Enfin, pour avoir une chance d'atteindre la certification souhaitée, le produit doit être dans une version stable et mature.

Des accords de reconnaissance mutuelle européens (SOG-IS) existent jusqu'au niveau d'évaluation EAL4, depuis 2010,

et pour des domaines techniques très spécifiques, comme les microcontrôleurs, jusqu'au niveau EAL7.

### La CSPN, une voix de la France dans le concert des certifications

Pour établir le niveau de confiance qu'on peut accorder à un produit de sécurité face à certaines attaques, les « Critères Communs » sont efficaces, reconnus internationalement, mais ils demandent un travail très conséquent car ils sont chers et longs à obtenir. Si le coût et la durée de la certification sont un obstacle, il existe une autre certification. L'ANSSI a créé, en 2008, la **CSPN, Certification de Sécurité de Premier Niveau**, solution suffisante quand le niveau de confiance visé n'est pas élevé. Elle consiste en des tests en « boîte noire » effectués en temps et délais contraints. L'évaluation de sécurité est faite, comme pour les Critères Communs, par un centre d'évaluation (CESTI) agréé par l'ANSSI. Il faut compter 25 jours pour qu'un produit obtienne, si les tests sont concluants, une certification CSPN ou 35 jours si le produit comporte aussi des éléments de cryptographie.

La CSPN est une certification française mais d'autres pays européens commencent à nous l'envier et vont sans doute l'adopter ou l'imiter. Les États-Unis y pensent aussi. La reconnaissance de la CSPN par l'Europe est un des objectifs de l'ANSSI.

## La Qualification, une certification qui peut être exigée

**La Qualification** est « *la recommandation par l'État français de produits ou services de cybersécurité éprouvés et approuvés par l'ANSSI* ». Dans la qualification,

le client, en général une administration

(10) Opérateur d'Importance Vitale.

ou un OIV<sup>10</sup>, définit la cible sur laquelle les tests vont porter. Elle comprend trois

niveaux : la qualification élémentaire qui peut être obtenue si le produit est certifié CSPN, la qualification standard qui requiert que le produit soit certifié « Critères Communs » au niveau EAL3+ et la qualification élevée pour laquelle le produit doit être certifié EAL4+. Alors que les certifications « Critères Communs » sont attribuées « à vie » mais pour une version précise du produit, la qualification est attribuée pour une durée de deux à trois ans puis doit être renouvelée.

## Une confiance objective établie ?

Utilisée à des fins de boucle d'amélioration de la qualité logicielle et de l'environnement de développement, les certifications « Critères Communs » ou CSPN et les Qualifications, quand cela est nécessaire, ont tout leur sens et donnent une confiance objective vis à vis du produit.

Mais pour que celle-ci soit établie, il convient de bien lire le rapport de certification ou de qualification qui n'est valable que :

- pour la version évaluée du produit ;

- dans les conditions d'utilisation et/ou d'exploitation qu'il décrit ;

- dans la limite des hypothèses et des menaces considérées par la cible de sécurité.

La certification d'un produit ne s'applique pas aux mises à jour ultérieures, sans maintenance de cette certification. Elle ne fournit donc aucune information sur les versions plus récentes.

Les certifications et qualifications sont un grand pas pour accorder une confiance objective à un produit de sécurité et sont aussi un bel exemple de coopération internationale avec les Critères Communs. Avec la CSPN, la France a fait preuve de capacités d'innovation et d'adaptation à la réalité du marché. Nul doute que d'autres pays l'imiteront.

## L'AUTEUR

**Lieutenant-colonel dans la Réserve Citoyenne de Cyberdéfense de la gendarmerie nationale, ingénieur diplômé, expert en cybersécurité, et aujourd'hui retraité actif, Gérard Peliks s'implique dans des associations comme l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information). Il est chargé de cours dans des masters et MBA dans des écoles d'ingénieurs et universités.**

**Il écrit des articles sur les dangers du cyberspace et coorganise les « Lundi de la cybersécurité » le soir, sur une base mensuelle, à l'Université de Paris Descartes.**



# La Blockchain

## au service de la sécurité

Par Jacques Favier et Élie Fontana

# P

Pourquoi l'armée s'intéresserait-elle à la blockchain ? Parce qu'en examinant les cas d'usage déjà développés par des militaires en France, ce qui est actuellement au stade de recherche, en répertoriant les obstacles qui restent à lever et en se plaçant dans la perspective des nombreux désordres possibles après la pandémie, le recours à la forme résiliente d'ordre qu'offre une blockchain doit être considéré comme une opportunité pour les visionnaires.



**JACQUES FAVIER**

Cabinet conseil  
« Catenae ».



**ÉLIE FONTANA**

Commandant  
de l'armée de Terre.  
Stagiaire à l'École  
de Guerre.

Transporter de façon sécurisée de l'information ou de l'argent, du matériel ou des pièces détachées est stratégique. Or, la logistique est l'un des domaines où la mise en œuvre d'une *blockchain* aurait des vertus tandis que la crise née de la pandémie plaide pour un intérêt accru des spécialistes de la sécurité envers une technologie porteuse d'une forme spécifique d'ordre.

### « La » Blockchain ?

Le concept de *blockchain* a émergé d'une innovation radicale : Bitcoin. La première fonction des protocoles qu'il a inspirés consiste à échanger des jetons numériques. Bitcoin en 2009 et ses copies privilégiaient la sécurité absolue de la base de données et des transactions. En 2014, Ethereum proposa une *blockchain* différente, avec un langage de programmation plus accessible et des programmes auto-exécutables. Une troisième génération de *blockchain* regroupe celles (Tezos, Cardano ou EOS) qui permettent une réelle mise à l'échelle

ou des mécanismes de gouvernance rationalisée.

L'important, ce sont deux principes fondamentaux : la distribution des données et celle du consensus. Un grand nombre de nœuds n'apporte pas une garantie robuste si la validation des écritures reste le fait de quelques-uns. Au-dessus du consensus algorithmique, il demeure toujours un consensus social critique.

Quant aux usages, on peut en retenir 4 familles : les règlements (projets privés de Facebook ou de JP Morgan et expérimentations au niveau des banques centrales) ; la notarisation et le traçage, notamment pour les secteurs stratégiques de la défense et de l'aérospatiale ; le vote et enfin les transactions entre machines.

### Pour quoi faire ?

Septembre 2019 a connu le premier déploiement d'un contrat auto-exécutable par une entité gouvernementale, le C3N de la Gendarmerie nationale, pour noter les justifications de dépenses subventionnées par Europol. Pour des raisons techniques, il fut choisi de le faire sur la *blockchain* publique *Tezos*. Le bénéfice d'une traçabilité infalsifiable et transparente coûtait moins de 0,003 € par enregistrement et cette preuve de concept ouvrait la voie à un changement de paradigme comptable et à la fluidification de la réponse logistique aux besoins opérationnels.

Les Armées (et les publications spécialisées) ont assez vite perçu la *Blockchain* comme un outil de remise en cause d'idées acquises. Depuis 30 ans, les évolutions les plus notables portent sur les technologies d'information et de communication mais toutes s'appuient sur un même type d'architecture radio en étoile. Au centre, les stations directrices sont de réels goulets d'étranglement et elles facilitent le travail du renseignement adverse du fait de leur fâcheuse caractéristique d'émettre beaucoup plus fort que les autres stations.

Si les forces armées adoptaient des protocoles de communication chiffrés avec une transmission de station en station par le chemin le plus direct, la perte d'un nœud

n'aurait pas d'incidence.

Avec une numérisation intégrale et en s'appuyant sur les technologies RFID<sup>1</sup> et *blockchain*, la logistique de transport pourrait enfin obtenir une vision exhaustive et en temps réel de l'intégralité de ses flux.

La politique de mainte-

nance sur les théâtres d'opérations en serait améliorée et cela permettrait des rapports plus clairs avec les entreprises civiles.

Pour la fonction « connaissance-anticipation », la question de la bascule sur une *blockchain* est plus difficile, vu l'importance

(1) La RFID (radio frequency identification), ou radio-identification, est une technologie qui permet de sauvegarder et récupérer des données à distance sur ce que l'on appelle des puces ou tags RFID ou encore des radio-étiquettes.

centrale des bases de données possédant un très haut niveau de confidentialité. La politique consiste à dégrader la base de données au fur et à mesure qu'on s'approche de la zone d'insécurité, pour limiter le risque de compromission en cas de perte de la base. La distribution décentralisée des bases de données "renseignement" ne pourra se faire qu'en l'assortissant d'une preuve d'une robustesse logique et équivalente à celle qui est reconnue en organisationnel.

En métropole, les hauts standards de sécurité sont plus aisément respectés qu'en opération. **Ceci devrait faciliter un déploiement décentralisé de données traditionnellement centralisées.** Plusieurs cas d'usages sont envisageables. Le plus accessible est une évolution de solutions déjà utilisées, une décentralisation de l'ensemble des processus administratifs, leur inscription dans un registre unique et transparent, auditable par tous. Les logiciels de signature électronique et de suivi de courriers, lourds et non universels, pourraient être remplacés par des solutions légères.

### Se pose aussi la question de la protection des confidentiels dits spécifiques.

La pandémie a forcé au confinement de très nombreux cadres militaires. Éloignés de leurs enceintes sécurisées, ils s'en sont davantage remis à des solutions de communication peu sécurisées. La concentration sur certains



© Human eyes on digital computer

Les solutions passent par la reconnaissance de la robustesse des protocoles décentralisés autant que par une adéquation aux besoins d'inviolabilité des transactions et d'une authentification numérique élargie.

serveurs de toutes ces données cruciales à la vie militaire est une vulnérabilité face à une panne d'envergure ou à une cyber-attaque qui aurait des conséquences importantes sur le fonctionnement d'une armée déjà contrainte d'adopter un fonctionnement alternatif. Le choix d'une distribution décentralisée des données rendrait plus robuste l'organisation. Les satellites de surveillance, les moyens de défense sol-air, les aéronefs d'alerte mais aussi les unités engagées en cas de catastrophe naturelle,

voire NRBC<sup>2</sup>, devraient être dotés d'un réseau décentralisé pérennisant la mission de protection une fois le premier choc encaissé. La paralysie que nous avons connue suggère le risque que

(2) Les risques NRBC (Nucléaires, Radiologiques, Biologiques, Chimiques) sont des risques à danger élevé, ayant pour enjeu la vie des populations civiles ou des militaires.

revêtirait un virus plus mortel, voire un *blackout* complet après une cyber-attaque de grande ampleur.

**Entrapercevoir les déclencheurs d'une crise et ses conséquences n'est pas suffisant. Il faut consentir le coût d'une préparation matérielle.** Les Américains poursuivent certes une politique d'investissements massifs dans les nouvelles

technologies, et la DARPA<sup>3</sup> expérimente, depuis 2016, un protocole de messagerie décentralisé. En 2019, elle en était encore à une demande d'information sur les capacités de la *blockchain* dans l'amélioration de la sécurité, du stockage ou du calcul. Au niveau de l'OTAN, le SHAPE<sup>4</sup>, a vocation à penser la standardisation permettant l'interopérabilité de ses membres. La *NATO Communication and*

(3) La Defense Advanced Research Projects Agency (DARPA) (« Agence pour les projets de recherche avancée de défense ») est une agence du département de la Défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire.

(4) Le Supreme Headquarters Allied Powers Europe (SHAPE) est le centre de commandement militaire des forces de l'OTAN en Europe.

*Information Agency* a lancé, en 2016, un appel à projet pour des solutions *blockchain*. Mais sa formulation ne laisse pourtant que peu d'espoir pour de vraies applications stratégiques. Les propositions en resteront sans doute davantage à la messagerie et au suivi logistique.

### Des défis nombreux

Dans chaque corps, l'intérêt pragmatique

pour la *blockchain* ne concerne encore que des profils particuliers, pas forcément majoritaires. Il faut lever les doutes, réfuter les craintes, trouver les mots pour faire admettre de nouvelles idées, rapprocher deux mondes qui ont à apprendre l'un de l'autre, faire comprendre qu'il ne s'agit pas d'un gadget pour informaticien.

L'existence d'une face sombre des cryptomonnaies n'est pas une raison suffisante pour ignorer la blockchain. Internet aussi a servi aux criminels. Si une invention ne sert pas aux criminels (surtout dans ses premiers pas) c'est probablement qu'elle n'apporte rien... L'automobile naissante a été utilisée en 1910 par la bande à Bonnot et en 1914 par le général Gallieni. Quant au routage en oignon (Tor), il n'a pas été développé pour faire circuler du contenu pornographique mais en partie par des militaires américains, pour augmenter la sécurité de leurs communications.

La seule parade au crime, comme la Gendarmerie Nationale l'a montré en appréhendant plusieurs cybercriminels, c'est une connaissance fine de la technologie. Pour traquer les transactions, mais aussi anticiper les coups à venir (monnaies plus anonymes, "laveries" crypto, etc.) mieux vaut être docteur en informatique et travailler en partenariat avec des start-ups de l'écosystème. L'échange de bonnes pratiques avec les sociétés Bitcoin est essentiel. Elles ont été les premières victimes des cybercriminels et les

principales plateformes de change se soumettent aux règles anti-blanchiment et anti-terrorisme. Plusieurs start-up (Score-chain, Elliptic...) ont développé des solutions de traçage.

Il s'agit d'un domaine en constante évolution et qui suscite de nombreuses rencontres, dont celles du FIC.

**Les nations occidentales recherchent dans les technologies un avantage comparatif et la blockchain doit y être comprise.** Certes l'IA concentre l'essentiel de l'attention mais les avancées relèvent davantage de la communication que de la percée technologique. En regard, la *blockchain*, technologie mature avec des cas d'usages accessibles, pourrait offrir des résultats opérationnels concrets. Il faut qu'elle soit rendue compréhensible aux militaires, admissible par l'opinion publique et qu'un dialogue soit maintenu avec les savants.

Il faut déminer deux sujets, la décentralisation des données et leur ouverture au public, en trouvant les moyens de les présenter, au mieux, à des militaires habitués à la hiérarchie plutôt qu'à des informaticiens « anarchisants ».

On a longtemps compté pour défendre le secret Défense sur le béton et le blindage, développant une "culture du coffre-fort" que les réalités numériques viennent bousculer. Avec l'accumulation des données

a crû la taille des *hacks* de sites qui se vantaient d'une sécurité *militaire*. Comme les parasites attirés par la grande culture, les hackers sont stimulés par l'entreposage de millions de téraoctets de données valorisables. Un fonctionnement disséminé est une défense naturelle contre ces prédateurs.

Il reste à expliquer le caractère public des grandes *blockchains*. Penser que "publiques" signifie ouvertes à tout vent est un contresens ; imaginer que les *blockchains* "privées" sont mieux sécurisées est un contresens pire encore.

Il faut enfin conforter la collaboration avec les savants nationaux, que ce soit dans des formations spécialisées (IRSEM, IHEDN, École de Guerre), des partenariats (Groupe Thalès avec les Écoles normales supérieures) ou des échanges intellectuels (Association des Réservistes du Chiffre et de la Sécurité de l'Information).

**Une fois abandonnée la logique du "château fort" il faut envisager trois axes de réflexion** sur ce qui touche au terrain dans lequel se déroulent les échanges, sur les traces, les indices, les preuves qui en résultent et enfin sur la maîtrise nécessaire de tous les "langages" impliqués dans ces échanges.

Dans l'espace numérique, le premier facteur de souveraineté tient à l'existence d'une capacité nationale d'entretien,

d'amélioration et de mise à jour du protocole source, mais aussi de développement et d'audit des programmes auto-exécutables. La territorialité des infrastructures constitue un autre élément clef de la souveraineté, en particulier pour la *blockchain* que le caractère distribué du stockage n'affranchit pas des logiques territoriales : une transaction validée voire simplement compilée par un nœud situé en territoire étranger peut être soumise à une loi différente de la loi française.

Enfin l'identité des citoyens est aussi un enjeu stratégique du fait des failles de souveraineté que la réalité numérique de notre pays provoque. Alors que les procédés d'identification par Facebook et Google sont extrêmement *users friendly*, l'authentification *France-Connect*, conçue en théorie pour l'interopérabilité et les échanges européens et mondiaux, comme le pivot de l'identité numérique des français et l'outil français permettant l'interconnexion dans le cadre du programme européen e-IDAS, risque de souffrir de son caractère centralisé et hexagonal (ou « seulement » européen).

Un système adapté au monde numérique et protégeant les données des utilisateurs devrait s'apparenter à un protocole informatique internationalement interopérable. Une *blockchain* permettrait une forme numérique de l'identité (des citoyens, des entreprises, pourquoi pas des robots et des machines) qui aille

dans la voie d'une identité garantie et rendue inviolable par la cryptographie. La technologie des « ZP » (*zero proof*) fournirait une voie de mise en œuvre.

### Go !

Nous n'éludons pas les défis. Mais les chocs nés de la pandémie peuvent provoquer une récession intellectuelle, une paresse qui laisse la porte ouverte aux GAFAM. Pour les plus visionnaires, les crises peuvent au contraire favoriser l'innovation de rupture. Adopter des architectures ouvertes et décentralisées en lieu et place des silos et des citadelles serait une révolution au sens où on va entendre ce mot au XXI<sup>e</sup> siècle.

### LES AUTEURS

**Jacques Favier, normalien, est agrégé d'histoire. Co-fondateur du cabinet conseil « Catenae ». Auteur de plusieurs livres sur Bitcoin et les blockchains, il est le secrétaire de l'Association francophone « Le Cercle du Coin ».**

**Le commandant Élie Fontana, de l'armée de Terre, est stagiaire à l'École de Guerre. Il est l'ancien chef de bureau adjoint à la Direction du Renseignement Militaire.**

# De la genèse de la loi

« Informatique et Libertés » à l'éloge de la transdisciplinarité

Par Alice Louis

**L**

(1) Yves Lenoir, Ingénieur de recherche à l'Ecole des Mines de Paris, « L'interdisciplinarité : aperçu historique de la genèse d'un concept ». Cahiers de la recherche en éducation, 1995, 2 (2), p 227-265.

« L'unification est un grand rêve [...]. Je me souviens que j'avais été frappé, lorsque j'avais lu «Le jeu des perles de verre» de Hermann Hesse» [...].

Cette unification était

réalisée par le biais de ce jeu de perles dont étaient sorties la musique, puis les mathématiques, *etc.* et finalement rassemblait toute la connaissance humaine en une seule pratique. »<sup>1</sup>



**ALICE LOUIS**

Consultante en Gouvernance du Patrimoine Informationnel & DPO Externe.

La genèse de la loi  
« Informatique  
et Libertés »

L'augmentation sans précédent des cyberattaques, depuis la crise sanitaire, oblige les acteurs du secteur public et privé à repenser leur modèle

(2) La Cybersécurité est définie par l'ANSSI comme suit : « l'état recherché pour un système d'information (SI) lui permettant de résister à des événements issus du cyberspace 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 la cybercriminalité et sur la mise en place d'une cyberdéfense». <https://www.ssi.gouv.fr/entreprise/glossaire/c/>

de gouvernance, avec l'objectif d'y intégrer des fonctions capables de répondre efficacement aux nouvelles exigences en matière de Cybersécurité<sup>2</sup>.

La protection des différentes entités contre les risques d'atteinte à leur patrimoine informationnel est notamment régie par le Droit de la Cybersécurité - droit pluridisciplinaire<sup>3</sup> eu égard à la diversité des bases textuelles qu'il englobe.

(3) Il est aussi transdisciplinaire. En effet, nonobstant les législations et réglementations spécifiques, le droit pénal, le droit des contrats, les droits dits « sectoriels » (citons la directive (UE) 2015/2366 relative aux services de paiement, dite DSP2, entrée en vigueur le 13 janvier 2018), le droit de la responsabilité civile, le droit du travail, le droit de la propriété intellectuelle, etc., comportent des articles applicables au domaine.

(4) Tina Malet, « XVIII<sup>e</sup> siècle L'Europe des Lumières », [https://www.herodote.net/L\\_Europe\\_des\\_Lumieres-synthese-2157.php](https://www.herodote.net/L_Europe_des_Lumieres-synthese-2157.php)

(5) Wikipedia, « la parabole des talents », L'Évangile selon Matthieu XXV, 14-30, <https://fr.wikipedia.org/>, le 19/09/19, disponible sur : [https://fr.wikipedia.org/wiki/Parabole\\_des\\_talents](https://fr.wikipedia.org/wiki/Parabole_des_talents)

(6) Luc Ferry, « Une brève histoire de l'éthique : de l'antiquité à nos jours, Cycle de conférence : philosophie du temps présent », Parenthèse Culture 2, <https://www.youtube.com/>, le 19/09/19, disponible sur : <https://www.youtube.com/watch?v=UkzBT-LQsGfI&t=4327s>

Parmi ces dernières, figure la loi « *Informatique et Libertés* » dont les principes et les valeurs, qui en sous-tendent la vision, sont issus de l'histoire de la philosophie morale\*, à l'époque où « la France, à l'apogée de sa civilisation, sert de modèle à l'Europe entière »<sup>4</sup>.

### \* FOCUS : LA PHILOSOPHIE MORALE ET LES LIBERTÉS INDIVIDUELLES.

**Dans la République de Platon, la cité est juste** lorsqu'elle reproduit l'ordre de « la nature » et la hiérarchie des êtres. Ainsi « le juste » n'est autre que « l'ajusté ». Tout en l'illustrant parfaitement, « la parabole des talents »<sup>5</sup> annonce la rupture avec cette vision aristocratique du monde<sup>6</sup>.

**Les textes fondateurs<sup>7</sup> de la deuxième vision morale** considèrent que les dons naturels n'ont aucune valeur sauf celle d'être mise au service du « bien » ou du « mal ». Quant à la vertu, c'est l'altérité, et, enfin, le labeur puisqu'en transformant la nature (l'agriculture) on se transforme soi-même (la culture).

(7) « Le contrat social » de J-J Rousseau et « Le fondement de la métaphysique des mœurs » d'E. Kant.

**Le siècle des Lumières sera celui de la renaissance** des libertés individuelles - liberté de conscience, liberté d'expression, liberté économique,

liberté contractuelle, droit au respect de la vie privée, etc. - qui sont la transposition juridique d'une philosophie des droits de l'homme.

**Mai 1968 incarne la troisième vision du monde.** Celle-ci annonce l'ère de la grande consommation ainsi que l'avènement des nouvelles technologies de l'information. À noter qu'en 1966, l'Académie française accueille le mot « Informatique ».

Hannah Arendt, philosophe et politologue allemande énonçait à propos des technosciences qu'elles pouvaient devenir l'outil d'un totalitarisme « *confisquant l'avenir des hommes* », si ceux-ci ne développaient pas

« *à leur égard une pensée critique* » en vue de préserver la démocratie<sup>8</sup>.

(8) Max Dauchet, « Les informaticiens et l'éthique du numérique », <https://www.lemonde.fr/blog/binaire/2014/03/11/>

(9) Philippe Boucher, journaliste au Monde, « Safari ou la chasse aux Français », <https://rewriting.net/wp-content>

(10) Bugbrother, « Safari et la (nouvelle) chasse aux Français », 23 décembre 2010, <https://www.lemonde.fr/blog/bugbrother/2010/12/23/safari-et-la-nouvelle-chasse-aux-francais/>

Le 21 mars 1974, le journal Le Monde<sup>9</sup> révélait l'existence du projet dénommé « *Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus* » (S.A.F.A.R.I.), initié par le Ministre de l'intérieur, Raymond Marcellin dont le parcours politique avait été jugé « complexe »,



(11) Après des siècles de régimes monarchiques, le référencement des citoyens vise à symboliser une appartenance commune à la République ainsi qu'une égalité devant la loi. C'est notamment la raison pour laquelle le NIR, plus connu sous le terme de numéro de sécurité sociale dans le Répertoire National d'Identification des Personnes Physiques (RNIPP) a été créé.

(12) Pierre Piazza, « Système d'enregistrement d'identité, numéro d'identification et "carte d'identité de Français" durant le Régime de Vichy (France, 1940-1944) » <https://journals.openedition.org/criminocorpus/3649>.

(13) <http://www.senat.fr/evenement/archives/D45/context.html>

en particulier, durant la Seconde Guerre mondiale<sup>10</sup>. S.A.F.A.R.I avait pour objectif d'interconnecter l'ensemble des fichiers de l'administration pour créer une base de données nationale. En outre, il prévoyait d'identifier chaque citoyen français par un numéro unique<sup>11</sup> ; ce qui ne manqua pas d'évoquer les heures les plus sombres de notre Histoire récente. En effet, rappelons que sous le gouvernement de Vichy, la loi du 27 octobre 1940 obligeait « *tout Français âgé d'au moins seize ans à se munir d'une «carte d'identité de Français [...] L'occupant y voyait la base nécessaire à la surveillance et au maintien de l'ordre* »<sup>12</sup>...

Face à la polémique que le projet S.A.F.A.R.I suscita, le Premier ministre d'alors, Pierre Messmer, s'engagea à le retirer et à créer concomitamment une Commission dite « informatique et libertés »<sup>13</sup>. Le rapport Tricot, que cette dernière publia en 1975, posa les principes généraux de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés,

qui fut adoptée le 6 janvier 1978.

L'article 1<sup>er</sup> de celle-ci dispose que : « *l'informatique doit être au service de chaque citoyen. [...] Elle ne doit porter atteinte ni à l'identité humaine ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

(14) Le « paquet européen » inclut également la Directive dite « Police-Justice » n°2016/680 du 27/04/2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données (applicable uniquement aux fichiers de la sphère pénale).

### Les éléments substantiels des bases textuelles

À l'instar d'autres domaines du droit français, notamment du Droit de la propriété intellectuelle, ce régime de protection a très largement inspiré le législateur européen. La directive 95/46 du 24 octobre 1995, transposée dans le droit national par la loi n° 2004-801 du 6 août 2004 substituée à la notion « *d'informations nominatives* », celle de « *données à caractère*

*personnel* ». Il est précisé que la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique consacre notamment le droit à l'autodétermination informationnelle, qui renforce le consentement, et la maîtrise des données *post mortem*.

Par ailleurs, le « paquet européen »<sup>14</sup>, pu-

blié le 4 mai 2016 au *Journal Officiel de l'Union européenne*, qui comprend le Règlement Général pour la Protection des Données (R.G.P.D), adapté dans le droit national par la loi n° 2018-493 du 20 juin 2018, enrichit la notion de « *données à caractère personnel* » avec de nouveaux critères d'identification de l'individu (génétiques, biométriques, etc.). En outre, il inclut les éléments qui suivent :

- Exigences de proportionnalité et de limitation (obligation de loyauté, finalités déterminées, *etc.*)
- Mesures organisationnelles et techniques (privacy by design et by default, DPO, *etc.*)
- Obligation de sécurité renforcée (risque élevé pour les personnes concernées, *etc.*)
- Garanties des sous-traitants (Data agreement, co-responsabilité)
- Création de nouveaux droits de la personne (droit à l'oubli = l'effacement, droit d'accès, *etc.*)
- Charge de la preuve (l'accountability : responsable du traitement, *etc.*)
- Augmentation des sanctions pécuniaires (dimension pénale notamment sur le consentement, *etc.*)

Plus globalement, les 99 articles et les 173 considérants du RGPD traduisent une volonté de responsabiliser les entités, qui, tout en veillant à préserver leur équilibre économique, devront intégrer une démarche éthique \*.

### \* FOCUS : LES THÉORIES DE L'ÉTHIQUE

L'éthique normative forme des théories qui permettent d'évaluer moralement les personnes et leurs actions selon les critères du « juste » et du « bien ».

L'éthique appliquée « applique » les normes de l'éthique normative à des contextes pratiques (Cf. l'éthique du numérique).

La méta-éthique quant à elle, étudie les fondements conceptuels, épistémologiques et ontologiques de l'éthique normative.

### L'éloge de la transdisciplinarité

Au cœur de la conformité et de l'éthique, qui comportent, désormais, des enjeux hautement stratégiques pour l'ensemble des organisations, **se trouve le délégué à la protection des données** (dit DPO).

Il est précisé que les acteurs publics et la plupart des entités du secteur privé ont l'obligation de le désigner. Le DPO

y tient un rôle majeur. En effet, rappelons qu'au titre de « *garant de la préservation du respect de la vie privée, de la sécurité juridique et technique* », le DPO est susceptible d'identifier, à l'aide

du **registre des activités de traitement**,

(15) Gérard Haas, « Gouvernance des données, ce que le RGPD a changé », Maison du Barreau, 22 mai 2019, [https://www.youtube.com/watch?v=fnMX1wy-YrWY&feature=emb\\_title](https://www.youtube.com/watch?v=fnMX1wy-YrWY&feature=emb_title)

4 832 points de (non) conformité<sup>15</sup>, parmi lesquels :

- Champ d'application (notamment territorial),
- Finalité, licéité, loyauté, transparence, consentement et analyse d'impact sur les droits et libertés des personnes,

(16) Il conviendra de vérifier la cohérence technique de bout en bout : protection des postes de travail, sécurité des réseaux, du Cloud, etc.

- Politique de sécurité (gestion des droits d'accès, chiffrement, anonymisation, suppression/purge des données, etc.<sup>16</sup>),

- Stratégie de conservation,
- Notification des failles de sécurité (CNIL, etc.).

Nonobstant son plan d'action (qui intégrera les éléments susvisés), pour la mise en œuvre duquel il devra exprimer toutes ses capacités de sensibilisation, parfois même d'influence, le DPO doit déterminer

(17) Gérard Haas, *ibidem*.

« la doctrine de l'entreprise »<sup>17</sup> - à titre

d'exemple, celle de « l'Intérêt légitime » qui exonère le responsable de traitement d'obtenir un quelconque consentement.

Son expertise, sa parfaite compréhension de l'activité, sa maturité pour la direction / le pilotage de projets et son sens aigu de la communication auprès d'interlocuteurs va-

riés, etc., démontreront la solidité ainsi que le caractère éminemment transdisciplinaire de cet acteur de la gouvernance.

Aussi, le DPO saura initier des échanges constructifs afin d'assurer une collaboration efficiente avec l'ensemble des services, en particulier, avec le DSI et/ou le RSSI.

*A fortiori*, dans un contexte de gestion de crise où leurs travaux communs (Chartes utilisateurs, télétravail, Plan d'Assurance Sécurité, etc.) permettront de déployer un système et des process « agiles ». In fine, son « objectif de neutralisation des risques d'atteinte aux données

(18) Gérard Haas, *ibidem*.

à caractère personnel »<sup>18</sup> pourrait représenter

l'opportunité pour les organisations d'adopter une approche plus globale de la « data », et ce, notamment, en vue de valoriser l'intégralité de leur patrimoine informationnel. Il en ressort, s'agissant d'une vision à long terme, que le DPO se révèle être un véritable levier de développement.

### Propos conclusif

*Le projet architectural majeur du vingt et unième siècle sera d'imaginer, de construire et d'aménager l'espace interactif et mouvant du cyberspace.*

*Le rôle de l'informatique et des techniques de communication à support numérique ne serait pas de « remplacer l'homme » ni de s'approcher d'une hypothétique « intelligence artificielle » (forte), mais*

*de favoriser la construction de collectifs intelligents où les potentialités sociales et cognitives de chacun pourraient se développer et s'amplifier mutuellement ».*

*Peut-être alors sera-t-il possible de dépasser la société du spectacle pour aborder une ère post-médias, dans laquelle les techniques de communication serviront*

(19) Pierre Lévy,  
« L'Intelligence collective », Editions La Découverte,  
1995, p. 25.

*à filtrer les flux de connaissances, à naviguer dans le savoir et à penser ensemble [...] »<sup>19</sup>.*

## AUTEURE

Alice Louis a principalement effectué son parcours professionnel dans le domaine des médias, notamment, en tant que Directrice Juridique du pôle d'agences de presse et d'illustration du Groupe Hachette Filipacchi Photos. Elle a aussi exercé comme Conseil en organisation auprès de plus petites entités (entreprises et structures ayant une mission d'intérêt général). Titulaire d'un DEA en Droit des Médias (IP/IT), et, plus récemment, d'un MBA en Management de la Cybersécurité, l'auteure accompagne, aujourd'hui, les dirigeants dans leur approche globale de la DATA.

Enfin, passionnée par toutes les questions inhérentes à « l'Éthique du numérique », l'auteure publie régulièrement des articles sur le sujet. Elle est, par ailleurs, Directrice du projet « Fonds Cyber Éthique pour une Souveraineté Numérique ».

# Réflexions sur l'ingénierie

sociale et le rôle de l'utilisateur en tant qu'acteur de la sécurité collective et collaborative

Par Denise Gross

Il y a tout juste un an, cette revue anticipait la thématique du FIC 2020 : « remettre l'humain au cœur de la cybersécurité ». Une prophétie dont la pertinence est évidente. Il est difficile d'imaginer une période dans laquelle le rôle de l'utilisateur sur le cyberspace aurait pu être plus important qu'en 2020. Une année disruptive, traversée par une pandémie, une crise mondiale et une accélération forcée de la transformation numérique. L'être humain a perdu ses repères. Il s'est retrouvé confiné mais hyperconnecté, envahi par l'incertitude et les fake news : un terrain de jeu pour les ingénieurs sociaux.



**DENISE GROSS**

Avocate au barreau de La Plata, Argentine.

## 1. Une année d'ingénierie sociale

L'ingénierie sociale<sup>1</sup> est un ensemble de compétences pluridisciplinaires,

(1) GROSS, D.  
L'ingénierie sociale : la prise en compte du facteur humain dans la cybercriminalité. Thèse de doctorat en droit pénal et sciences criminelles, Université de Strasbourg, 2019, pp. 25, 37, 61.

de méthodes et de techniques, qui permet à celui qui s'en sert de tirer profit des vulnérabilités humaines. Actuellement, le recours aux technologies est très fréquent dans toutes les phases d'une attaque. Or, ces outils ne sont pas

indispensables et ils seront seulement utiles si l'aspect humain est correctement exploité.

L'année 2020 nous a confirmé que l'ingénierie sociale s'adapte aux circonstances pour contourner les barrières de sécurité. Deux exemples nous aideront à visualiser ce postulat.

## COVID-19 et ingénierie sociale

L'emploi du vocabulaire épidémiologique en cybersécurité n'a jamais été aussi approprié. Le coronavirus mute et l'ingénierie sociale aussi. C'est l'une des raisons pour lesquelles elle est toujours efficace. La pandémie

(2) Le vishing est l'utilisation de la technologie VoIP (voix sur IP) dans le but de duper quelqu'un en lui faisant divulguer de l'information personnelle et/ou financier.

(3) Smishing est la contraction de SMS et de Phishing. On l'appelle également Hameçonnage par SMS. Le smishing est un message texte envoyé à un utilisateur sur son téléphone dans le but de l'inciter à partager ses données personnelles, ou télécharger un virus ou un programme malveillant à son insu.

(4) Le spear-phishing (littéralement pêche au harpon) est un mélange de techniques classiques de phishing et d'ingénierie sociale. Ce volet ingénierie sociale permet de cibler l'attaque en utilisant des thèmes liés au travail quotidien ou aux intérêts de la cible.

(5) Le ransomware est une forme dangereuse de logiciel malveillant qui s'infiltre dans les ordinateurs et les appareils mobiles pour kidnapper des fichiers précieux et les garder en otage.

déclarée en mars par l'OMS a bouleversé les individus, les entreprises, les organismes et les États. La surexposition des utilisateurs sur Internet, le stress, l'infobésité, le partage impulsif de contenus anxiogènes ainsi que la crise économique, politique et sanitaire et enfin l'augmentation de barrières techniques de protection des systèmes d'information ont largement contribué à l'épanouissement de l'ingénierie sociale. Elle se nourrit de ces facteurs personnels et situationnels pour préparer des attaques rentables, avec un taux de réussite plus favorable qu'en temps normal.

Une simple consultation sur des sites spécialisés et des plateformes de signalement permettra au lecteur de constater que la plupart des cyberattaques commises cette année, constituent

des faits: phishing, vishing<sup>2</sup>, smishing<sup>3</sup>, spear-phishing<sup>4</sup>, ransomware<sup>5</sup>,

(6) La fraude 419 (aussi appelée scam 419, ou arnaque nigériane) consiste à promettre la survenance d'une grosse somme d'argent dans le futur, exigeant de la victime qu'elle communique des éléments d'identité bancaire ou qu'elle fasse un paiement en amont afin de permettre la réalisation du gain à venir. La dénomination 4-1-9 vient du numéro de l'article du code nigérian sanctionnant ce type de fraude.

(7) D'après le support technique de Twitter : <https://twitter.com/Twitter-Support>; [https://blog.twitter.com/en\\_us/topics/company/2020/an-update-on-our-security-incident.html](https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html) Voir aussi : FRENKEL, S., POPPER, N., CONGER, K. & SANGER, D., A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam, The New York Times [page consultée le 17 juillet 2020], disponible sur : <https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html>

arnaques 419<sup>6</sup>, arnaques au président (FOVI), escroqueries sur des plateformes de commerce électronique et des campagnes de désinformation. La majorité des prétextes a été construite autour de l'évolution de la maladie et de la diffusion de moyens de prévention, des mesures économiques pour faire face à la crise, des systèmes de paiement en ligne, de l'offre de produits et de services nécessaires dans le cadre de la pandémie. Nous devons aussi mentionner des attaques telles que : grooming, sextorsion, chantage à la webcam. Il ne faut pas oublier les attaques physiques, si l'on pense au nombre d'escroqueries et de vols signalés suite à des faux contrôles ou des fausses campagnes de détection de la COVID.

## 1.2. Twitter : une attaque « mémorable » d'ingénierie sociale

Le 15 juillet 2020, un groupe d'employés de la plateforme Twitter a été visé par un « phone spear-phishing attack »<sup>7</sup>. Une sorte de chaîne d'authentification s'est produite

dans le sens où les identifiants des cibles initiales ont servi à accéder au système, puis à collecter des informations concernant le fonctionnement interne de la boîte et ensuite à viser d'autres employés ayant des privilèges, notamment, des droits d'accès aux outils de support des comptes Twitter (« account support tools »). Grâce à ces derniers, les attaquants ont touché 130 comptes de personnalités publiques, dont Joe Biden, Bill Gates, Elon Musk, Jeff Bezos, et d'entreprises comme Apple et Uber. Ils auraient tweeté depuis 45 comptes compromis, accédé aux messages privés (DM) de 36 comptes et téléchargé l'historique et les données stockées sur 7 comptes. Nous avons ici une double attaque d'ingénierie sociale, car elle a été appliquée dans un premier temps contre le personnel de Twitter puis aux abonnés au travers des tweets. En usurpant l'identité de ces célébrités, les attaquants ont sollicité du public un investissement initial en bitcoins, en leur promettant de recevoir le double de cette somme ultérieurement. La confiance qu'inspire un milliardaire, le fait qu'il décide d'aider les gens parce que « c'est le moment » pour le faire, l'ambition des abonnés, le sens d'urgence (l'offre n'était valable que pendant 30 minutes), révèlent l'efficacité des techniques d'influence sémantique. En quelques heures, les victimes de cette arnaque aux cryptomonnaies auraient transféré 120.000 dollars environ à l'adresse indiquée dans les posts.

Twitter a confirmé que c'était une attaque d'ingénierie sociale et rappelé l'importance du rôle de l'employé en charge de ce type de service. Le réseau a annoncé le renforcement des moyens de détection et de prévention des accès non autorisés à ses systèmes, par exemple, à travers des campagnes de phishing. Or, à aucun moment il n'affirme que ce fait ne se reproduira pas, au contraire, il s'engage à communiquer ouvertement les informations à chaque fois qu'un incident comme celui-ci sera détecté. Par conséquent, il y a beaucoup de travail à faire pour conserver la confiance des internautes.

## 2. L'utilisateur dans le cadre de la prévention et de la détection des stratégies d'ingénierie sociale

Selon l'ANSSI, la cybersécurité représente un « état recherché pour un système d'information lui permettant de **résister** à des événements **issus du cyberspace** susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes offrent ou

qu'ils rendent accessibles »<sup>8</sup>. Or, force est de constater que l'ingénierie sociale ne peut pas être

(8) Glossaire ANSSI : <https://www.ssi.gouv.fr/entreprise/glossaire/c/>

circonscrite au cyberspace. Elle existait bien avant son apparition. Elle est transverse, elle combine le monde physique et l'espace numérique, elle bouleverse la « sécurité » que nous devons aborder de manière intégrale pour ne pas

(9) Sources : <https://www.cnrtl.fr/etymologie/s%C3%A9curit%C3%A9> ; <https://www.larousse.fr/dictionnaires/francais/s%C3%A9curit%C3%A9/71792>

seulement « résister » aux attaques.

La sécurité a été définie<sup>9</sup> comme étant la « confiance de celui qui croit n'avoir aucun sujet

de crainte » ou un « état de tranquillité qui résulte de l'absence de danger ». Ce terme est issu du latin « *securitas* » et « *securus* », signifiant « exempt de soucis », comme le fait d'être « objectivement à l'abri du danger ». Alors, est-elle une réalité objective ou un état d'esprit ? Les sentiments et, en particulier, la confiance peuvent être une arme à double tranchant. D'une part, celle-ci est la clef pour développer l'écosystème numérique et d'autre part, une confiance excessive ou mal placée peut être très dangereuse.

S'il s'agit d'une situation plutôt objective ou bien d'un objectif à atteindre : comment peut-on garantir notre sécurité dans ce contexte difficile et à l'avenir ? C'est ici que nous pourrions penser à l'adaptation du concept de sécurité collective aux internautes ainsi qu'aux différents secteurs d'une société. La solidarité, le partage d'expériences, la répartition équitable des responsabilités et une volonté de protection mutuelle doivent fonder toute initiative sécuritaire. La cybercriminalité se propage lorsque les cyberattaquants s'organisent. Il serait donc intéressant de penser comme eux et de collaborer

entre nous, en tant que citoyens et cybercitoyens pour « booster » nos capacités.

La résilience est importante, certes, mais elle doit être notre dernier recours. La lutte contre l'emploi de l'ingénierie sociale à des fins illicites diffère de celle contre la COVID-19, dans le sens où il ne nous sera pas possible de trouver le vaccin qui va l'éradiquer. C'est pourquoi, nous devons toujours insister sur la prévention et sa détection précoce. Pour ce faire, trois piliers nous semblent nécessaires : l'éducation, l'utilisation positive d'ingénierie sociale et la coopération. Ce triptyque doit être synchronisé et exercé en continu, en reliant les aspects juridiques, techniques et sociaux. De cette manière, l'utilisateur ne sera pas qu'un facilitateur d'attaques mais aussi un atout pour notre sécurité.

## 2.1. Sans éducation la (cyber)sécurité demeurera une utopie

L'éducation est la base de toutes nos préconisations. Les risques liés aux usages d'Internet doivent être abordés dès l'école primaire. Il faut accélérer la prise de conscience et travailler sur le discernement des utilisateurs, surtout en ligne. La maîtrise des nouvelles technologies n'est pas synonyme d'une réelle compréhension des cybermenaces.

## 2.2. Pentesting : un usage positif de l'ingénierie sociale

Ces tests devraient être mis en place, de manière périodique, dans tous les



(10) Pentester est la contraction de « penetration test », test d'intrusion en français. Le rôle de ce professionnel de la sécurité informatique est de trouver toutes les failles de sécurité d'un système puis de procéder à des tests d'intrusion, autrement dit des attaques contrôlées grandeur nature.

organismes car ils nous aident à réfléchir comme un ingénieur social, en stimulant notre esprit critique, et à apprendre à gérer les crises. L'utilisateur doit se sentir encouragé à s'adapter aux outils et à travailler sur ses erreurs sans avoir été humilié ou pénalisé à cause de cela. L'employeur et la hiérarchie jouent ici un rôle central. Du côté du pentester<sup>10</sup>, il ne faut pas oublier la barrière légale et éthique qui le distinguera d'un cyberdélinquant.

### 2.3. L'initiative GILS : un exemple argentin de collaboration multidisciplinaire

Quant à la coopération, les partenariats sont fondamentaux. Le monde académique représente un terrain d'entente entre les différents secteurs car il s'agit d'une usine à idées et d'un espace de recrutement d'experts, d'une richesse capable de faire évoluer le marché, les technologies ainsi que l'ordre juridique et politique d'une société. Ici, nous pouvons trouver des réponses holistiques à notre phénomène transversal.

(11) Contact : gils@frlp.utn.edu.ar

Le Groupe de Recherche sur l'Ingénierie Sociale (GILS)<sup>11</sup> de l'Université

Technologique Nationale de La Plata, en Argentine, est né à partir de la constatation de la nécessité de réunir des spécialistes

pour aborder correctement ce sujet. Il a pour mission la structuration des échanges entre des hackers (dans le bon sens du terme), des experts en sécurité, des experts judiciaires, des psychologues, des criminologues, des avocats, des membres des forces de l'ordre, des ingénieurs en informatique, des RSSI, des professeurs et des chercheurs, afin d'étudier en profondeur l'ingénierie sociale et de proposer des recommandations. Le GILS participe à des manifestations académiques. Il offre des formations en interne, en externe et « s'auto-forme », car les formateurs sont à la fois instruits par leurs propres collègues, en fonction de leurs métiers. Parallèlement à ces activités, le GILS se divise en sous-groupes dédiés à des axes de recherche spécifiques et temporaires. En outre, les partenariats qui se développent avec des ONG et les forces de l'ordre favorisent la collaboration du groupe à des projets innovants, comme par exemple, le

concours au sein de l'Ekoparty Security Conference, dans lequel les participants s'engagent à chercher sur Internet des enfants disparus, en exploitant des informations obtenues à partir des techniques d'OSINT<sup>12</sup>.

(12) Le renseignement de sources ouvertes ou renseignement d'origine sources ouvertes (ROSO), (en anglais : open source intelligence, OSINT) est un renseignement obtenu par une source d'information publique.

### Conclusions et perspectives

Même si les États ont l'obligation d'assurer la sécurité de leurs citoyens, il n'est pas possible de faire abstraction du contexte actuel et de continuer de regarder ailleurs. Nous devons collaborer pour renforcer notre sécurité, en ligne et hors ligne. L'humain est vulnérable mais il n'est pas faible. La « nouvelle normalité » est aussi une source d'inspiration pour les ingénieurs sociaux. La crise que nous sommes en train d'affronter devrait donc constituer une opportunité pour que l'utilisateur puisse trouver la place qu'il mérite. En attendant, n'oublions pas que l'hygiène numérique et informationnelle sera toujours le meilleur geste barrière pour notre protection et celle de notre entourage.

### AUTEURE

**De nationalité argentine, Madame Denise Gross est avocate au barreau de La Plata. Elle est titulaire d'un Master II en « sécurité publique », obtenu à l'Université d'Auvergne et Docteur de droit pénal et sciences criminelles de l'Université de Strasbourg, après avoir soutenu sa thèse en 2019 intitulée : « L'ingénierie sociale : la prise en compte du facteur humain dans la cybercriminalité ». Parallèlement à ses études, elle a collaboré avec des ONG à Buenos Aires dans le cadre de campagnes de sensibilisation du public aux risques d'Internet. Actuellement, elle poursuit ses travaux sur cette thématique en tant que coordinatrice juridique du Groupe de Recherche sur l'Ingénierie Sociale de l'Université Technologique Nationale de La Plata.**

# La part humaine

## déterminante face aux crises majeures et son rôle dans la cybersécurité

Par Daniel Guinier

# L

Les grands systèmes, en particulier ceux du monde cyber sont complexes et ne sont pas exonérés de crises majeures. Si l'effet de sidération laisse dubitatif devant l'impensable pour les sceptiques, l'absurdité serait d'être persuadé que seul advient ce qui a été envisagé, alors que ces systèmes sont peu diversifiés et très interconnectés jusqu'au niveau mondial, introduisant la possibilité d'une crise majeure systémique. Il s'agit ici d'apporter une compréhension globale des phénomènes, d'exposer certains aspects de la part humaine et les conditions favorables à la maîtrise de telles crises.



DANIEL GUINIER

Docteur ès Sciences, Certifications CISSP, ISSMP, ISSAP et MBCI. Expert judiciaire honoraire.

**Caractéristiques des crises majeures et aspects théoriques**  
Les crises sont variées

(1) Avec les risques à grande échelle, la propagation est rapide du fait de réseaux, l'ubiquité du sinistre est constatable, l'impact est décuplé par l'interdépendance et la durée, auxquels s'ajoute une pénurie générale de matériels, d'équipements, de services, de compétences, etc.

en termes d'**origine** *naturelle, accidentelle, malveillante, erreurs, etc.*, de **secteur** : *cyber, santé, finances, politique, etc.*, d'**étendue localisée** ou à *grande échelle*<sup>1</sup> d'**impact** direct et indirect, plus ou moins grave, de **durée** *plus ou moins longue suivant plusieurs phases.*

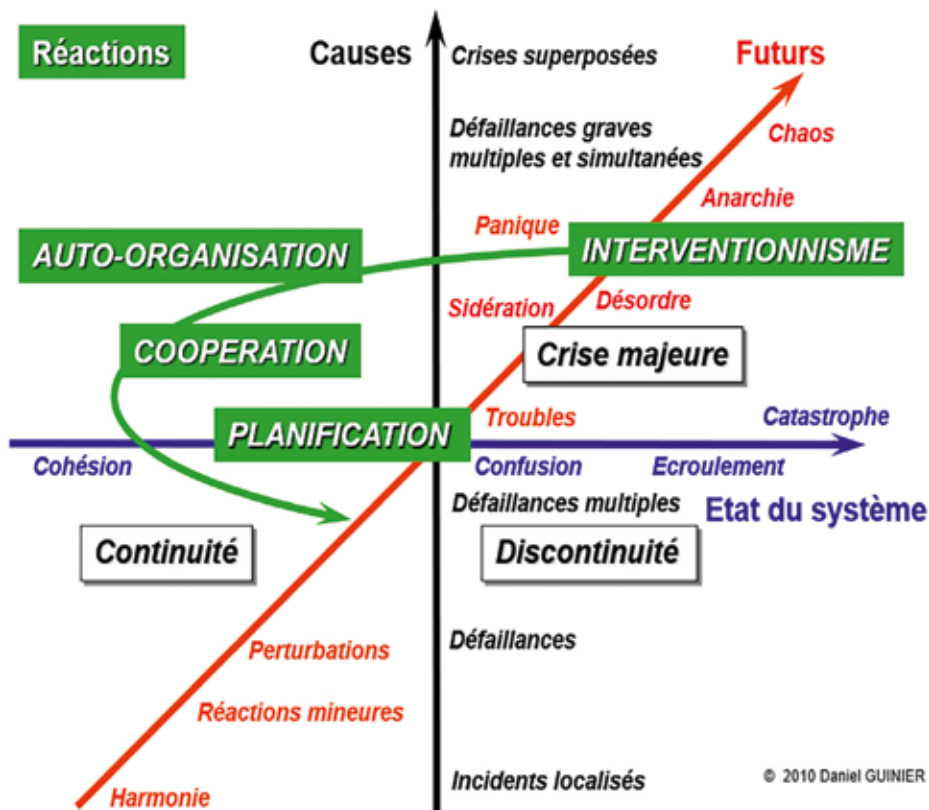
Leur caractère inattendu et brutal est associé à des scénarios jugés impensables ou à des conditions ignorées ou sous-estimées. En fait, **il existe des causes profondes** à cette situation. Certaines sont liées à l'imposture ou s'attachent à des aspects psychosociologiques, d'autres traitent de déficits, tandis que la survie impose d'avoir pris des dispositions pour s'adapter.

**Une crise majeure évoque une catastrophe ou un désastre** où les lieux et les infrastructures, les moyens matériels et les

données, les ressources humaines et les compétences, essentiels et vitaux, sont atteints ou manquants, conduisant à un sinistre majeur.

La figure suivante illustre la situation générale engendrée par différentes causes provoquant l'aboutissement du système

à la catastrophe et l'attachement à divers futurs conduisant au chaos. Elle indique de façon superposée les réactions, avec notamment la position centrale de la planification, l'importance de la coopération et de l'auto-organisation, jusqu'à l'interventionnisme des pouvoirs publics dans les cas extrêmes.



(2) La réponse est complexe en réalité, puisqu'il n'est pas possible de prévoir le moment de la transition à l'état critique, alors que cet état ne subsistait pas auparavant et que seuls les symptômes l'indiqueront, mais un peu tard...

(3) Le chaos résulte d'un comportement apparemment sans loi, mais pourtant gouverné par une loi propre aux systèmes dynamiques, lesquels, malgré des futurs apparemment déterminés, n'en restent pas moins imprédictibles après une légère variation. Ce phénomène relève de la «sensibilité aux conditions initiales».

## Les crises sont communément rattachées à plusieurs théories :

*théorie de l'état critique, du chaos, et des catastrophes*, laissant penser qu'elles ont un caractère plus prédictible qu'il n'y paraît. **L'état critique** est une propriété globale de la complexité des systèmes. Il résulte d'une évolution naturelle convergente vers un état surcritique pouvant engendrer des réactions en chaîne et aboutir à un désastre. Il est constatable par des symptômes, engendrés par la préexis-

tence de vulnérabilités et de fautes qui ont dégradé le système de façon non révélée, ou des incidents ou des signaux faibles non traités, ceci dans ses diverses composantes techniques, organisationnelles ou humaines. Un tel état critique nécessite des mesures conjointes pour rendre le système sous-critique<sup>2</sup> afin d'en reprendre le contrôle effectif et permettre le retour une situation normale. Selon **la théorie du chaos**<sup>3</sup>, il faudrait veiller aux conditions initiales et éliminer la corrélation entre la dynamique et les événements passés, pour espérer plus de prévisibilité. À son tour, **la théorie des catastrophes** indique la nécessité d'éviter une bifurcation abrupte en agissant sur les paramètres de contrôle *criticité* et *dépendance*,

qui gouvernent le comportement du système, pour le maintenir dans un état métastable et éviter de l'entraîner vers une catastrophe.

Il s'en dégage des dispositions qui s'imposent à **l'évitement des crises**. Elles sont liées à la prévention et à la sûreté, à la réduction de la complexité et à la recherche d'étanchéité pour éviter la propagation et les réactions en chaîne. D'autres concernent **la protection** pour en réduire l'impact et assurer la continuité des affaires.

## La part humaine individuelle paradoxale

L'homme peut être **le meilleur comme le pire** des constituants de la cybersécurité du fait des conséquences de son fonctionnement cognitif et psychologique.

**L'homme est le maillon faible** quand la baisse des performances liée à la fatigue, à des pressions excessives et au déclin de vigilance augmente le risque d'erreurs. Celles qui sont issues de sa pensée intuitive et émotionnelle peuvent être utilisées à son encontre, **comme dans la majorité des cyberattaques**, en tirant profit de la manipulation et de l'ingénierie sociale pour susciter des réponses quasi-immédiates, en jouant sur des leviers d'influence pour le faire opérer de façon automatique et sur des biais cognitifs pour l'entraîner dans des défauts de jugement. À ceci peuvent s'ajouter des caractéristiques psychologiques : *difficultés*

*à communiquer, à admettre et à signaler ses erreurs, résistance au changement, etc.* Enfin, lors d'une crise brutale, la perte de repères et le stress auxquels il est soumis entraînent un état de démotivation, voire de sidération durable de plusieurs jours sans réaction.

**L'homme sera cependant le meilleur** quand il dispose d'une richesse informationnelle inégalée par sa connaissance et sa familiarité avec le milieu. Il peut être en mesure de faire face à des situations exceptionnelles, à condition de bénéficier d'une formation et d'un entraînement adéquats, de procédures opérationnelles, d'aides techniques pour l'orienter vers la recherche et la mise en œuvre d'une solution. Il est aussi un excellent régulateur face à des situations inédites, pour trancher et juger dans l'incertitude extrême, montrant des possibilités de diagnostic parfois supérieures à celles attendues. Pour finir, lors d'une crise, il est en mesure de réapprendre rapidement, de s'adapter et de développer une capacité d'ingéniosité et de création, à condition toutefois d'être suffisamment motivé. Les capacités humaines de dépassement et d'adhésion ont été pleinement démontrées face à la crise majeure inédite à très grande échelle engendrée par la pandémie de la Covid-19.

### **L'imposture humaine et les déficits chroniques dans les organismes**

**L'imposture** relève d'une image moins

brillante qu'il n'y paraît, privilégiant la réputation avant les compétences et la forme plutôt que le fond, obligeant à déguiser la réalité dans un esprit compétitif. En contrepartie, elle développe du stress et des angoisses. Il lui correspond celle des hommes qui tenteront de donner une image d'eux-mêmes aussi parfaite que possible. Elle s'exercera avec d'autant plus de succès que l'organisme est fragilisé par une perte de sens. Ceci participe autant à la genèse de la crise qu'à l'impréparation pour y faire face. Concernant les divers niveaux de responsabilités : *direction, cadres et personnels informatiques*, une étude d'envergure montre que ni l'intelligence émotionnelle, ni l'honnêteté n'apparaissent essentielles pour la réussite professionnelle.

**Les déficits chroniques** sont vus comme des points communs d'engendrement de catastrophes. Leur caractère pathologique est en rapport avec la faiblesse intrinsèque des systèmes et de leur résilience pour la poursuite de l'activité en cas de sinistre ou suite à des cyberattaques d'envergure généralisées. Ils se retrouvent bien souvent avec plus d'ampleur dans les organismes de petite taille.

**Les déficits culturels** se rapportent à **l'infailibilité** (*l'organisme pense ne pas avoir été victime de cyberattaque*), au **simplisme** (*le système d'information est considéré comme peu complexe et le recours à des méthodes comme*

*improductif*, et au **nombrilisme** (*aucune remise en question et peu d'ouverture vers l'extérieur*). **Les déficits managériaux** se réfèrent à l'**ignorance** (*peu d'attention portée aux incidents précurseurs, et il n'existe ni veille, ni formation en sécurité*), au **désengagement** (*pas de sensibilisation et aucune politique de sécurité*), et à l'**absence de planification** (*aucun plan de continuité d'activité et pas de procédures d'urgence*). **Les déficits organisationnels** concernent la **subordination** (*la fonction sécurité est placée sous l'autorité de l'informatique*), la **dilution** (*l'action spontanée est privilégiée de façon informelle*), et la **rigidité** (*la structure actuelle est considérée comme satisfaisante et une fonction sécurité serait vue comme une source de désordre*).

C'est dans ce cadre que s'exprime la dynamique du risque jusqu'à l'état de crise majeure ou de catastrophe.

**Il importe de les identifier pour les corriger et disposer d'un contexte favorable rendant compte des activités humaines**, dans leur conduite comme dans la façon dont elles sont organisées et contrôlées. Ainsi, les dimensions humaines, organisationnelles et technologiques sont concernées, impliquant des mesures complémentaires visant à réduire l'occurrence des risques et à en **limiter l'impact sur les affaires**, notamment **quand survient une crise majeure de toute nature** attachée à un système brutalement dégradé, possiblement dans la durée. Une politique

de sécurité et des plans formels sont attendus pour la survie des organismes.

### La nécessaire planification et l'adhésion de l'humain

**Un plan de continuité d'activité** (PCA) décrira la poursuite des opérations essentielles sans aucune interruption, avec une **vision globale d'un organisme entier**, tandis qu'une solution de secours s'inscrira seulement dans une vision restreinte purement technique. Ses objectifs sont de pouvoir **répondre à une situation catastrophique et de maintenir ou reprendre les processus d'affaires** au vu de délais privilégiant le plus critiques. **Le PCA sera conçu selon une démarche méthodique** comportant plusieurs étapes, visant à établir des exigences structurées en termes de fonctionnalités, *pour la couverture des objectifs*, et d'assurance, *pour la confiance à satisfaire ces objectifs*, **en s'appuyant sur les normes en vigueur<sup>4</sup>**.

(4) La suite de normes ISO 22301, en particulier.

**Il sera exécuté selon les plans d'actions et procédures établis**, testés, mis à jour et validés, conformément aux exigences actualisées. Des changements, justifiés par la situation, pourront cependant être accordés après examen et sous la responsabilité de la cellule de crise.

**Depuis plusieurs décennies, malgré les incitations** à s'intéresser davantage à « *la part de l'homme* », l'impact

(5) 10 % après une conférence, 30 % après une démonstration, elle peut atteindre 75 % par la pratique et jusqu'à 90 % suite à une implication personnelle dans un fait marquant, selon le National Training Laboratory (Bethel).

(6) Les personnels innovants et demandeurs, peu nombreux, seront moteurs pour former une majorité précoce avec les optimistes et servir de leaders et de relais pour inciter les suiveurs silencieux et ainsi constituer une majorité plus apte à convaincre les pessimistes qui ont une vision plutôt négative du changement qui leur paraît être une pression. Il restera enfin à traiter la partie minoritaire des résistants qui suspectent le changement, le considérant comme une menace.

des campagnes de sensibilisation apparaît insuffisant<sup>5</sup> malgré les efforts consentis. Il s'agit donc de couvrir le facteur humain en développant **une pédagogie interactive ciblée, innovante et créative pour capter l'attention**, ce qui nécessite avant tout **le ralliement de tous** en prenant en compte la diversité des attitudes et la résistance au changement dans les organismes. Après l'établissement d'une politique et des décisions au plus haut niveau il importe de rechercher **l'adhésion par basculement majoritaire** à partir d'un seuil critique de groupes favorables<sup>6</sup>, pour bénéficier de comportements positifs

durables, soutenus par des exercices et des contrôles, en insistant sur l'implication et l'interdisciplinarité au vu de la **variété des acteurs et des risques métiers**.

### En conclusion,

une gestion des ressources humaines adaptée devrait permettre l'application d'une politique de sécurité prenant mieux

en compte « *la part de l'homme* », **pour développer une culture** respectueuse des mesures humaines, organisationnelles, procédurales et techniques, de façon à garantir au mieux **la cybersécurité, l'évitement et la maîtrise des crises** de toute nature. **La perspective** se trouve signifiée dans la littérature : « *Les germes de la crise étaient là. On eût pu en distinguer la présence...* » (André SIEGFRIED, *L'âme des peuples*). « *Puis, la crise avait fini par les atteindre directement. L'un perdit son emploi ... un autre claquait des dents et touchait du bois* » (Marcel AYMÉ, *Maison basse*). Elle est attachée à la **capacité d'adaptation** résultant de la prise en compte de la **globalité des risques et des liens entre les systèmes**. Elle relève aussi de la **superposition de crises**, figurant une possible catastrophe, et la nécessité d'une remise en question profonde, avec **plus d'humilité et moins de certitudes** que par le passé, dont il devrait être tiré les leçons pour éviter de subir un désastre.



## Bibliographie sélective

- Bruns H. et al., 2018. Can Nudges Be Transparent and Yet Effective? *J of Economic Psychology*. vol. 65, avril, pp.41-59.
- Guinier D., 1994. Oriented-scenario dynamics in information systems safety. Introduction to propagation paths, channels of risk and «revulsion momentum», *ACM Sigsac*, vol.12, n° 3, pp.6-11.
- Guinier D., 1995. Development of a specific criminology dedicated to information technologies, 7th Ann. CITSS, Ottawa, 16-19 mai, pp. 21-45.
- Guinier D., 1995. Catastrophe et management - Plans d'urgence et continuité des systèmes d'information, Ed. Masson, 339 pages.
- Guinier D., 1997. Application of Chaos Theory to the management of security development - Finding a conciliatory position for improving information system security in an organism, *Proc. 9th Ann. CITSS*, Ottawa, 12-16 mai, pp. 383-400.
- Guinier D., 2002. Systèmes d'information : état critique et désastre - Dispositions essentielles mises en évidence par les apports théoriques, *Expertises*, n° 263, octobre, pp.341-344.
- Guinier D., 2006. In l'encyclopédie de l'informatique et des systèmes d'information - La politique de sécurité, pp. 1486-1498. Vuibert Sciences.
- Guinier D., 2007. PRA/PCA : une obligation légale pour certains et un impératif pour tous. *Legalis.net*, Edition des Parques, n° 2, juin, pp. 5-18.
- Guinier D., 2009. Face à une pandémie annoncée et à la crise suivante... - Réponses pour la continuité de l'activité des entreprises *Expertises*, n° 340, octobre, pp.337-342.
- Guinier D., 2016. Cyberattaques et catastrophes : de l'imposture et autres causes à la sidération des entreprises. *Expertises*, n° 418, novembre, pp. 371-376.
- Guinier D., 2018. Modèle de représentation des cyberattaques, mesures génériques et prospective. *La revue juridique Dalloz IP/IT*, mars, pp. 163-169. Article ayant obtenu le Prix de la Gendarmerie nationale 2019 - Recherche et réflexion stratégique.
- Guinier D., 2020. La crise suivante est bien là ! Premières leçons de cette nouvelle pandémie de Covid-19 et aide possible des technologies numériques. *Expertises*, n° 457, mai, pp. 177-182.

- Kahneman D., 2012. Système 1 / Système 2 : Les deux vitesses de la pensée, Flammarion, Essais, 545 pages.
- Kappelman L. et al., 2016. Skills for success at different stages of a IT professional's career. Communications ACM, vol. 59, n°8, pp. 84-70.
- Kervern G.Y. et Rubise P., 1991. L'Archipel du danger : introduction aux cindyniques, Economica, 460 pages.
- Kets de Vries M.F.R., 2010. La face cachée du leadership. 2° Ed., Pearson, 346 pages.
- Perrow C., 2007. The next catastrophe – Reducing our vulnerabilities to natural, industrial, and terrorist disasters. Princeton Press, 377 pages.

## AUTEUR

**Daniel Guinier est Docteur ès sciences, certifié CISSP, ISSMP, ISSAP en sécurité des SI, et MBCI en continuité et gestion des crises.**

**Il est expert de justice honoraire et consultant en politiques et stratégies de cybercriminalité et de cybersécurité pour le Conseil de l'Europe et l'UE, après avoir été expert en cybercriminalité devant la Cour pénale internationale de La Haye. Chargé de cours universitaires et auprès de grandes écoles, il a partagé sa carrière entre le CNRS et comme PDG d'une société spécialisée en SSI et entre temps a été professeur à la US Naval Postgraduate School. Il est l'auteur de très nombreux articles et de plusieurs ouvrages précurseurs, dont « Sécurité et qualité des SI - Approche systémique - La part de l'homme » en 1991, et « Catastrophe et management - Plans d'urgence et continuité des SI » en 1995, édités par Masson.**

**Il est colonel (RC) de la gendarmerie nationale, en Alsace, chargé du Forum du Rhin supérieur sur les Cybermenaces de 2009 à 2013.**

# Culture de la sécurité

et expérience des FHO  
dans les industries à risques

Par Marc-Xavier Joubert, Robert Breedstraet et Stéphane Deharvengt

L

L'organisation et le déploiement de la cybersécurité sont confrontés aux mêmes problématiques rencontrées au cours des dernières décennies dans les domaines de la sécurité des vols, de la sûreté nucléaire ou encore de la sécurité industrielle. Tous les Responsables de la Sécurité des Systèmes d'Information pourraient témoigner de la difficile éva-

luation coût-bénéfice de la sécurité, du défi que représente le compromis entre sécurité et disponibilité informatique, mais également de l'importance du fameux « facteur humain » ou de la nécessaire implication du « top management » ...

Les professionnels de la sécurité industrielle voient ici un écho aux mêmes défis qu'ils affrontent depuis des dizaines d'année. Pour dépasser la vision technique et procédurale de la sécurité, l'industrie (aéronautique, ferroviaire, nucléaire, chimique...) a étudié en profondeur les Facteurs Humains et Organisationnels (FHO) et le concept de culture de sécurité nécessaires à l'émergence et au maintien d'un niveau acceptable de sécurité. Quels enseignements pourrait-on donc tirer du management de la sécurité dans ces



**MARC-XAVIER  
JOUBERT**

Président de Suez  
Advanced Fire  
Engineering.



**ROBERT  
BREEDSTRAET**

Division information  
security officer.  
Adjoint au Corporate  
CISO d'Amadeus  
IT Group.



**STÉPHANE  
DEHARVENGT**

Adjoint chef  
de mission sécurité,  
sûreté, qualité  
du contrôle aérien  
français. Direction  
des Services  
de la Navigation  
Aérienne. DGAC.

industries à risques pour construire des cultures de cybersécurité adaptées aux défis de la métamorphose numérique de nos sociétés ?

Les professionnels de la cybersécurité et leurs managers devraient aller puiser dans cette ressource académique, scientifique et expérimentale pour en dégager les lignes directrices utiles au déploiement efficace de leurs politiques de sécurité et les adapter au contexte particulier de la menace cyber et de sa dimension intentionnelle. Nous ne traiterons pas ici de la manière dont ces industries intègrent les risques cyber. Nous irons plutôt explorer les concepts clefs qui ont permis d'atteindre un haut degré de sécurité de fonctionnement dans ces secteurs, puis nous qualifierons plus précisément la menace cyber et évoquerons les spécificités d'une culture de cybersécurité.

### Un regard « Facteurs Humains et Organisationnels » sur la sécurité

*« Les FHO [...] doivent aujourd'hui permettre d'élaborer une logique de sécurité, avec des normes bien sûr, mais aussi la prise en compte de la variation des conditions réelles et donc l'existence d'une sécurité gérée, ajustée par l'intelligence des hommes. »*  
(Amalberti and Boissières 2014).

Les Facteurs Humains et Organisationnels expriment une tension entre deux acteurs de la gestion de la sécurité, les humains et les organisations humaines, qui doivent

s'articuler autour d'une stratégie permettant de faire face à la variabilité des processus maîtrisés.

### Le rôle de l'humain dans la gestion de la sécurité

L'humain intervient partout, qu'il soit acteur de première ligne (pilote ou manipulateur) ou acteur de l'entreprise (compagnie aérienne, site industriel, concepteur...). L'entreprise est une organisation humaine faite de processus managériaux et industriels, d'outils technologiques plus ou moins complexes et d'acteurs avec leurs compétences respectives. On retrouve bien sûr en cybersécurité les mêmes composantes procédurales (méthode AGILE, règles de codage...), technologiques (software et hardware) et humaines (développeur, concepteur, pentesteur...).

La question de l'erreur humaine est indissociable de l'histoire de la sécurité dans les industries à risques. Pour de multiples raisons - biais d'attribution rétrospectif, recherche d'un coupable - l'humain garde souvent le mauvais rôle dans les récits d'accidents alors que la plupart du temps, il est le facteur de sécurisation et de rattrapage qui rend ces systèmes techniques aussi sûrs. L'erreur peut être vue soit comme la cause d'un problème, soit comme le symptôme d'un souci plus profond (Dekker 2000). On retrouve également cette vision dans le domaine de la cybersécurité.



Afin de dépasser ce vieux débat, il faut prendre de la hauteur et s'interroger sur les mécanismes qui créent la sécurité ou la cybersécurité.

### Les compromis des stratégies de sécurité

La tension entre humain et organisation se traduit concrètement par deux manières de gérer la sécurité, complémentaires et interdépendantes (Groupe de travail de l'Icsi « Culture de sécurité » 2017).

**La « Sécurité Gérée »** repose sur la compétence des acteurs, cette compétence étant un facteur de résilience du fait de leur forte adaptabilité. On a pu en voir un exemple très récent dans la crise sanitaire de 2020 lorsque les soignants ont réorganisé des services entiers des hôpitaux. Cependant le niveau de sécurité obtenu est peu élevé, puisqu'il s'agit de réagir dans l'urgence, sans plan bien préparé.

**La « Sécurité Réglée »** repose sur la prévision et le management des situations à risques, voire à les éviter si les conditions de sécurité ne sont pas remplies : un pilote peut décider de ne pas décoller ou d'aller atterrir ailleurs si les conditions techniques ou météorologiques ne rentrent pas dans des limites acceptables. Le système est très robuste mais il est peu adaptatif en cas de choc imprévisible : il s'arrête dans ce cas. Il en résulte un très haut niveau de sécurité – on les appelle de systèmes ultra-sûrs (nucléaire, aviation civile).

Chaque domaine possède ainsi ses stratégies, ses palettes d'actions, qui résultent de compromis stratégiques, de nature économique, de niveau de sécurité, et d'acceptabilité sociale. (Amalberti 2013). En fonction des domaines dans lesquelles elle va s'appliquer, la cybersécurité repose sur des choix plus ou moins explicites en fonction des stratégies de l'entreprise : c'est la logique portée en particulier par la Loi de Programmation Militaire sur la protection des Opérateurs d'Importance Vitale de certaines industries (avec en deuxième rideau des opérateurs de services essentiels), en leur demandant l'identification de leurs systèmes d'importance vitale (tous les systèmes ne concourent pas aux fonctions essentielles) puis en leur appliquant des règles de sécurisation au niveau adéquat.

Mais alors, comment qualifier la sécurité

ou la cybersécurité d'un système ?

### **Qu'est-ce qu'être sûr ou en (cyber) sécurité ?**

En écho à cette dualité sécurité gérée et sécurité réglée, l'état de sécurité peut être envisagé sous deux angles : statique et dynamique. Sous l'angle statique, la sécurité est comme un stock qui se caractérise par l'absence d'accident. Elle est un fait objectif constaté par des experts qui analysent la situation de façon rétrospective (« jusqu'à présent tout va bien »). L'effet pervers de cette approche est qu'elle peut conduire à rechercher l'élimination des imprévus (réduction de la probabilité des événements redoutés), à considérer l'homme comme le maillon faible faisant des erreurs et, *in fine*, à renforcer la bureaucratie.

Sous l'angle dynamique, la sécurité est un processus et se caractérise par la somme des accidents évités. Il s'agit d'une construction permanente qui se traduit davantage par un ressenti de sécurité. Dans ce cadre, la sécurité est orientée pour que l'organisation soit capable de faire face à l'imprévu, en s'appuyant sur les hommes comme ressource pour rattraper les variabilités du système et du contexte. Il serait toutefois vain d'opposer ces deux visions qui, au contraire, doivent dialoguer au sein de l'organisation. En médecine, la santé est une propriété émergente, qualifiée par différents signes physiologiques et indicateurs relatifs à la qualité de vie. Dans les processus industriels, la sécurité

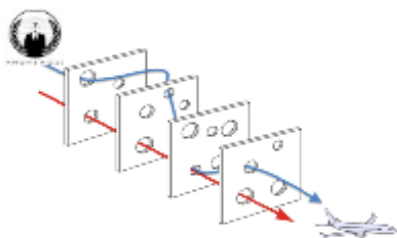
est également mesurée par divers indicateurs et constats (Reason 1995). La cybersécurité en tant qu'état du système d'information que l'on peut caractériser et mesurer est donc également une propriété émergente de l'interaction entre les acteurs, les processus et les techniques.

Ainsi, la cybersécurité serait un état du système sociotechnique : on « est en cybersécurité », c'est-à-dire que l'on a mis toutes les barrières humaines et techniques nécessaires pour s'assurer que les dangers sont maîtrisés à un niveau acceptable, dépendant de compromis stratégiques sociotechniques.

Cette notion de maîtrise demande à être explicitée. Dans le cadre des systèmes de management, il est demandé de se donner des objectifs de sécurité, d'identifier les dangers et les manières de les maîtriser ou de les atténuer, puis d'effectuer le suivi de la performance en analysant les accidents ou incidents et d'améliorer le système si besoin (Paries, Macchi et al. 2018). La partie la plus difficile concerne souvent l'identification des dangers ou des menaces sur le système : on ne peut évidemment pas tout prévoir, en particulier dans le domaine cyber où la menace revêt des caractéristiques singulières.

### **La nature particulière de la menace cyber**

Cependant, la cybersécurité introduit la gestion d'un processus particulier qui est celui de la protection contre une attaque, avec en arrière-plan une intentionnalité malveillante, celle de l'attaquant. Cette dimension demande une réflexion dépassant



les cas classiques de gestion de probabilité de pannes ou de dégradation des conditions opérationnelles.

### Les trous du cyber-gruyère

Les industries à risques tentent de maîtriser les vulnérabilités (les trous) dans les différentes barrières de protection mises en place (règlements, formations, conception, procédures...). En évitant qu'une succession de problèmes survienne, on casse la chaîne accidentelle. C'est le principe du modèle de Reason (Swiss Cheese). (Reason 1997).

Lors d'une attaque de type cyber, l'attaquant, doué d'une intelligence, va tenter de créer des trous dans les défenses ou d'exploiter ceux qui existent déjà pour

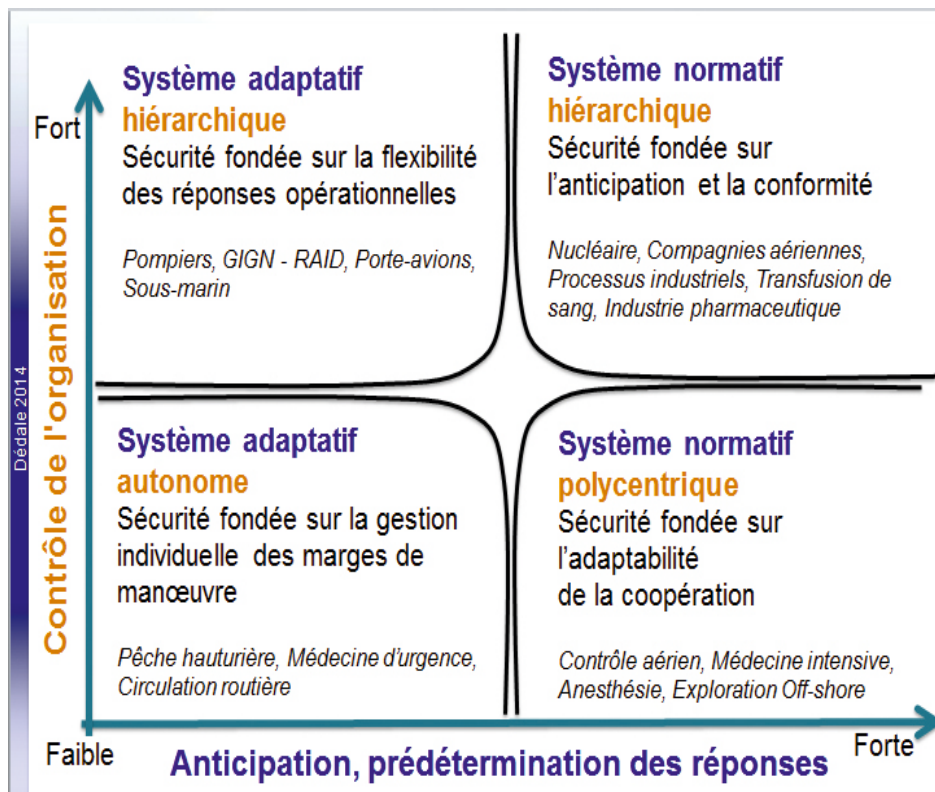
tracer son chemin d'attaque. La différence réside ici dans l'intentionnalité de la menace.

Dans les analyses de risques (sécurité industrielle ou sécurité des biens et des personnes), l'intention des intervenants est d'éviter l'accident pour mener à bien la mission, c'est-à-dire produire avec un niveau de qualité déterminé ou amener des passagers d'un point A à un point B en toute sécurité. Sur ce chemin, des erreurs, des omissions peuvent se produire, parfois même des violations de procédure mais l'intention est de bien faire son travail. Sauf si on est un terroriste, on ne se lève pas le matin en se disant qu'on va provoquer un accident industriel.

Dans un contexte de cybersécurité, on assiste à l'affrontement entre deux intentions, l'une en charge du fonctionnement du Système d'Information, parfois génératrice d'erreur ou d'incidents, l'autre animée d'une intention malveillante, cherchant parfois à provoquer l'accident redouté ou, tout au moins, à profondément perturber le fonctionnement normal.

### Des menaces et des organisations

En fonction de la précision de la connaissance de la menace, les industries à risques ont développé des modes de gestion de la sécurité adaptés. Le schéma suivant présente sur l'axe horizontal la connaissance formelle des situations à risques, l'axe vertical les capacités de contrôle des organisations



opérant dans ces situations. Plusieurs exemples illustrent ces concepts.

### Quel positionnement de la Cybersécurité ?

Il existe de nombreuses motivations à construire un système intégré de management de la cybersécurité.

D'abord, cela permet de sauver du temps et de l'énergie. On bénéficie ainsi de l'expérience et des leçons apprises par les autres entreprises, en construisant un langage et une terminologie communs.

Pour des raisons de responsabilité, de visibilité et de conformité, on peut ainsi prouver que la cybersécurité est rigoureusement gérée et on peut fournir



les indicateurs qui le prouvent. On utilise des composants renouvelables : des stratégies, des standards de sécurité et des objectifs de cybersécurité communs à toutes les strates de l'entreprise. Cela garantit des processus de cybersécurité stables basés sur des méthodologies établies. Tout cela permet de bâtir une défense en profondeur et de faire travailler

tout l'écosystème de l'entreprise à l'amélioration constante de la cybersécurité.

Un système intégré de management de la sécurité permet de relier le cadre stratégique de la cybersécurité, les catalogues des contrôles et le bon fonctionnement des processus critiques de cybersécurité, c'est-à-dire :

### Relations entre « frameworks », contrôles et processus



Sources : ISO, NIST et Gartner



la gouvernance, la gestion des règles (« policies management »), l'information et la formation à la cybersécurité, le management des vulnérabilités, le management des identités et de leurs accès ainsi que la gestion des incidents.

Il est évident qu'une gestion rigoureuse de ces processus est une manière fiable de réduire les risques liés à la digitalisation des entreprises tout en s'assurant que l'humain œuvrera à plus de sécurité et cela grâce aux contrôles mis en place.

Ces aspects sont familiers aux RSSI qui déploient ces structures au sein de leurs entreprises afin de remplir leur rôle de détection, de réaction, et in fine de protection des systèmes d'information. On retrouve ainsi les mêmes composantes organisationnelles et techniques qui fondent la stratégie de sécurité des systèmes à risques. Sur ces points, les organisations devraient s'inspirer des acteurs plus avancés tel que le secteur bancaire, déjà très expérimenté en matière de sécurisation des transactions financières.

Cependant, la composante essentielle sera toujours la partie humaine du système sociotechnique que l'on abordera sous l'angle de la culture de cybersécurité.

### Construire la culture de cybersécurité

*"Few things are so sought after and yet so little understood."*(Reason 1997). La culture de sécurité est un concept scientifique difficile à appréhender. Mais elle peut se construire en cybersécurité de la même manière que dans la sécurité industrielle.

Il faut pour la cybersécurité un complet changement de paradigme. Tant qu'elle sera vue comme un simple problème que des techniciens peuvent solutionner avec des outils techniques, on n'arrivera pas à construire une culture de la cybersécurité digne de ce nom. Construire cette culture est très probablement le plus grand changement des entreprises pour la prochaine décennie. Il est nécessaire d'introduire la cyber au centre même du business.

Sans une intégration poussée par le sommet de la hiérarchie et avec tout le soutien des comités exécutifs, un tel changement ne sera pas possible. Nos dirigeants doivent prendre la responsabilité de comprendre et d'adapter la culture de leur entreprise afin d'y inclure de bon niveau de réflexes de cybersécurité. La mise en place d'une stratégie et d'un cadre sécuritaire (ISO27K ou NIST) en sera la conséquence

logique.

L'Institut pour une Culture de Sécurité Industrielle (ICSI) a défini les 7 attributs d'une culture de sécurité intégrée. Comme nous pouvons le voir ci-dessous, ceux-ci sont facilement transposables dans un contexte cybersécurité :

1. Conscience partagée des risques les plus importants,
2. Culture interrogative,
3. Culture intégrée, mobilisation de tous,
4. Équilibre pertinent entre le réglé et le géré,
5. Attention permanente aux trois piliers (technique, système de management, FHO),
6. Leadership du management et implication des salariés,
7. Culture de la transparence afin de générer la confiance.

Bien qu'il nous paraisse évident de cultiver la transparence et de partager les renseignements que nous possédons, il est encore difficile pour une entreprise d'admettre qu'elle a subi une attaque cyber ou bien d'évoquer ses vulnérabilités.

Il est donc délicat d'instituer cette culture

de la transparence mais nous pouvons et devons faciliter le partage des informations et des renseignements. De nombreux forums ont déjà été ou sont en train d'être mis en place pour ce faire : les États européens à travers leurs agences de sécurité informatique mettent en place des réseaux de CERT (« Computer Emergency Response Team ») qui œuvrent en ce sens, des regroupements sectoriels se sont créés, notamment aux États-Unis. Ils permettent de partager les indices de compromission et aident ainsi collectivement à améliorer le niveau de protection de ceux qui acceptent ce partage et donc ce niveau de transparence.

On apprend de nos erreurs : pour anticiper, pour améliorer les connaissances sur la menace, pour développer des procédures robustes. Au niveau d'une entreprise, il faut donc connaître la vie de tous les jours et les différences entre ce qui est prescrit et ce qui réellement réalisé. Les acteurs de terrain doivent avoir suffisamment confiance pour reporter les événements sans craindre de sanction en retour.

Toutefois, l'idée de sanction, déjà délicate dans le domaine de la sécurité industrielle, paraît encore plus difficile en contexte cyber : comment distinguer l'erreur de la faute, face à une menace qu'on ne comprend pas ou que l'on n'a pas détectée ?

Lors de la conception de la formation à la culture sécurité délivrée en 2020 à l'en-

semble des agents du contrôle aérien français, la mention du signalement d'évènement à caractère cyber a été mentionnée. Même si la notion de signalement d'évènement sécurité est très ancienne et ancrée dans les mœurs, tout particulièrement chez les contrôleurs aériens, la modernisation croissante des systèmes de navigation aérienne nécessite d'étendre cette culture du report. Celle-ci permet également de toucher les acteurs « non-opérationnels ».

### Se préparer à la crise : résilience et construction du sens

La menace cyber fait peser un risque bien plus grand (tant en probabilité qu'en étendue) de crises majeures touchant l'ensemble d'une organisation. Les attributs clefs de cette culture de sécurité doivent donc être complétés par une meilleure préparation à la crise afin de rendre les organisations plus résilientes.

D'après Erik Hollnagel (Hollnagel, Pariès et al. 2010), une organisation résiliente arrive à maintenir en permanence la situation sous contrôle, qu'elle soit prévue ou imprévue. Cela revient à s'interroger en permanence autour de deux questions fondamentales : Qu'est ce qui fait perdre le contrôle ? Comment maintenir ou regagner le contrôle ? Il définit ainsi quatre attitudes clés qui doivent être entretenues dans les organisations et qui font échos aux concepts abordés précédemment :

1. Apprentissage : connaître le passé (faits

objectifs et structurés) diffusé au travers d'un REX (Retour d'expérience) analysé et partagé ;

2. Réponse : savoir quoi faire et savoir le faire, notamment par des procédures réellement opérationnelles et connues ;
3. Monitoring : savoir quoi chercher (ce qui est critique) et le mesurer par des indicateurs prospectifs ;
4. Anticipation : savoir à quoi s'attendre (potentiels et scénarios) y compris l'impensable.

En complément, Karl Weick (Vidaillet 2003), au travers de l'analyse de la catastrophe de Mann Gulch nous éclaire sur quatre dimensions de la souplesse organisationnelle qui augmentent la résilience :

1. La capacité à improviser et à bricoler de nouvelles solutions, même sous la pression. Ceci sous-entend l'entretien d'une forme de créativité et de capacité d'initiative en dehors des phases de crise,
2. Un système de rôles à tenir, partagé entre les acteurs de l'organisation, qui permet à chacun de savoir quels rôles doivent être tenus en toutes circonstances (exemple : le chef, le secrétaire, le communicant...), même lorsqu'on est seul,

3. Une attitude de sagesse, comprise comme la capacité à prendre en permanence de la distance vis-à-vis de ses croyances, de ses certitudes et de sa propre confiance,
4. L'entretien de relations respectueuses entre les acteurs qui permettent d'être à l'écoute de solutions nouvelles, d'accepter en confiance la répartition des rôles.

### Conclusion

Sans vouloir imposer un point de vue extérieur, la communauté cyber pourrait bénéficier d'un échange approfondi avec la communauté de la sécurité industrielle. D'un côté, ce que les sciences sociales dans les industries à risque nous disent : reconsidérer l'humain comme un élément de sécurisation du système et d'adaptation aux imprévus, des choix stratégiques et tactiques portant sur les caractéristiques des défenses mises en œuvre. De l'autre, ce que la déclinaison des théories actuelles en sécurité apporte au vu des spécificités des systèmes d'information : une intentionnalité malveillante, les caractéristiques de la résilience organisationnelle en réponse à une cyberattaque. Cet échange pourrait se concrétiser par le déploiement d'une culture de cybersécurité maîtrisée permettant d'atteindre un état de cybersécurité acceptable. En particulier, la transparence dans le report d'événement et le partage d'information suite à une analyse, valeur primordiale pour la culture sécurité,

devraient pouvoir trouver son expression dans une culture de cybersécurité.

Ce cheminement demande des efforts de la part des décideurs pour prendre en compte une réalité qui est loin d'être simple mais que ces connaissances et pratiques permettent d'éclairer. Cette dimension des enjeux de la transformation numérique ne doit pas être sous-estimée, en particulier si l'on veut responsabiliser les acteurs de terrains, adapter les espaces de travail, et construire la confiance qui sous-tend toute transformation. Quant au chemin de croix des RSSI, qu'il s'agisse de ressources, de budget, de compétences, d'arbitrages, de responsabilités, d'accès aux décideurs, il n'est pas sans rappeler celui du Directeur Sécurité. La prévention a souvent le mauvais rôle par rapport aux enjeux opérationnels immédiats, mais elle sera toujours plus payante qu'un accident ou une crise cyber majeure qui paralysera l'entreprise et affectera durablement son image.

## Bibliographie

Amalberti, R., Ed. (2013). Navigating Safety, Necessary compromises and trade-offs, Theory and Practice. Berlin, Springer.

Amalberti, R. (2017). « Les FHO dans l'entreprise : trois rails éclatés ? » Tribunes de la Sécurité Industrielle 1: 5.

Amalberti, R. and I. Boissières (2014). Interviews croisées. 6ème assises

nationales des risques technologiques - Le Journal.

Dekker, S. W. A. (2000). The Field Guide to Human Error, Ashgate.

Groupe de travail de l'Icsi « Culture de sécurité » (2017). La culture de sécurité. Comprendre pour agir. Cahiers de la Sécurité Industrielle. D. Besnard, I. Boissières, F. Daniellou and J. Villena. Toulouse, France, Institut pour une Culture de Sécurité Industrielle. Numéro 2017-01.

Hollnagel, E., J. Pariès, et al. (2010). Resilience Engineering in Practice: A Guidebook, Ashgate Publishing, Ltd.

Pariès, J., L. Macchi, et al. (2018). « Comparing HROs and RE in the light of safety management systems. » Safety Science.

Reason, J. (1995). « Safety in the operating theatre. Part 2: Human error and organizational failure. » Current Anaesthesia and Critical Care 6(2): 121-126.

Reason, J. (1997). Managing the risks of organizational accidents. Aldershot, UK.

Vidaillet, B. (2003). Le sens de l'action : Karl E. Weick, sociopsychologie de l'organisation / [F. Allard-Poesi, G. Koenig, H. Laroche, C. Roux-Dufort], Vuibert.

## AUTEUR

**Marc-Xavier Joubert – Président de Suez Advanced Fire Engineering**

Au sein de SUEZ, Marc-Xavier Joubert dirige une start-up innovante pour développer des solutions environnementales pour lutter contre les incendies.

Après avoir servi au sein de l'Aviation Légère de l'Armée de Terre, il a rejoint SUEZ où il a acquis une expertise dans la gestion des risques environnementaux et industriels dans leurs dimensions techniques, humaines et organisationnelles.

Il était précédemment directeur de la performance et des risques industriels du Groupe SUEZ.

Il est également membre de la commission scientifique risques accidentels de l'INERIS. Diplômé de l'Ecole Spéciale Militaire de Saint-Cyr et d'un Master Spécialisé en Facteurs Humains et Organisation de l'ESCP Europe, il est auditeur IHEDN – INHESJ de la première session nationale Souveraineté Numérique et Cyber-sécurité.

## AUTEUR

**Robert Breedstraet - Division information security officer, adjoint au Corporate CISO d'Amadeus IT Group.**

Robert Breedstraet dirige le département gouvernance et contrôle, le management de projets de cyber sécurité comme la gestion des identités et des accès, la protection de la marque Amadeus.

Il a aussi sous son autorité les responsables régionaux de sécurité informatique (Amérique, Inde, Asie-Pacifique, Europe et Moyen Orient). Robert a une expérience de plusieurs dizaines d'années en informatique et en particulier dans le domaine de la réservation aérienne.

Il est également représentant d'Amadeus dans différents groupes internationaux, informaticien et titulaire d'une maîtrise en politique économique, il est auditeur IHEDN – INHESJ de la première session nationale Souveraineté Numérique et Cyber-sécurité.

## AUTEUR

**Stéphane Deharvengt – adjoint chef de mission sécurité, sûreté, qualité du contrôle aérien français à la Direction des Services de la Navigation Aérienne - DGAC**

Stéphane Deharvengt dirige l'équipe en charge du Système de Management de la DSNA (Contrôle aérien français) dans ses composantes Sécurité, Sûreté (physique et cybersécurité) et Qualité. Son expertise est issue des travaux qu'il a mené dans la conception et l'application de stratégies complexes de maîtrise de la sécurité des vols et du contrôle aérien : Règlements opérationnels (retour d'expérience, systèmes de management, gestion de la fatigue) et de certification avion (conception cockpit et cabine, A380), Gestion des risques sécurité et cyber, Formations facteurs humains, nombreux programmes de recherche appliquée à la sécurité aérienne.

Il est également représentant français dans différents groupes internationaux. Ingénieur aviation civile de formation, il est titulaire d'un doctorat en ergonomie et auditeur IHEDN – INHESJ de la première session Souveraineté Numérique et Cybersécurité.



## POUR QUE L'EUROPE NE SOIT PAS UNE COLONIE NUMÉRIQUE

La souveraineté numérique européenne se heurte aux intérêts d'acteurs étrangers en situation quasi monopolistique sur le marché digital. La collecte des données, leur valorisation et leur intégration dans une intelligence artificielle requièrent la protection de la vie privée, un traçage consenti et le contrôle des modes de stockage pour susciter la confiance de l'utilisateur et une sécurité commerciale. En conséquence, l'Europe se dote d'un arsenal juridique : le RGPD en matière de protection des données, le Règlement « e-Privacy » quant au traçage et à la manifestation du consentement, le « privacy-shield » qui traite du transfert des données hors d'Europe avec un niveau de protection équivalent fourni par les gestionnaires étrangers des données.

La loi est également un instrument de régulation économique du numérique par la taxation fiscale des activités dans le ressort européen, la correction du déséquilibre contractuel entre les plateformes et les utilisateurs. Elle joue également un rôle pour tempérer les pratiques concurrentielles abusives en garantissant le choix des services ou de solutions logicielles. Elle remet en cause, par de récentes décisions, les contrats d'entreprise qui asservissent des travailleurs indépendants ou qui instaurent des conditions de travail non conformes au droit du travail des pays européens.



# La loi : atout ou obstacle

## à la souveraineté digitale européenne ?

Par **Cécile Doutriaux**

# A

Après l'enthousiasme des débuts de l'hyper connectivité, force est de constater qu'être relié à tous, à tous moments et à tous les endroits du monde suscite désormais moins de ferveur. Pourtant, les entreprises numériques développent toujours de nombreuses solutions, afin créer ou de répondre à de nouveaux besoins pour les citoyens et les organisations.

Les enjeux ont considérablement évolué depuis l'avènement d'Internet et au-

jourd'hui les États doivent intégrer le Big Data, l'industrie 4.0, la robotique et l'intelligence artificielle. Certaines sociétés digitales sont présentes sur de nombreux marchés et ont acquis un pouvoir

prépondérant, dans le commerce et la logistique (Amazon, Shopify), l'information (Google News, Twitter), le transport (Uber), le tourisme (Booking), le divertissement (Tik Tok, Youtube, Twitch) ou la publicité (Google, Facebook). Elles génèrent de la donnée précieuse (d'usage, d'achat, de comportement) et l'utilisent pour mieux comprendre les usagers et influencer les décisions des citoyens et notamment des consommateurs.

Ces entreprises numériques jouent un rôle important dans de nombreux secteurs et devraient donc être soumises au contrôle des autorités judiciaires, civiles et administratives. Pourtant, elles fixent leurs propres règles, inspirées du modèle économique nouveau qu'elles ont su créer et qui échappent encore au droit actuel, sur certains points. Si certains États ont su s'affirmer sur le marché digital, tels que les États-Unis avec les GAFAM (Google, Apple, Facebook, Amazon, Microsoft)



**CÉCILE  
DOUTRIAUX**

Avocate.  
Cabinet Juris  
Défense.

et les NATU (Netflix, Air BNB, Tesla et Uber), la Chine avec les BATX (Baidu, Alibaba, Tencent, Xiaomi) et la Russie (avec Yandex, VKontakte), les Européens peinent à faire émerger des acteurs indépendants sur le marché du numérique. En effet, la production de masse, les économies d'échelle qui en découlent, le développement commercial axé exclusivement sur le client, une forte image de marque et la fidélisation des consommateurs à leurs produits, font que tout nouvel entrant sur le marché ne peut produire qu'à des coûts unitaires supérieurs, ce qui entrave toute possibilité de développement pérenne. Ainsi, force est de constater que l'Union Européenne est encore

(1) Rapport d'information de Mme Catherine MORIN-DESAILLY, fait au nom de la commission des affaires européennes n° 443 (2012-2013) - 20 mars 2013.

aujourd'hui « une colonie du numérique ». <sup>1</sup> L'Union Européenne, confrontée à ses limites stratégiques et techniques, vit un moment historique car, sans confiance et

adhésion de tous, elle ne peut rivaliser avec les entreprises étrangères et prospérer.

Différents moyens peuvent être employés pour contrer la concurrence étrangère et faire émerger une souveraineté numérique européenne. La loi constitue-t-elle un moyen efficace pour permettre aux entreprises européennes de prendre une place pleine et entière sur le marché du digital ou constitue-t-elle un obstacle à l'innovation pour les entreprises ? Quels sont les moyens juridiques utilisés par l'Union

Européenne pour imposer une souveraineté numérique, alors qu'elle est confrontée à des acteurs étrangers qui gouvernent le marché depuis deux décennies ?

Dans ce combat, la loi est-elle un facteur d'union ou de division ? Instaure-t-elle véritablement une collaboration ou révèle-t-elle la concurrence exacerbée entre les Etats ?

### I - La loi, instrument de collaboration pour la souveraineté européenne

Les moteurs de recherche américains, leaders sur le marché, sont en position de force pour collecter en masse les données de leurs utilisateurs et ainsi développer l'internet des objets et l'intelligence artificielle.

Selon le rapport « Crémier » de la Commission européenne sur la politique de concurrence à l'ère digitale, 64 % des recherches en ligne aux États-Unis sont réalisées

via Google et ce chiffre atteint 90 % en Europe. Ces sites connaissent ainsi les centres d'intérêts des internautes grâce aux mots-clés qu'ils entrent dans le moteur, les sites qu'ils fréquentent grâce aux liens sur lesquels ils cliquent, la position géographique de l'internaute, estimée sur la base de l'adresse IP. Concrètement, Google exploite les recherches en ligne pour personnaliser la publicité, Amazon conserve les historiques de consultation et d'achat sur son site. Quant aux réseaux sociaux, Facebook

ou Twitter, ils collectent et revendent

(2) Le Boston Consulting Group a publié, en novembre 2012, une étude évaluant à 315 milliards d'euros, en 2011, la valeur des données personnelles collectées auprès des utilisateurs européens et annonçant qu'en 2020, ces données pourraient représenter mille milliards d'euros et induire une création de valeur équivalant à 8 % du PIB européen.

(3) Selon l'article 37-1, cette désignation est obligatoire notamment lorsque le traitement est effectué par une autorité publique ou un organisme public, mais aussi lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ». Ses principales missions sont de contrôler le respect du règlement, de conseiller le responsable des traitements sur son application et de faire office de point de contact avec l'autorité de contrôle, de répondre aux sollicitations de personnes qui souhaitent exercer leurs droits.

des données personnelles que les utilisateurs acceptent de leur confier volontairement.

Les données sont aujourd'hui considérées comme « l'or noir » du marché numérique et c'est en toute logique que les entreprises digitales les placent au cœur de leur stratégie de développement.<sup>2</sup>

Au-delà du potentiel économique qu'elles représentent, les données collectées en masse et leur croisement (Big data) mettent en péril la protection de la vie privée alors que, dans la société de l'information, la croissance du marché digital repose sur la confiance des citoyens.

Après quatre années d'intenses négociations législatives, l'Union Européenne s'est dotée du Règlement Général sur la Protection des Données (RGPD) N° 2016/679, le 27 avril 2016. Cette refonte était indispensable

(4) Selon l'article 17, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans certains cas et dans les meilleurs délais, de données à caractère personnel la concernant.

(5) Selon l'article 20, les personnes concernées ont le droit de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement. Elles ont aussi le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

(6) Selon l'article 22, toute personne a le droit, dans certains cas, de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

puisque les évolutions technologiques des dernières décennies ont rendu notamment nécessaire une révision de la Directive 95/46/CE du 24 octobre 1995.

Depuis le 25 mai 2018, le RGPD est entré en vigueur dans les 27 États membres de l'Union européenne et fait office de loi officielle pour la protection des données. Ce règlement reprend et précise des règles existantes concernant les droits des personnes concernées par la collecte des données (information, transparence, finalité, droit d'accès, consentement, confidentialité...). Il crée également de nouvelles obligations telles que la désignation d'un délégué à la protection des données (DPO),<sup>3</sup> le consentement positif avec l'acceptation explicite des cookies sur les sites internet, le droit à l'effacement,<sup>4</sup> à la portabilité des données personnelles,<sup>5</sup> la possibilité de refuser le profilage dans certains cas<sup>6</sup> et la réalisation

(7) Cette étude a pour but, selon l'article 35, de prévoir les mesures pour diminuer les conséquences possibles des dommages potentiels relatifs à la protection des données personnelles.

(8) Selon l'article 22 du RGPD.

(9) Selon l'article 83 du RGPD, l'une des premières amendes administratives peut atteindre jusqu'à 10 000 000 € ou pour une entreprise, jusqu'à 2 % de son chiffre d'affaires annuel mondial total de l'exercice précédent. Le montant retenu concerne toujours le montant de la sanction le plus élevé, lorsque les manquements aux RGPD concernent les obligations incombant au responsable du traitement et au sous-traitant, à l'organisme de certification et à l'organisme chargé du suivi des codes de conduite. En cas d'infractions plus importante et liée au non-respect du RGPD, l'amende administrative peut atteindre jusqu'à 20 000 000 € ou dans le cas d'une entreprise, l'amende correspond à 4 % du chiffre d'affaires mondial (le montant le plus important sera là aussi retenu).

d'étude d'impact sur la vie privée.<sup>7</sup>

Le règlement européen impose également aux organisations la protection des données « dès la conception » des produits, services et systèmes et consacre la règle de la « sécurité par défaut » qui implique la protection préétablie de la vie privée des utilisateurs, notamment par la « minimisation » de la collecte de leurs données personnelles.<sup>8</sup> Enfin, le RGPD responsabilise les entreprises, qui n'ont plus à demander une autorisation préalable de traitement des données personnelles, mais qui, en contrepartie, doivent être en mesure, à tout moment, d'apporter les preuves qu'elles respectent la réglementation. A défaut, elles s'exposent à des sanctions financières importantes, allant jusqu'à 4 % du chiffre d'affaires mondial annuel d'une entreprise ou 20 millions d'euros (le montant le plus élevé étant retenu), en cas de non-respect.<sup>9</sup>

(10) Rapport de la CNIL, chargée de collecter les manquements et les cas de violations du droit défini par le règlement européen, publié le 26 mai 2019, accessible sur la page <https://www.cnil.fr/fr/1-de-rgpd-une-prise-de-conscience-inedite> consultée le 30 septembre 2020.

plaintes au niveau européen ont été adressées aux autorités de contrôle, ce qui signifie que les citoyens souhaitent manifestement maîtriser davantage leurs données personnelles. L'instauration du « Comité Européen de la Protection des Données » par le RGPD a permis une meilleure coopération européenne opérationnelle entre les CNIL européennes pour diligenter les 1.013 procédures concernant plusieurs milliers de personnes.

(11) Dont M. Gary Shapiro, l'organisateur du salon CES (Consumer Electronic Show, salon annuel réunissant des startups du monde entier et de nombreux entrepreneurs américains).

(12) Voir l'interview accordée au Journal Économique le 12 novembre 2018, accessible à la page consultée le 30 septembre 2020 <https://www.lejournal-economique>.

L'application du RGPD a commencé à produire ses premiers résultats. La CNIL a réalisé un bilan chiffré, en mai 2019,<sup>10</sup> qui révèle que sur une période allant de mai 2018 à mai 2019, plus de 11.900 plaintes en France (+ 30 %) et 144.376

Il est certain que ces nouvelles contraintes n'ont pas forcément été accueillies avec conviction par les entreprises, puisque leurs obligations ont été alourdies.

Pour certains <sup>11</sup>, le RGPD constitue une erreur qui va entraver considérablement la capacité d'innovation européenne, ce qui conduirait « l'Europe

à perdre du terrain sur la Chine et sans doute aussi sur les États-Unis », <sup>12</sup>

En réalité, l'UE place le citoyen au centre de cette guerre économique et utilise la loi, d'un point de vue stratégique, pour contrer la dominance des entreprises américaines et asiatiques notamment.

Le RGPD constitue ainsi une arme pour rendre plus difficile l'accès au marché européen et pourrait obliger, à terme, les entreprises étrangères concurrentes à revoir leur modèle économique, puisque les données sont également protégées hors des frontières européennes.

### A. La protection des données sur le territoire européen

Depuis l'entrée en vigueur du RGPD, des plaintes ont été déposées partout en Europe contre les géants du Web américain : Google, Apple, Facebook, Amazon et LinkedIn.

Ces plaintes ont abouti en France à la condamnation de Google, pour infraction au RGPD, à une amende de 50 millions d'euros en 2019, confirmée le 19 juin 2020 par un arrêt n° 430810 du Conseil d'État. Des plaintes contre Facebook et Amazon sont actuellement instruites par l'équivalent irlandais et luxembourgeois de la CNIL. La CNIL n'est pas le seul organisme français à être entré en guerre économique contre les puissantes sociétés américaines. En effet, les associations de citoyens engagent, elles aussi, des actions judiciaires pour condamner les sociétés américaines pour non-respect de clauses

contractuelles relatives à la consommation et au RGPD. Ainsi, l'association UFC QUE CHOISIR a obtenu, le 7 août 2018, du Tribunal de Grande Instance de Paris, la condamnation de **Twitter** à supprimer plus de 250 clauses abusives et/ou illicites présentes dans ses « Conditions d'utilisation » et sa « Politique de confidentialité » et à 30 000 € de dommages et intérêts. Le 12 février 2019, elle a obtenu la condamnation de **Google**, par le Tribunal de Grande Instance de Paris pour 209 clauses abusives et illicites dans ses « Conditions d'utilisation » et « Règles de confidentialité ». Elle a aussi obtenu la condamnation de **Facebook**, par le Tribunal de Grande Instance de Paris, le 9 avril 2019, qui a jugé abusives et illicites 430 clauses pour non-respect de ses obligations en matière de données personnelles. Le réseau social a également été condamné à verser 30.000 € de dommages et intérêts. Plus récemment, le 12 juin 2020, l'association UFC « QUE CHOISIR » a obtenu la condamnation de la société **Apple**, par le Tribunal judiciaire de Paris, qui a jugé illicites ou abusives plusieurs clauses concernant les données personnelles. En effet, Apple estimait notamment que l'adresse IP, l'indicatif postal ou encore la géolocalisation des utilisateurs n'étaient pas des données « personnelles », et de fait n'étaient pas protégées par les règles du RGPD. De plus, cette société ne respectait pas les règles relatives au consentement, au droit d'accès et au droit d'opposition.

(13) Ici 20 000 € en réparation du préjudice occasionné à l'intérêt collectif des consommateurs et 10 000 € pour les frais de justice.

Si les sanctions financières prononcées contre ces sociétés mondiales paraissent dérisoires<sup>13</sup>, il n'en reste pas moins qu'en terme d'image,

il est préjudiciable pour ces sociétés d'être condamnées pour non-respect des droits des citoyens. De plus, pour lutter contre la concurrence étrangère, la protection des données européennes s'applique également hors des frontières de l'Union Européenne.

## B. La protection des données hors de l'Union Européenne

Pour affirmer sa souveraineté numérique, la commission européenne a décidé de renforcer ses propres règles, pour les rendre plus efficaces.

### 1. Le règlement e-Privacy

En France, le 19 février 2020, le Sénat a adopté, à l'unanimité, une proposition de loi visant à garantir « le libre choix du consommateur dans le cyberspace », notamment en matière de plateformes et d'applications, pour réguler la concurrence

(14) Voir la synthèse du sénat sur la page <http://www.senat.fr/rap/19-301/119-301-syn.pdf>

et démanteler les GAFAM, dont le chiffre d'affaires serait comparable aux recettes fiscales françaises.<sup>14</sup>

qui a pour objet de remplacer la directive « e-Privacy » de 2002 (2002/58/CE), actualisée en 2009 avec la directive 2009/136/CE, également appelée « Directive Cookie ». Ce règlement a pour principal objectif de renforcer le marché unique numérique (MUN) européen en protégeant d'avantage les données des citoyens. En effet, les sociétés commerciales tracent et recensent l'historique des activités menées par un individu sur internet, grâce au dépôt de cookies, afin d'identifier ses besoins pour lui proposer des produits ou des services. Il s'avère que les principales plaintes des citoyens portent sur la collecte déloyale

(15) La pratique de l'opt-out dans le domaine de l'email marketing, qui consiste à envoyer un email commercial à un individu, sans lui avoir demandé auparavant son autorisation, mais en lui permettant cependant dans le cadre du message de solliciter à ne plus être dans la liste des destinataires, en est l'illustration.

de leurs données personnelles, sans leur consentement et sur le défaut d'information quant aux finalités réelles du traitement, mis en place à leur rencontre. En effet, il est encore possible, actuellement, pour une entreprise, de poser et de stocker des cookies, sans tenir véritablement compte

de la volonté de l'utilisateur de ne pas être suivi dans ses activités.<sup>15</sup> De plus, se voir interdire l'accès à un site ou une application, en cas de refus d'être tracé, est encore fréquent.

L'Union Européenne a aussi décidé d'aller plus loin dans la protection des données en 2019 avec le Règlement « e-Privacy »

L'idée de l'e-Privacy serait alors d'offrir aux utilisateurs la possibilité de s'opposer à tout *tracking*, en amont, dans le paramé-

trage de leurs outils numériques (ordinateur, tablette, téléphone mobile), sans devoir réitérer systématiquement ce refus, à chaque visite de sites internet ou d'utilisation d'applications. Par défaut, les entreprises numériques seraient donc obligées d'intégrer ce refus, dès la conception de leurs produits et de leurs services, ce qui aurait pour effet de les rendre moins attractifs pour les entreprises commerciales, qui collectent massivement les données pour personnaliser leurs offres et pour les revendre à d'autres entreprises. Ce règlement inquiète les industries numériques, qui redoutent qu'une protection renforcée des données personnelles entrave leur activité et l'innovation, notamment pour l'Internet des objets. Certaines sociétés pensent ainsi que ce règlement risque de mettre économiquement en péril leurs activités et elles n'ont pas tort en réalité. En effet, il semble assez prévisible que la majorité des citoyens

déclineront ce consentement et ce d'autant plus qu'ils se déclarent désormais particulièrement sensibles à la protection de leurs données personnelles.<sup>16</sup>

La loi peut donc, ici, apparaître comme un frein à l'innovation et au développement des entreprises numériques, au sein même de l'Union Européenne.

Pourtant, la loi reste une tentative, utilisée comme une autre, pour défendre le marché européen, à l'intérieur des frontières européennes, mais aussi en dehors des frontières. En effet, l'article 3 du RGPD prévoit l'application extra-territoriale du règlement aux entreprises établies en dehors de l'Union européenne dès qu'elles ciblent les données personnelles des résidents européens, ce qui concerne de nombreuses entreprises américaines et asiatiques.

### Le Privacy shield

Avec la globalisation des échanges et l'utilisation croissante des nouvelles technologies, le nombre de transferts de données, hors de France et de l'Europe, ne cesse de croître. Là encore, l'UE recourt à la loi pour contrer les sociétés concurrentes étrangères.

En effet, le transfert de données hors de l'Union européenne et de l'Espace Economique Européen est possible, à la seule condition d'assurer un niveau de protection des données suffisant et approprié, conforme au RGPD. Afin de pouvoir « s'auto-certifier » conformément aux exigences européennes en matière de protection des données personnelles, une entreprise établie aux États-Unis doit être soumise aux pouvoirs de contrôle et d'exécution de la Commission Fédérale du Commerce (« FTC ») ou du Département des Transports américain (« DoT »). Le Privacy Shield, succédant au Safe Harbor (lui-même invalidé

(16) En France, selon la CNIL, 68 % des Français se disent plus sensibles à la protection de leurs données personnelles, depuis l'entrée en vigueur du RGPD - Voir le rapport d'activité de la CNIL du 9 juin 2020, sur la page <https://www.cnil.fr/fr/la-cnil-publie-son-rapport-dactivite-2019>, consultée le 2 octobre 2020.

par la CJUE en 2015), avait été reconnu par la Commission européenne (décision 2016/1250) comme offrant un niveau de protection adéquat aux données à caractère personnel, transférées par une entité européenne vers des entreprises établies aux États-Unis.

(17) CJUE, gr. ch., 16 juill. 2020, aff. C-311/18, Data Protection Commissioner c/ Facebook Ireland Limited, Maximilian Schrems.

(18) Le FISA autorise les organismes de surveillance, comme le FBI ou la CIA, à exploiter les données des ressortissants non américains, même situés hors du territoire des États-Unis, dès lors que ces données sont détenues par des personnes morales américaines.

(19) L'E.O. 12333 permet notamment « l'acquisition d'une communication non publique par des moyens électroniques sans le consentement d'une personne qui est partie à une communication électronique ».

Pourtant, la Cour de justice de l'Union européenne (CJUE) a rendu le 16 juillet 2020 un arrêt dans l'affaire dite « Schrems II » invalidant la décision d'adéquation du Privacy Shield, adoptée en 2016.<sup>17</sup> En effet, le *Privacy Shield* prévoyait des limitations à la protection des données en vertu d'exigences relatives à la sécurité nationale, notamment par le biais des programmes et services de renseignement : l'article 702 du « *Foreign Intelligence Surveillance Amendment Act (FISA)* »<sup>18</sup> et l'« Executive Order 12333 » (E.O. 12333).<sup>19</sup>

Ces textes permettent une surveillance massive des ressortissants non-américains et c'est la raison pour laquelle la CJUE a invalidé la décision 2016/1250 de la Commission européenne, sans remettre en cause la décision de la Commission

2010/87/CE sur les clauses contractuelles types.

L'association Noyb, dont le président d'honneur est Max Schrems, qui a initié les actions engagées contre Facebook devant les juridictions européennes, a interrogé 33 entreprises (dont Microsoft, Apple, Nike, Netflix...) sur l'annulation du Privacy Shield.

(20) [https://noyb.eu/files/web/Replies\\_from\\_controllers\\_on\\_EU-US\\_transfers.pdf](https://noyb.eu/files/web/Replies_from_controllers_on_EU-US_transfers.pdf)

Dans son rapport du 25 septembre 2020,<sup>20</sup> l'association expose que les sociétés Airbnb, Netflix et WhatsApp n'ont jamais

répondu à ses sollicitations et que la majorité des autres entreprises l'ont renvoyé vers leur politique de confidentialité (Blizzard, Coinbase, Instagram, Revolut). En revanche, pour la société Microsoft, il est toujours possible de transférer des données personnelles vers les États-Unis, en vertu des clauses contractuelles types.

C'est dans ce contexte que le Comité Européen de la Protection des Données (CEPD) s'est prononcé, le 23 juillet 2020, en exposant que ni les clauses contractuelles types, ni les BCR ne constituent de « garanties appropriées » suffisantes pour le transfert de données vers les États-Unis. Dès lors, il conviendrait de suspendre ou d'interdire tous les transferts vers les USA ou bien adapter les clauses contractuelles types (CCT) en prévoyant des mesures supplémentaires, si besoin est, pour assurer cette protection.



Effectivement, si les clauses contractuelles des sociétés américaines comportent de nouvelles garanties, conformes au RGPD, il sera difficile juridiquement de s'opposer aux transferts des données européennes vers les États-Unis.

## 2. La loi, comme instrument de guerre économique

Selon la commission européenne, certaines sociétés américaines empêchent illégalement une concurrence et les consommateurs européens de bénéficier d'un réel choix de services, ce qui à terme, crée des situations de monopoles et augmente les prix.

En effet, tout utilisateur a pu constater l'existence de difficultés pour désinstaller Youtube ou Chrome sur Android et Apple Music sur iOS. Or, la pré-installation forcée et l'impossibilité de désinstaller certaines applications font que les utilisateurs téléchargent rarement des applications européennes, offrant les mêmes fonctionnalités.

Ces pratiques commerciales anticoncurrentielles sont sanctionnées par le droit national et européen, car elles faussent la concurrence qui s'exerce entre les entreprises et porte préjudice à celles qui souhaitent se faire une place sur le marché.

En organisant la dissémination du pouvoir économique, le droit protège ainsi la société contre les concentrations et partage le pouvoir économique entre différents

acteurs, plutôt qu'entre les mains d'une minorité dominante.

### A. Les entreprises numériques sanctionnées par le droit de la concurrence

L'article 102 du traité sur le fonctionnement de l'Union européenne (TFUE) interdit les abus de position dominante susceptibles d'affecter le commerce dans l'UE et de fausser ou de restreindre la concurrence.

Ainsi, la commission européenne intervient régulièrement pour condamner les entreprises américaines qui menacent de manière abusive le développement d'entreprises numériques européennes souveraines et, à titre d'exemple, a infligé de lourdes sanctions à Google, pour un montant total atteignant 8,25 milliards d'euros.

En effet, **en 2017**, la Commission a sanctionné Google d'une amende de 2,42 milliards d'euros, pour abus de position dominante sur le marché des moteurs de recherche, en favorisant son propre service de comparateur de prix, tout en rétrogradant les services de ses rivaux.

**En 2018**, Google a été une nouvelle fois condamnée par la Commission à une amende de 4,34 milliards d'euros, pour avoir abusé de sa position dominante sur les systèmes d'exploitation mobile, dans le but de favoriser exclusivement

son application de recherche Google Search et son navigateur Google Chrome. Concrètement, Google exigeait des fabricants qu'ils préinstallent ces applications et payait même des fabricants et des opérateurs de réseaux mobiles pour qu'ils les préinstallent en exclusivité sur leurs appareils. Bien évidemment, ces pratiques ont porté préjudice aux moteurs de recherche concurrents et Google est aujourd'hui obligé de permettre aux utilisateurs Android de choisir leur moteur de recherche et leur navigateur web, lors de la configuration de leur nouveau smartphone. Dès lors, le 8 janvier 2020, la société Google a communiqué la liste, par pays européens, des alternatives à son moteur de recherche, étant précisé qu'il s'agit principalement de DuckDuckGo et d'Info.com, mais aussi du moteur de recherche Qwant pour la France. Depuis le 1<sup>er</sup> mars 2020, Google propose à l'utilisateur de choisir son navigateur par défaut, parmi une proposition de quatre choix, en plus de Chrome. Cette disposition a pour objectif à terme de favoriser les moteurs de recherche nationaux ou européens, pour collecter d'importantes masses de données, destinées à favoriser le développement de l'internet des objets et de l'intelligence artificielle.

Google a aussi été condamnée **en 2019** à une amende de 1,49 milliard d'euros, pour abus de position dominante à travers la régie publicitaire AdSense, car elle imposait des clauses d'exclusivité dans

(21) À titre d'exemple, l'enquête « Google shopping » menée par la Commission européenne en 2008, pour abus de position dominante pour avoir favorisé son service de comparaison des prix sur son moteur de recherche a pris fin 7 ans plus tard et a abouti à une condamnation en juin 2017, alors que la plupart des services de comparateurs de prix rivaux de Google ont été évincés du marché.

(22) Régies par le règlement 1/2003 du 16 décembre 2002 et son article 8 permet de les prendre « dans les cas d'urgence justifiés par le fait qu'un préjudice grave et irréparable risque d'être causé à la concurrence ».

(23) <http://www.senat.fr/rap/a19-548/a19-54810.html>

(24) Comme l'a illustré sa décision prise le 16 octobre 2019 envers la société américaine Broadcom, premier fournisseur mondial de puces utilisées dans les décodeurs de télévision et les modems.

les contrats passés avec des sites web tiers, contraignant les éditeurs à réserver l'espace le plus rentable sur leurs pages de résultats de recherche aux publicités de Google et exigeant un nombre minimal de publicités de Google sur ces pages.

Ces sanctions sont importantes, mais parfois, la société dominante parvient à les contourner. Ainsi, la société Google a mis en place un système d'enchères, pour proposer des moteurs de recherche alternatifs aux utilisateurs d'Android, ce qui lui a permis en réalité de faire payer à ses concurrents une partie de l'amende prononcée à son encontre. De plus, les procédures sont longues et les sanctions arrivent souvent à un moment où les entreprises monopolistiques

ont consolidé leur position dominante et évincé les concurrents émergents, de sorte que l'objectif stratégique initial de l'Union Européenne n'est pas atteint.<sup>21</sup>

L'Autorité de la concurrence Européenne a donc décidé de recourir plus souvent à des mesures conservatoires,<sup>22</sup> permettant d'entraver les activités de ces sociétés dominantes, avant même qu'une décision définitive ne soit rendue, grâce à la directive (UE) 2019/1 du Parlement européen et à la directive « ECN+ »<sup>23</sup>, qui prévoit la possibilité, pour l'ensemble des autorités nationales de concurrence de se saisir d'office, pour protéger le marché européen d'avantage en amont.<sup>24</sup>

Cependant, lutter contre la rapidité de pénétration de ces entreprises sur les marchés, du fait de l'adhésion forte des consommateurs placée au centre de leur démarche commerciale, reste difficile.

D'autres voies juridiques doivent par conséquent être utilisées, au niveau européen, raison pour laquelle l'Union Européenne a récemment initié des travaux, en vue d'instaurer de nouvelles réglementations.

## **B. Le recours au droit de la consommation pour limiter l'emprise des sociétés digitales**

### **1. Le règlement « Plateform to Business » (P2B)**

Ce règlement est entré en vigueur, le 12 juillet 2020, pour encadrer les relations entre les services d'intermédiation en ligne ou les moteurs de recherche et les entreprises utilisatrices, c'est-à-dire les professionnels qui offrent des biens

ou des services à des consommateurs par leur intermédiaire. Ici, il s'agit de protéger les professionnels qui pourraient se trouver dans une relation déséquilibrée avec une plateforme ou avec les moteurs de recherche américains.

Le règlement impose ainsi plusieurs contraintes aux plateformes et notamment l'obligation d'information et de transparence des conditions générales quant aux comportements qui pourront générer la restriction, la suspension ou la résiliation du service, avec l'obligation de motiver cette décision et de respecter un préavis minimum de 30 jours, avant la mise en œuvre de cette mesure.

Concernant la transparence des algorithmes et le traitement des données, les plateformes doivent désormais préciser les principaux paramètres déterminant le classement des offres sur la plateforme et doivent informer les entreprises utilisatrices de la possibilité d'influer sur le résultat des classements en contrepartie d'une rémunération directe ou indirecte de la plateforme.

En réalité, ces obligations sont similaires à celles qui existent déjà en droit français à la charge des plateformes, dans le cadre de leurs obligations générales d'information précontractuelles depuis la loi n°2016-1321 pour une République numérique, du 7 octobre 2016.

La principale faiblesse de cette réglementation est qu'aucune sanction financière n'a été directement prévue. Aussi, une autre directive européenne dite « une nouvelle donne pour les consommateurs » vise à modifier quatre directives en matière de consommation : la directive 93/13/CEE du 5 avril 1993 sur les clauses contractuelles abusives, la directive 98/6/CE du 16 février 1998 sur l'indication des prix des produits offerts aux consommateurs, la directive 2005/29/CE du 11 mai 2005 sur les pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs et la directive 2011/83/UE sur les droits des consommateurs, transposée en droit français par la loi n° 2014-344, du 17 mars 2014, dite « Hamon ».

Adoptée le 17 avril 2019, elle prévoit notamment des obligations renforcées de transparence pour les plateformes en vue de mieux protéger les consommateurs et surtout la possibilité de prononcer une amende maximale d'au moins 4 % du chiffre d'affaires annuel de l'opérateur dans chaque État membre, en cas d'infraction à la législation de l'Union Européenne en matière de consommation.

Les États membres devront transposer cette directive au plus tard le 28 novembre 2021, date à laquelle elle entrera en application.

### a. Le « Digital Services Act » (DSA)

Dans le cadre de la stratégie numérique européenne, la Commission européenne a annoncé un ensemble de mesures relatives aux services numériques visant à renforcer le marché unique des services numériques et à promouvoir l'innovation et la compétitivité européenne.

Après avoir réglementé le commerce électronique par la Directive 2000/31/CE du 8 juin 2000, inchangée depuis vingt ans, hormis quelques adaptations sectorielles, la Commission européenne a donc initié une réflexion, le 19 février 2020, autour d'un « Digital Services Act » pour : « Façonner l'avenir numérique de l'Europe ». <sup>25</sup>

(25) [https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020\\_fr.pdf](https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_fr.pdf)

(26) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers>.

L'objectif de cet acte est de limiter la concentration des entreprises numériques (réseaux sociaux et moteurs de recherche notamment) dans l'espace économique européen, afin de permettre une concurrence saine et équitable pour les nouveaux entrants et les concurrents existants, face à des plateformes bien installées, mais aussi pour diversifier le choix des consommateurs. <sup>26</sup>

Cette réglementation concerne également la situation des travailleurs indépendants des plateformes et la possibilité d'accepter ou de refuser la publicité ainsi que le ciblage en ligne notamment.

Une vaste consultation publique a été lancée de 2 juin au 8 septembre 2020 par la Commission européenne pour recueillir les avis des européens sur cette future législation qui, une fois élaborée, sera soumise à l'examen du Parlement européen et au vote des 27 Etats membres. Consultée, la société Google a rendu son avis le 3 septembre 2020. Elle déclare redouter l'entrave portée à ses activités par l'Union Européenne et estime que la Commission doit mettre en place une législation qui « encourage la croissance économique et l'innovation » et demande que « les nouvelles règles n'entraînent pas de coûts et de charges excessifs pour les entreprises, ce qui les

(27) <https://www.blog.google/around-the-globe/google-europe/more-responsible-innovative-and-helpful-internet-europe/>

empêcherait de se développer rapidement et d'offrir leurs services dans l'UE et dans le monde entier ».<sup>27</sup>

Effectivement, si toutes les réglementations envisagées sont adoptées, les entreprises américaines pourraient, à terme, perdre leur situation de monopole. De plus, il existe d'autres lois pour affirmer la souveraineté européenne sur le marché du numérique, notamment au niveau fiscal et social.

### 3. La loi européenne, porteuse d'égalité fiscale et de valeurs sociales

La régulation économique du numérique est une nécessité au niveau national, européen et international. Les questions soulevées par la dominance des géants du numérique ne sont pas seulement économiques car elles concernent aussi nos valeurs sociales.

#### A. La taxation fiscale des géants américains du numérique

L'objectif est de rétablir une certaine égalité fiscale avec les entreprises nationales et européennes, fortement imposées en comparaison.

(28) La loi n° 2019-759 du 24 juillet 2019 portant création d'une taxe sur les services numériques et modification de la trajectoire de baisse de l'impôt sur les sociétés.

(29) <https://www.gouvernement.fr/sites/default/files/contenu/>

En matière fiscale, le législateur français a institué une taxe spécifique visant certains géants du numérique par la loi n° 2019-759 du 24 juillet 2019<sup>28</sup> qui ne s'applique qu'aux services numériques pour lesquels les données des utilisateurs sont le plus

fortement mises à contribution dans la création de valeur. Selon les déclarations du ministère de l'Économie et des finances du 6 mars 2019, la fiscalité serait inéquitable entre les entreprises puisque le taux d'imposition moyen d'une entreprise « numérique » dans l'Union Européenne serait de 9,5 %, alors que le taux d'imposition moyen d'une entreprise dans l'Union Européenne serait de 23,2 %.<sup>29</sup>

Cette taxe vise expressément les activités de publicité ciblée, de vente de données en ligne et de services d'intermédiation entre internautes. Seules sont concernées les entreprises dont le chiffre d'affaires est supérieur à 750 millions d'euros au niveau mondial et à 25 millions d'euros à l'échelle de la France.

Le montant de la taxe est calculé en appliquant un taux de 3 % sur le chiffre d'affaires réalisé en France et elle aurait rapporté à l'État français 350 millions d'euros depuis son application.

Par mesure de rétorsion, le gouvernement américain a annoncé, le 10 juillet 2020, qu'il imposait des droits de douane supplémentaires de 25 % sur les produits français d'une valeur commerciale

(30) Soit 1,15 milliard d'euros aux produits cosmétiques et aux sacs à main dans un délai de 6 mois.

de 1,3 milliard de dollars,<sup>30</sup> ce qui a contraint la France à geler sa taxe puis finalement à l'appliquer pour l'année 2020.

Cette mesure est intéressante puisque certaines puissantes sociétés numériques américaines qui offrent leurs services, gratuits pour l'utilisateur, sont financés principalement par la publicité. En effet, en 2019, sur les 70,6 milliards de dollars de chiffre d'affaires enregistrés par Facebook, 69,6 milliards (soit 98 %) provenaient de recettes publicitaires. Intégré au sein du conglomérat Alphabet<sup>31</sup> en 2015, Google réalise 83 % de son

(31) <https://itsocial.fr/articles-decodeurs/que-cache-la-transformation-de-google-en-conglomerat-alphabet/>

(32) Informations transmises lors de l'audition de Google par la mission d'information de l'assemblée nationale du 20 février 2020, consultable sur la page

chiffre d'affaires grâce aux recettes publicitaires.<sup>32</sup> Au total, une trentaine de groupes sont concernés dont Google, Amazon, Facebook, Apple, mais aussi Meetic, Airbnb, Instagram et Criteo.

Concrètement, cette taxe vise à imposer les géants du numérique à hauteur

de 3% du chiffre d'affaires numériques (revenus publicitaires, commissions touchées par les plateformes, revenus liés à la re-vente de données personnelles) réalisé en France. D'autres Etats membres de l'Union européenne (UE), tels que le Royaume-Uni, l'Espagne, l'Italie, la République tchèque et l'Autriche, se sont engagés dans un processus législatif identique, alors même que la Commission européenne, qui soutient ce projet, souhaite éviter un amoncellement de dispositions nationales, désharmonisées sur ce sujet. Cette taxation est d'autant moins évidente que la position des 27 membres de l'Union Européenne n'est pas unanime. En effet, des pays tels que l'Irlande (avec Facebook, Google et Apple), la Suède, la Finlande, le Danemark et le Luxembourg (avec Amazon) offrent une fiscalité avantageuse aux entreprises numériques américaines qui implantent leur siège social dans leur État.

Le 15 mai 2020, le Parlement européen a voté une résolution réclamant la mise

en place de cette taxe sur les grandes entreprises du numérique et, le 21 juillet 2020, les États membres ont proposé de mettre en place « une redevance numérique », au plus tard le 1er janvier 2023. Les négociations sont en réalité menées à plusieurs niveaux et dans différentes institutions où les États ont vocation à se réunir. Ainsi, l'Organisation de coopération et de développement économiques (OCDE), a obtenu l'accord de principe de 137 États, le 29 janvier 2019, pour réformer les règles fiscales actuelles, en faveur d'une plus juste taxation de l'économie numérique. Elle s'est engagée à présenter une proposition concrète d'accord en octobre 2020, lors du « G20 Finances » de Washington. Toutefois, en raison de la crise sanitaire mondiale, les États-Unis ont déclaré, le 17 juin 2020, vouloir se concentrer principalement sur la gestion de cette crise, avant d'envisager la question de la fiscalité internationale.

Compte tenu de la divergence de positions des dirigeants européens et de l'échéance relativement lointaine de ces dispositions, une solution, pour les États serait de s'affranchir de l'Union Européenne et ce d'autant plus qu'en matière de fiscalité chaque État membre reste souverain pour élaborer sa propre taxation.

Toutefois, la limite de cette position stratégique est que les sociétés taxées ont dû et déjà décidé de répercuter les

(33) Apple a décidé d'ajuster ses tarifs appliqués aux développeurs iOS. Amazon a fait de même avec les vendeurs tiers et Google avec les annonceurs, dans de nombreux pays tels que la France, l'Allemagne, l'Italie, la Turquie.

coûts engendrés par cette nouvelle fiscalité sur leur partenaires (développeurs, vendeurs et annonceurs),<sup>33</sup> ce qui aurait pour effet d'annuler tout effet bénéfique. Finalement, les sociétés numériques dominantes répercutent

le montant de la taxe fiscale sur leurs partenaires commerciaux ou sur les consommateurs, ce qui rend cette stratégie assez inefficace.

## B. La contestation des travailleurs et des professionnels

La notoriété des plateformes américaines telles qu'Uber, airBnB, Booking n'est plus à démontrer. Ces entreprises ont su astucieusement prendre une place de choix sur le marché économique et dans les habitudes de consommation des citoyens.

Pendant, le développement économique de ces plateformes, après avoir connu auprès des consommateurs un succès retentissant sur les marchés nationaux de l'Europe, semble être, pour partie du moins, remis en question non seulement par les États européens et par les entreprises concurrentes mais aussi par les travailleurs. De fait, en Europe, des procédures ont été engagées par ces derniers, supposés indépendants, pour obtenir la requalification de leur contrat d'entreprise en contrat de travail.

Le statut d'indépendant des coursiers de Deliveroo, Uber East, Frichti, Stuart, Take Eat Easy, Foodora est ainsi contesté dans de nombreux pays et plusieurs décisions de justice ont déjà donné raison aux livreurs. En Belgique, la plateforme de livraison Deliveroo est accusée de ne pas payer de cotisations sociales pour les milliers de coursiers qu'elle fait travailler dans le pays. En Espagne, la justice a estimé que Deliveroo a fait passer comme indépendants des centaines de livreurs qui auraient dû être déclarés comme salariés, évitant ainsi de payer 1,2 million d'euros de cotisations sociales. En France, le conseil des prud'hommes de Paris (section commerce 19/0773) a condamné la société Deliveroo, le 4 février 2020, à verser 30 000 d'euros au livreur qui l'avait assignée.

Le 4 mars 2020, la Cour de cassation, par un arrêt de la chambre sociale n° 374 (19-13.316), a confirmé la décision du 10 janvier 2019, de la Cour d'appel de Paris, qualifiant un chauffeur Uber de salarié de la plateforme et non de travailleur indépendant, en raison de l'existence d'un lien de subordination. En effet, selon la Cour de cassation, « Le chauffeur qui a recours à l'application Uber ne se constitue pas sa propre clientèle, ne fixe pas librement ses tarifs et ne détermine pas les conditions d'exécution de sa prestation de transport. L'itinéraire lui est imposé par la société et, s'il ne le suit pas, des corrections tarifaires sont

appliquées ». L'argument avancé par la plateforme pour contrer ce raisonnement, à savoir la liberté offerte au chauffeur de se connecter lorsqu'il le souhaite à l'application, a été purement et simplement écarté.

Ces procédures, qui remettent en question le modèle économique de ces sociétés, ne sont pas seulement engagées devant les juridictions prud'homales par les travailleurs, mais également devant les juridictions pénales pour travail dissimulé et devant le tribunal des affaires de la sécurité sociale, pour obtenir le recouvrement des cotisations qui auraient dû être versées par ces sociétés aux administrations françaises, telles que l'URSSAF, Pôle emploi...

Pour les plateformes américaines et européennes des requalifications massives entraîneraient une forte augmentation des coûts notamment en raison des cotisations sociales à verser, des droits aux congés payés, à la formation, ce qui pourrait remettre en cause le modèle économique des sociétés numériques.

Mais plus qu'une guerre économique, il s'agirait aussi d'une guerre idéologique puisque selon La Fédération nationale des auto-entrepreneurs (FNAE), la vaste majorité des chauffeurs n'auraient pas l'intention de devenir des salariés car beaucoup sont dépendants financièrement de ces applications ce qui les dissuade



d'entamer des poursuites. Selon cette fédération, cette décision risque de mettre en péril plus de 180 plateformes qui existent en France dans tous les domaines et qui ont fait travailler 280 000 personnes au moins une fois en 2019.

D'autres plateformes sont également contestées, par la voie judiciaire, par les professionnels de différents secteurs, tels que *Booking* par les restaurateurs ou *Airbnb* par les hôteliers. Il est intéressant de relever que la CJUE s'est prononcée en faveur de l'encadrement de leurs pratiques. En effet, le 22 septembre 2020, la CJUE a validé le recourt aux articles L. 631-7 et L. 631-7-1 du Code de la consommation français pour limiter, dans sa portée nationale mais non locale, l'usage d'*Airbnb* dans les communes de plus de 200 000 habitants en France.

En définitive, recourir à la loi, pour contrer la concurrence des entreprises étrangères, en situation de monopole sur le marché numérique européen, est utile et relativement efficace, même si la commission européenne doit aller beaucoup plus loin pour affirmer une réelle souveraineté numérique indépendante. De plus, seules les sociétés américaines, en position de monopole sont essentiellement visées, ce qui ne remettrait pas en cause l'innovation et le développement des entreprises européennes.

Développer un positionnement conforme

à la protection des données personnelles, à laquelle les consommateurs déclarent être si sensibles, peut même constituer une différenciation concurrentielle favorable, par rapport à leurs concurrents étrangers.

### En conclusion...

L'UE a adopté une véritable posture défensive et se sert de la loi pour mettre en place un protectionnisme économique, destiné à lutter contre la concurrence américaine et chinoise. En limitant et en interdisant certaines pratiques, les États et l'Union Européenne ont clairement déclaré la guerre aux sociétés américaines en situation de monopole sur leur marché.

Cependant recourir à la loi revient à adopter une posture exclusivement défensive, adoptée par défaut, alors que la « guerre » menée entre les États est avant tout technologique et économique. Effectivement, la loi peut rendre l'accès au marché européen plus difficile mais cela suffira-t-il à affirmer la souveraineté numérique européenne ? On peut légitimement en douter pour l'instant et d'autres mesures, plus offensives, devront être employées.

### 1. Systématiser les sanctions pour non-respect du RGPD

Les condamnations prononcées au titre de la protection des données personnelles sont importantes symboliquement. On doit cependant noter que Google, Ama-

zon, Facebook et Apple génèrent annuellement près de 700 milliards de dollars de chiffre d'affaires et que ces sanctions sont intégrées comme de simples charges de fonctionnement, dans le cadre du budget global des plateformes concernées. Elles devraient donc être davantage alourdies pour être dissuasives, ce qui permettrait aussi de réinvestir les fonds récoltés dans la recherche opérationnelle, le développement et l'innovation européenne.

Cependant, limiter la dominance des entreprises américaines sans entraver l'innovation des sociétés européennes reste un exercice délicat. L'établissement de règles pour éviter les dérives est essentiel mais comment contrer ces entreprises technologiquement et économiquement ?

## 2. Le rachat par les sociétés américaines des entreprises européennes prometteuses

Si la domination de grands groupes américains est frappante dans le monde numérique, l'Union européenne est riche en nombreux talents, qui peinent toutefois à acquérir une dimension européenne et mondiale. Pour renforcer leur position dominante, les GAFAM ont procédé, ces dix dernières années, à environ 400 acquisitions de startups prometteuses avec un chiffre d'affaires limité mais dont le potentiel est estimé très important et parmi lesquelles figurent de

nombreuses entreprises françaises. Or, la plupart finissent rachetées par des sociétés étrangères comme Spotify, lancé en 2008 et rachetée par la société américaine Facebook en 2011, et Price Minister rachetée par une société japonaise en 2010.

Il est donc fondamental d'interdire le rachat de startups françaises et européennes innovantes ou de limiter fortement la part détendue par les sociétés concurrentes étrangères dans ces entreprises, comme le font les États-Unis qui n'hésitent pas à affirmer leur protectionnisme en interférant dans les transactions commerciales opérées, pour imposer l'entreprise américaine Oracle lors du rachat du réseau social chinois *Tik Tok*. La Chine ayant, par réaction, élaboré en septembre 2020, une nouvelle réglementation qui visait à limiter les exportations technologiques chinoises.

(34) Ce réseau social qui offre le partage instantané de vidéos et une messagerie pour favoriser les rencontres, a été fondé en 2015 par Sacha Lazimi, Jérémie Aouate et Arthur Patora.

(35) <https://www.lesechos.fr/tech-medias/high-tech/yubo-le-reseau-social-francais-qui-cartonne-a-letranger-1254408>

Au niveau national, il serait par exemple regrettable que le réseau social français *Yubo*,<sup>34</sup> extrêmement populaire aux États-Unis, soit finalement racheté par Facebook qui a déjà racheté *Instagram* en 2015. En effet, cette startup a levé 11,2 millions d'euros

en 2019 auprès d'*Iris Capital*, *Idinvest Partners*, *Alven*, *Sweet Capital* et *Village Global*, qui compte parmi ses investisseurs Mark Zuckerberg et Jeff Bezos, ce qui pourrait annoncer un potentiel rachat par un géant du Net.<sup>35</sup>

Il est intéressant de constater que les États qui ont su prendre une place de choix sur le marché digital sont essentiellement ceux qui ont su, à l'instar de la Chine et des États-Unis, assumer, sans complexe, un certain protectionnisme numérique. Par conséquent, il serait temps que les États européens soient plus attractifs pour leurs sociétés nationales en priorisant leurs subventions à leur égard et en relocalisant l'activité de certains sous-traitants, pour permettre une meilleure indépendance des sociétés locales. Malgré les efforts fournis pour adapter et utiliser le droit, afin de faire émerger la souveraineté numérique européenne, des efforts importants restent à fournir.

Curieusement, la solution pourrait provenir davantage des États-Unis eux-mêmes qui souhaitent limiter l'influence, voire démanteler les entreprises américaines qui entravent aussi leurs concurrents sur leur territoire national. En effet, les effets néfastes de leur abus de position dominante se retrouvent également sur le marché intérieur américain et en 2019, le gouvernement des États-Unis a décidé d'ouvrir une enquête contre

les géants du numérique.

(36) <https://www.usine-digitale.fr/article/que-faut-il-retenir-de-l-audition-des-patrons-d-apple-facebook-google-et-amazon-par-le-congres-americain.N990419>

Le 29 juillet 2020, Sundar Pichai (Alphabet, maison-mère de Google), Tim Cook (Apple), Mark Zuckerberg (Facebook) et Jeff Bezos (Amazon)

ont été interrogés par les élus américains devant la Commission judiciaire de la Chambre des représentants.<sup>36</sup> Lors de cette audition, il a été considéré que leurs pratiques avaient un effet démesuré sur l'économie et la démocratie américaines. Au niveau économique, ces plateformes « abusent toutes de leur contrôle sur les technologies actuelles pour étendre leur pouvoir » en imposant leurs propres produits, ce qui nuirait à une saine concurrence et aux consommateurs. Ainsi, cette commission estime que ces sociétés doivent être démantelées pour assurer le respect des lois antitrust américaines et n'exclut pas de recourir à de nouveaux décrets si nécessaire.

Reste à savoir toutefois si le Congrès décidera de réviser les lois anticoncurrentielles existantes et si de fait, ce démantèlement aura bien lieu, à l'image de Bell Telephone Company dans les années 80.

Finalement, tous les États semblent s'accorder sur la nécessité de mettre fin au monopole des GAFAM et paradoxa-

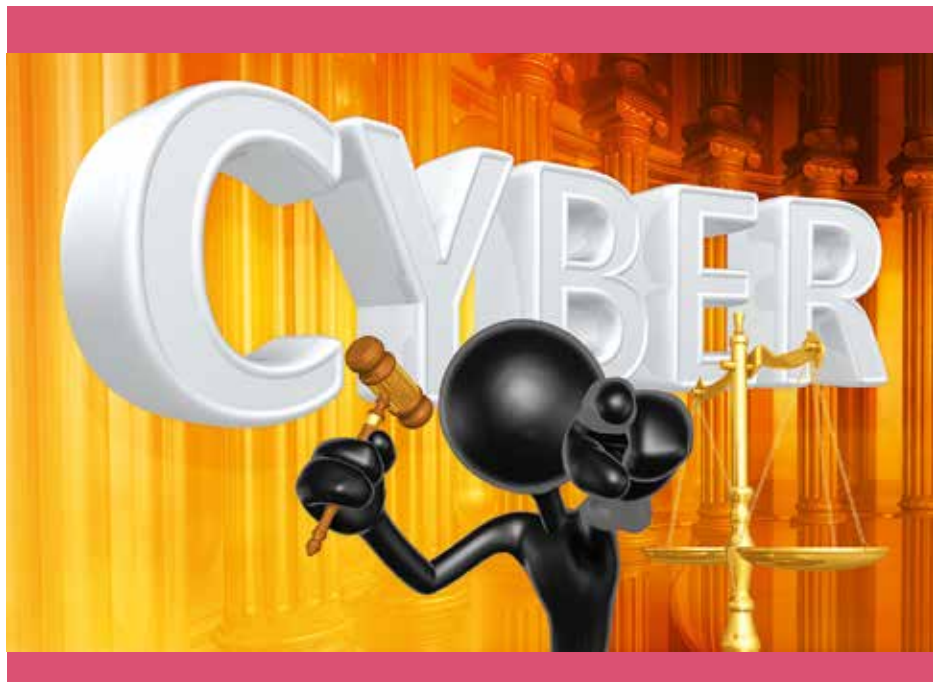
lement, si l'Union Européenne ne parvient pas à mettre fin à la domination des entreprises américaines, la solution pourrait provenir des États-Unis ! Ce mouvement est d'autant plus intéressant à observer que s'agissant de la protection des données, il semblerait que le RGPD, pourtant si décrié par certaines sociétés américaines, inspirerait la législation de certains États fédéraux américains, puisque le gouvernement de l'État de Californie, berceau de la Silicon Valley, a adopté en juin 2018 le « California Consumer Privacy Act ».

d'une souveraineté numérique européenne.

(37) Puisqu'elle concerne uniquement les entreprises dont le chiffre d'affaires annuel (généré sur le territoire californien) est supérieur ou égal à 25 millions de dollars ayant au moins 50 000 consommateurs californiens et dont la moitié des revenus provient de la vente des données personnelles des consommateurs et si les peines prévues semblent dérisoires (jusqu'à 7500 \$ contre 20 millions d'euros pour le RGPD).

Cette réglementation, entrée en vigueur le 1<sup>er</sup> janvier 2020, instaure plus de transparence quant à la finalité de la collecte des données et des droits d'information, d'accès et d'opposition à la vente des données collectées. Si elle a une portée nettement moins importante que le RGPD<sup>37</sup>, il n'en reste pas moins que la volonté de contrer les sociétés

en position de monopole sur le marché numérique semble devenir de plus en plus unanime et pourrait tout à fait aboutir à un démantèlement, ce qui pourrait, enfin, favoriser l'émergence



© Scott Maxwell - AdobeStock

## AUTEURE

**Maître Cécile Doutriaux, avocate, fondatrice du cabinet Juris Défense Avocats, est membre de la Chaire Cyberdéfense & Cybersécurité des écoles de Saint-Cyr SOGETI & THALÈS, de la Réserve Citoyenne Cyberdéfense et auditeur de l'IHEDN. Elle enseigne le droit des technologies de l'informatique et de la communication au Conservatoire National des Arts & Métiers (formation labellisée par la CNIL).**

## CLOUD ACT

The Clarifying Lawful Overseas Use of Data Act

### US CLOUD-ACT : UNE VISION EUROPEENNE RESTRICTIVE ET PORTEUSE DE VALEURS

L'objectif de l'US CLOUD ACT est de faciliter le traitement judiciaire nord-américain de données et de Méta-données numériques, y compris les interceptions de communications, situées hors des États-Unis. Il impose une coopération bilatérale entre les États-Unis et des États « agréés » en abrogeant les mécanismes classiques de droit international et en imposant de fait une extra-territorialité judiciaire. Se posent les questions de la nature des données, de l'évolution de décisions des autorités judiciaires américaines quant aux réquisitions des autorités légales et fédérales, des conditions de stockage, de communication à des tiers et de conservation des données.

L'Union européenne penche pour la réalisation d'un accord sur l'accès transfrontière aux données, au niveau européen et non national, uniquement à des fins judiciaires. Il s'agit de faciliter l'obtention de la preuve numérique par les enquêteurs et magistrats européens au cours de l'enquête pénale tout en assurant aux citoyens le respect de leurs droits. Elle n'intègre donc pas une finalité de « renseignement » comprise, de fait, dans l'initiative américaine. La Commission européenne se situe donc au niveau de la protection des principes, règles et valeurs communes des Etats-Membres et de la défense de l'espace européen de liberté, de sécurité et de justice.

# Le US Cloud Act

vu de France : craintes légitimes ou peurs inutiles ?

Par Emmanuelle Legrand

# S

**Sans prétention d'exhaustivité, le présent article a pour ambition de proposer au lecteur quelques clés**

(1) Le texte est disponible en anglais à : <https://www.govtrack.us/congress/bills/115/s2383/text>

(2) <https://www.lesechos.fr/tech-medias/high-tech/bruno-le-maire-vent-debout-contre-le-cloud-act-americain-991515>

**de lecture du US Cloud Act et de la recommandation de la Commission européenne en vue de négociations UE-US, à partir de l'analyse des textes, afin de mieux comprendre le cadre dans lequel pourrait s'inscrire l'action de l'Union européenne.**



**EMMANUELLE LEGRAND**

**Magistrate de liaison française en Europe du Sud Est**

Signé par le président Trump, le 23 mars 2018, le US Cloud Act a suscité de nombreuses réactions aux États-Unis comme en Europe. En France, des craintes ont

(3) Cet accord a été signé en octobre 2019 : <https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists> ; en décembre et janvier 2020, le Département de justice américain a adressé sa certification au Congrès américain, avec une prise d'effet prévue en juillet 2020 : <https://www.justice.gov/dag/page/file/1236281/download>.

(4) <https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us> ; l'Australie a préparé une loi à cette fin : <https://www.lexology.com/library/detail.aspx?g=2cf0f577-4a6b-4523-b04c-4674296f9f74>.

(5) <https://www.consilium.europa.eu/fr/policies/e-evidence/>

notamment été exprimées quant aux risques encourus par les entreprises nationales<sup>2</sup>.

En octobre 2019, le département de justice américain annonçait la signature du premier « Executive agreement » (accord gouvernemental) avec le Royaume-Uni<sup>3</sup>. Quelques jours plus tard, l'ouverture de négociations avec l'Australie était officialisée<sup>4</sup>.

De son côté, la Commission européenne présentait, en avril 2018, au Conseil ses propositions « E-evidence »<sup>5</sup> visant à faciliter l'accès transfrontière à la preuve

numérique et recevait mandat, le 6 juin 2019, pour ouvrir des négociations avec les États-Unis sur le même sujet. Les deux initiatives européennes partent du constat largement partagé par les magistrats et enquêteurs européens de la lenteur des outils traditionnels de l'entraide pénale, peu adaptés aux spécificités de la preuve électronique. Ce constat a déjà conduit les services d'enquête de nombreux pays à s'adresser directement aux fournisseurs de services américains pour obtenir des données techniques, et ce sans cadre juridique international clair, laissant ainsi le droit national et la jurisprudence fixer les limites d'une pratique développée pragmatiquement au fil du temps.

(6) On opposera ici par souci de simplicité les données de trafic, qui ne révèlent pas le contenu des échanges entre les personnes mais apportent des informations techniques sur ces échanges, aux données de contenu, qui contiennent le contenu d'une communication écrite ou verbale.

Les échanges directs des enquêteurs avec les fournisseurs de services américains reposent en l'état sur deux principes : d'une part, en général, seules les données de trafic<sup>6</sup>, souvent utiles pour orienter l'enquête, peuvent être communiquées aux enquêteurs étrangers, conformément au droit

américain. D'autre part, cette communication aux services d'enquête étrangers intervient sur une base volontaire, après analyse au cas par cas par les fournisseurs de service américains, selon les règles fixées par eux et par le droit américain<sup>7</sup>. C'est donc aujourd'hui dans un cadre

(7) Voir notamment la recommandation de la Commission européenne en faveur de l'ouverture de négociations avec les États-Unis en vue d'un accord sur l'obtention transfrontière de la preuve électronique en matière pénale, page 5 : « As regards non-content data, due to the growing number of Mutual Legal Assistance requests addressed to the United States of America, the U.S. authorities have encouraged EU law enforcement and judicial authorities to request non-content data from U.S. service providers directly, and U.S. law allows but does not require U.S.-based service providers to respond to such requests. An EU-U.S. Agreement would provide more certainty, clear procedural safeguards and reduce fragmentation for EU authorities to access non-content data held by U.S. service providers. It would also allow for reciprocal access by U.S. authorities to data held by EU service providers. »

(8) On pourra citer notamment Christakis, Theodore, 21 Thoughts and Questions about the UK/US CLOUD Act Agreement: (and an Explanation of How it Works – With Charts) (October 13, 2019). European Law Blog, October, 2019, Available at SSRN: <https://ssrn.com/abstract=3469704>

juridique incertain, reposant pour beaucoup sur la bonne volonté des acteurs privés, que les enquêtes pénales en France, comme en Europe, peuvent avancer, ou pas.

De nombreuses publications ont fait état des craintes suscitées par la promulgation de l'US Cloud Act. Toutefois, peu ont tenté de déchiffrer les termes employés, pourtant riches d'enseignements<sup>8</sup>.

Les craintes exprimées sur le US Cloud Act apparaissent-elles véritablement fondées, à la lumière des termes choisis par ses rédacteurs et par l'Union européenne ?

## Le US Cloud Act (1<sup>ère</sup> partie) : la clarification d'une pratique en matière d'obtention de données stockées à l'étranger

L'US Cloud Act s'organise en deux parties.

La première constitue le « Microsoft fix »



(9) Les modifications touchent le titre 18 du US Code, intitulé « Crimes and criminal procedure », et concernant donc a priori les enquêtes pénales. Plus précisément, ce sont les chapitres 119 (« Wire and electronic communications interception and interception of oral communications ») et 121 (« Stored wire and electronic communications and transactional records access ») qui sont modifiés par le Cloud Act.

(10) <https://www.nextinpact.com/article/27715/105782-une-etude-dresse-lesenjeux>

(11) Voir 18 U.S. Code §2713 : <https://www.law.cornell.edu/uscode/text/18/2713>

en amendant la loi de procédure américaine et en entérinant la possibilité pour les autorités américaines d'accéder à des données quel que soit leur lieu de stockage.

Le Cloud Act modifie ainsi le titre 18 du US Code<sup>9</sup>.

Il clarifie une pratique qui avait été remise en cause par la société Microsoft, dans le cadre du bras de fer juridique engagé en 2014 contre le gouvernement américain, en refusant de communiquer à ce dernier des données stockées en Irlande<sup>10</sup>. La promulgation du Cloud

Act, sans attendre la décision de la Cour suprême, est ainsi venue clore le débat juridique.

Désormais, une autorité américaine peut légalement requérir la production de données auprès de sociétés, quel que soit le lieu de stockage de ces données<sup>11</sup>.

### Le US Cloud Act et le juge américain : à quelles entreprises ne s'appliquera-t-il pas ?

Le Cloud Act ne précise toutefois pas à quelles entités cette obligation de communication des données aux autorités américaines est limitée. Ainsi, par défaut,

on peut penser que toute entreprise

(12) Aucun élément en sens contraire ne semblant en l'état amener à une autre conclusion. Dans le même sens que l'auteur : <https://www.justice.gov/opa/press-release/file/1153446/download>

(13) 18 U.S. Code § 2713 « Required preservation and disclosure of communications and records »

(14) <https://www.law.cornell.edu/us-code/text/18/2713>

(15) Cette dernière formulation suscite un intérêt particulier lorsque l'on s'interroge par exemple sur la situation d'une société française qui n'aurait de lien avec les États-Unis que son service de stockage de données en ligne.

(16) <https://ppp.worldbank.org/public-private-partnership/legislation-regulation/framework-assessment/legal-systems/common-vs-civil-law>

tombant sous le coup de la compétence des juridictions américaines (US jurisdiction) est susceptible d'être concernée<sup>12</sup>.

La section §2713 de l'*US Code*<sup>13</sup> définit néanmoins le fournisseur de service concerné comme étant celui qui *a la possession, la garde ou le contrôle* des données, où que se situe la communication<sup>14</sup>. Cette obligation s'applique aux fournisseurs de service de communication électronique comme aux services informatiques à distance<sup>15</sup>.

Les sociétés américaines ne semblent donc pas être les seules concernées. Le droit américain, rappelés-le, est un droit de *Common law*, qui évolue

essentiellement par les décisions des tribunaux<sup>16</sup>. Or, nul ne sait en l'état comment le juge américain interprétera la notion de « US jurisdiction » dans l'application spécifique du *Cloud Act*.

Comparaison n'est pas raison. Néanmoins, il n'est pas inutile de rappeler que les

(17) <https://www.kirkland.com/publications/article/2019/03/can-your-overseas-company-be-taken-to-us-court>

(18) En matière civile notamment, il est question de « long-arm jurisdiction » ou « long-arm statute » : <https://www.law.cornell.edu/wex/long-arm-statute>. Littéralement, les autorités judiciaires américaines peuvent donc, selon les domaines juridiques et les textes et jurisprudences, recourir à la théorie du « bras long » pour retenir leur compétence, parfois qualifiée d'extraterritorialité par certains observateurs. Voir à ce propos le rapport d'information sur l'extraterritorialité de la législation américaine déposée en octobre 2016 par la Commission des affaires étrangères et la Commission des finances de l'Assemblée nationale : <http://www.assemblee-nationale.fr/14/pdf/rap-info/i4082.pdf>

(19) Voir notamment sur la loi dite de blocage française du 26 juillet 1968 : <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JOR>

(20) En se dispensant ainsi du processus législatif habituellement applicable en matière de traités internationaux. Voir notamment C. Bradley, J. Landman Goldsmith, O.A. Hathaway, *The failed transparency regime for executive agreements: an empirical and normative analysis* : <https://www.ssrn.com/abstract=3589900>

juridictions américaines peuvent parfois retenir, notamment en matière civile<sup>17</sup>, leur compétence 'élargie'<sup>18</sup>, parfois même en tenant volontairement en échec les lois de blocage étrangères<sup>19</sup>.

Reste à savoir si, dans l'hypothèse d'une interprétation large du juge américain sur l'application du Cloud Act aux sociétés étrangères, ces dernières estimeront devoir répondre aux demandes des autorités américaines ou si les initiatives nationales ou européennes leur apporteront des réponses.

### La réponse de l'Union européenne (2<sup>e</sup> partie) : négocier un accord complet au niveau européen en matière pénale

Dans sa seconde partie, l'*US Cloud Act* autorise également le gouvernement américain à conclure des accords gouvernementaux (*Executive agreements*), avec des gouvernements étrangers<sup>20</sup>.

(21) A noter sur ce point que le US Cloud Act modifie également les dispositions du US Code relatives aux outils de pen register et de trap and trace (voir notamment 18 U.S.Code §3121, qui crée une exception au principe de délivrance d'un mandat du juge notamment dans le cas d'une demande d'un gouvernement étranger dans le cadre d'un « executive agreement »). <https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf>.

(22) [https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence\\_en](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en)

(23) Contrairement à ce que certains observateurs ont pu percevoir, les propositions E-Evidence de la Commission européenne d'avril 2018 ne pouvaient pas constituer une « réponse » au US Cloud Act, promulgué en mars 2018, car elles résultent directement des engagements pris par la Commission européenne dès 2015 dans le cadre de l'agenda sur la politique européenne de sécurité ([https://ec.europa.eu/commission/presscorner/detail/en/IP\\_15\\_4865](https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4865)), de la déclaration commune des ministres de la justice et de l'intérieur des Etats-Membres et des représentants des institutions européennes sur le sujet de l'accès à

L'objectif affiché est de faciliter l'obtention des données électroniques, y compris de contenu et en temps réel (non stockées), notamment des interceptions de communications<sup>21</sup>, sous réserve pour l'État partenaire de répondre aux exigences fixées par le *Cloud Act*, et le cas échéant après avoir modifié sa loi interne. C'est à cette seconde partie de l'*US Cloud Act* que semble répondre la recommandation de la Commission européenne<sup>22</sup>, présentée au Conseil en février 2019, en vue de l'ouverture de négociations avec les États-Unis. Cette recommandation eut pu paraître inutile si, comme cela a pu être évoqué de manière erronée, les propositions E-Evidence d'avril 2018, toujours en cours de discussion, avaient constitué une réponse au *Cloud Act*. Tel ne semble pas être le cas<sup>23</sup>.

S'agissant de négociations UE-US, la lecture attentive des termes

la preuve électronique au lendemain des attentats de Bruxelles en 2016 (<https://www.consilium.europa.eu/fr/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/>), des consultations réalisées par la Commission européenne, des conclusions du Conseil de l'Union européenne demandant à la Commission en novembre 2017 de faire des propositions d'amélioration de l'accès trans-frontière à la preuve électronique (<https://www.consilium.europa.eu/media/31666/st14435en17.pdf>), et à une étude d'impact détaillée, le tout bien avant la promulgation du US Cloud Act. La véritable question est donc de savoir si le Cloud Act ne constitue pas, lui, une réponse aux efforts annoncés de la Commission de faciliter l'accès aux données au sein de l'Union européenne.

(24) Extrait de la recommandation de la Commission européenne, du 5 février 2019 page 4: « The European Union has an interest in a comprehensive agreement with the United States of America, both from the perspective of protecting European rights and values such as privacy and personal data protection and from the perspective of our own security interests. »

(25) <https://www.justice.gov/dag/page/file/1153466/download>



© EisenhansL - Fotolia

Le CLOUD Act est une alternative aux réglementations découlant du droit de l'UE. Son approche pose la question de la construction d'un modèle cohérent d'échange et de protection des données personnelles et d'échange d'informations probatoires dans le cadre de procédures pénales.

choisis par la Commission européenne, adoptés par le Conseil, suggère ainsi qu'elle n'entend pas inscrire ces négociations dans le cadre d'un accord gouvernemental, ni dans les conditions fixées par le Cloud Act. La possibilité d'un simple accord-cadre ne semble pas non plus être la piste privilégiée par la Commission<sup>24</sup>.

En effet, tandis que le Cloud Act favorise la conclusion d'accords

(26) La recommandation de la Commission européenne adoptée en juin 2019 par le Conseil mentionne clairement l'intérêt d'un accord au niveau européen : « An agreement between the European Union and the United States would offer a number of practical advantages: (...) It would reduce the risk of fragmentation of rules, procedures, and harmonise the rights and safeguards through a single negotiation mandate for all European Union Member States with the United States ensuring non-discrimination between European Union Member States and their nationals (...) »

bilatéraux avec des Etats remplissant les conditions fixées par les États-Unis en matière d'État de droit<sup>25</sup>, la Commission, gardienne des traités, semble adopter l'approche consistant à refuser qu'un État tiers s'octroie unilatéralement le rôle d'évaluateur de la situation de l'État de droit dans l'Union européenne, au profit d'une application harmonisée<sup>26</sup> du droit et des valeurs de l'Union au sein des États-Membres,

(27) On pourra citer à titre d'exemple le mandat d'arrêt européen, la décision d'enquête européenne, le renforcement des droits des victimes, ou celui des droits des suspects et accusés.

(28) Extrait du US Cloud Act : "the term 'qualifying foreign government' means a foreign government".

(29) [https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence\\_en](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en)

(30) Du point de vue de l'auteur, le terme anglais original « order » ne saurait, du point de vue du droit français, recouvrir la notion de l'injonction, bien qu'utilisée par les juristes-linguistes de la Commission européenne dans la version française de la recommandation de la Commission européenne. Cette notion d'injonction, utilisée en matière civile, a en effet des conséquences juridiques totalement différentes de celle évoquée ici en matière pénale. Le terme « order » se rapproche donc davantage en droit français de la notion de réquisition judiciaire, en ce que cela oblige le destinataire à y répondre.

et du maintien d'un espace commun de liberté, de sécurité et de justice.<sup>27</sup>

Ainsi, si le fait de savoir si l'Union européenne pouvait ou non être qualifiée de gouvernement étranger pour conclure un accord gouvernemental selon les termes du US Cloud Act<sup>28</sup> a pu susciter des réflexions intéressantes, ce débat est en réalité sans grand intérêt, l'Union européenne ne s'étant pas engagée dans cette voie, tout en en prenant acte. Dès le titre de la recommandation de la Commission, le ton semble donné<sup>29</sup> : il s'agit en l'état de négocier un accord sur l'accès transfrontière à la preuve électronique, au niveau européen et non national, et uniquement à des fins de coopération judiciaire en matière pénale.

Cet intitulé n'a pas suscité beaucoup de réactions mais est pourtant riche de sens, puisque l'Union européenne fixe un cadre clair pour les négociations, et a fortiori quant à

(31) Le US Cloud Act fait seulement référence au « US gouvernement » et ne précise pas que son champ d'application se limite aux procédures judiciaires. Il semble préciser, certes, l'intervention d'un juge dans certains cas. Toutefois, pour ne citer l'exemple que du FBI, ce dernier ne dispose pas seulement des pouvoirs que l'on assimilerait en France à de la police judiciaire (<https://www.wsj.com/articles/fbi-wants-audit-firm-to-review-how-it-makes-fisa-wiretap>). Par ailleurs, la notion de « law enforcement » reste très large, et la mention de l'intervention d'un juge dans le texte du Cloud Act ne préjuge pas forcément, en l'absence de toute précision complémentaire, du cadre juridique dans lequel s'exercerait la communication de données. Le Cloud Act, s'agissant des exigences applicables aux États contractants en matière de minimisation des procédures, fait d'ailleurs une référence explicite aux procédures en vigueur selon le Foreign Intelligence Surveillance Act de 1978 (50 U.S.C. 1801).

l'utilisation des données qui seraient éventuellement recueillies en vertu d'un tel accord. Or, le texte américain précise, quant à lui, en modifiant la section §2523 du titre 18 du US Code, que les « réquisitions »<sup>30</sup> aux entreprises doivent avoir pour objectif d'obtenir de l'information relative à la prévention, la détection, l'investigation ou la poursuite des infractions graves, incluant le terrorisme. Le *US Cloud Act* ne définit pas la notion d'infraction grave. Le droit français non plus.

La première difficulté soulevée par le texte du Cloud Act est de savoir de quel type de procédure on parle, puisque le rôle premier du système pénal n'est pas, en principe, de prévenir et de détecter mais de réprimer les infractions commises. Or, le Cloud Act ne précise pas qu'il s'appliquerait aux

seules procédures pénales. Il ne précise pas non plus quelles seraient les autorités américaines qui s'adresseraient aux fournisseurs de services de l'État contractant<sup>31</sup>.

(32) A cette époque, le Royaume-Uni était pourtant toujours soumis, a priori, au principe de loyauté envers l'Union européenne.

(33) Voir l'article de Paul Greaves et Peter Swire « New developments for the UK and Australian executive agreements with the US under the Cloud Act » : <https://www.crossborderdataforum.org/new-developments-for-the-u-k-and-australian-executive-agreements-with-the-u-s-under-the-cloud-act-2/>

Dans cet article les auteurs notent notamment que la proposition de loi visant à adapter la procédure australienne mentionne la possibilité pour les autorités de solliciter les fournisseurs de service dans le cadre du renseignement. Ce choix n'est donc pas anodin.

(34) Alliance des services de renseignements américains, australiens, britanniques, canadiens et néo-zélandais : [https://fr.wikipedia.org/wiki/Five\\_Eyes](https://fr.wikipedia.org/wiki/Five_Eyes)

(35) Citons entre autres le principe du contradictoire, de la proportionnalité, du respect des droits de la défense ou encore le droit au recours effectif.

En réalité, on relèvera que le premier accord gouvernemental conclu par les États-Unis l'a été avec le Royaume-Uni<sup>32</sup>, avant de se tourner vers l'Australie<sup>33</sup>. Autrement dit, des accords entre trois pays du club dit des « Five Eyes »<sup>34</sup>. La question qu'on ne formule jamais clairement est donc celle-ci : l'objectif principal du Cloud Act et des accords gouvernementaux est-il vraiment de faciliter l'obtention de la preuve numérique dans le cadre pénal, dans le respect des principes généraux de la procédure pénale des États<sup>35</sup>, ou plutôt de faciliter le transfert de données collectées dans le cadre des activités de renseignement<sup>36</sup>? Cette question demeure entière mais d'importance, lorsqu'on analyse les termes choisis par la Commission européenne dans sa recommandation au Conseil.

Ainsi, sans préjuger de l'issue des négociations, la Commission,

(36) Aux États-Unis, l'autorisation nécessaire pour certaines activités de renseignement relève de la compétence de la United States Foreign Intelligence Surveillance Court. Les activités de renseignement ne sont donc pas totalement dépourvues d'un contrôle par un juge, sans que cela ne soit régi par les règles du procès pénal à proprement parler. La notion de juge ou de tribunal ne permet dès lors pas à elle seule de déterminer le cadre d'utilisation du US Cloud Act. loi FISA (Foreign Intelligence Surveillance Act) s'applique aux activités.

(37) Le mot « réciprocal » apparaît à 7 reprises dans la recommandation de la Commission européenne.

(38) La définition de la « US person » est donnée à l'article 18 U.S. Code §2523 et inclut tout citoyen ou national des États-Unis, tout étranger résident permanent légal, toute association de fait (« unincorporated ») dont un nombre substantiel de membres sont citoyens des États Unis ou étrangers résidents permanents légaux, ou toute société créée aux États-Unis.

en rappelant sa compétence, semble avoir proposé d'atteindre non un accord gouvernemental ou un accord-cadre, mais un accord complet au niveau européen assurant la protection adéquate et non discriminatoire des droits des citoyens de l'UE, dans le respect des principes et valeurs de l'Union, uniquement dans le cadre des procédures pénales et assorti de conditions claires et de garanties permettant aux autorités judiciaires européennes, dans le prolongement des propositions E-Evidence, d'user d'une nouvelle possibilité procédurale adaptée aux spécificités de la preuve numérique.

Le texte européen semble ainsi partir d'un présupposé différent du Cloud Act : la recherche d'un accord complet en matière pénale, aux conditions négociées, équilibrées, et fondées sur la réciprocité.

A titre d'exemple, l'objectif de réciprocité

recherché par la Commission européenne<sup>37</sup> est intéressant, alors même que le Cloud Act exclut toute demande de données visant directement ou indirectement les « US persons », dont la définition apparaît bien large<sup>38</sup>.

Si les négociations étaient intervenues dans le cadre de l'US Cloud Act, l'Union européenne, en affirmant son objectif de réciprocité, ne pourrait pas ignorer que l'application du principe de non-discrimination des citoyens de l'Union conduirait à un accord qui deviendrait presque sans intérêt pour les deux Parties.

(39) Le Conseil, dans sa directive de négociation, a repris l'essentiel des termes proposés par la Commission européenne, ne négligeant pas le fait d'inclure une clause relative à l'exclusion des faits pour lesquels la peine de mort ou la perpétuité réelle est encourue aux Etats-Unis.  
<https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/fr/pdf>.

Ces éléments conduisent à penser que la Commission européenne n'a pas entendu se situer au niveau du Cloud Act, mais à celui de la protection des principes, règles et valeurs communes des Etats-Membres et de la défense de l'espace européen de liberté, de sécurité et de justice<sup>39</sup>.

### La proposition européenne : vers un accord équilibré, protecteur des droits et des données ?

Le constat de l'Union européenne est celui des praticiens, demandeurs d'outils juridiques plus adaptés en matière d'obtention de preuve numérique. Toutefois, pris entre l'approche unilatérale du Cloud Act d'un

côté, et le RGPD et les propositions E-Evidence de l'autre, certains fournisseurs de services pourraient se retrouver confrontés à des conflits de loi<sup>40</sup>. Ainsi, l'un des objectifs affichés par la Commission semble de prévenir, et le cas échéant, de résoudre ces éventuels conflits de loi, tout en clarifiant le cadre juridique d'obtention des preuves numériques auprès des fournisseurs de services américains.

(40) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

(41) Autrement dit, le US Cloud Act ne pose en lui-même aucune obligation expresse pour les fournisseurs de service, ni aucune sanction. C'est ainsi qu'il appartient au pays partenaire, s'il souhaite conclure un accord gouvernemental, d'amender sa législation interne pour lui donner le cas échéant une portée extraterritoriale et pouvoir sanctionner les manquements, à l'instar de ce qu'ont fait les Etats-Unis avec la première partie du US Cloud Act.

Toutefois, le *Cloud Act* s'inscrit dans une philosophie juridique propre au droit américain. Ainsi, ce texte n'impose pas, en lui-même, d'obligation aux fournisseurs de services d'un Etat contractant. Il vise uniquement à lever les obstacles juridiques leur interdisant de répondre à une autorité étrangère, comme les lois de blocage, sur la base d'une coopération volontaire. Il ne semble toutefois résoudre ni le problème de l'absence de réponse ni les conséquences juridiques qui en découleraient, sauf à modifier son droit interne pour s'octroyer une compétence extraterritoriale.<sup>41</sup>

(42) Arrêt CJUE C-311/18 du 16 juillet 2020, Data Protection Commissioner contre Facebook Ireland Ltd, Maximilian Schrems, EE-CL:EU:C:2020:559 (<http://curia.europa.eu/juris/document/document.jsf?jsessionid=49B>)

(43) Le Bouclier de Protection des Données, mieux connu sous le nom de « Privacy Shield », est un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux États-Unis. Ce mécanisme est par conséquent considéré comme offrant des garanties juridiques pour de tels transferts de données. (Source CNIL).

La recommandation de la Commission semble en revanche adopter une autre approche, plus proche de ce que nous connaissons en droit français notamment, visant à fixer des règles communes, à définir les conditions dans lesquelles l'on pourrait s'opposer aux décisions des autorités judiciaires, tout en assurant un droit au recours effectif.

Par ailleurs, la nécessité d'un accord entre l'Union européenne et les États-Unis assurant l'équilibre entre l'efficacité d'un outil disponible pour les autorités judiciaires et la protection adéquate des droits des personnes et de leurs données apparaît encore plus trouver son

sens au regard de l'arrêt *Schrems II* du 16 juillet 2020<sup>42</sup>, par lequel la Cour de justice de l'Union européenne a invalidé le bouclier de protection des données<sup>43</sup> (*Privacy Shield*) conclu entre l'Union européenne et les États-Unis.

Ainsi, si le Privacy Shield est un accord visant les transferts de donnée à des fins

commerciales, la Cour, se référant à la Charte des droits fondamentaux de l'Union européenne, pointe les lacunes de la loi américaine en matière de sécurité nationale, qui, en l'état, ne permet pas d'assurer une protection adéquate, notamment en termes de proportionnalité et de recours effectif.

(44) Voir notamment Theodore Christakis, *After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, juillet 2020, [https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/#para\\_2](https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/#para_2)

(45) Voir notamment <https://cloud.google.com/blog/products/infrastructure/announcing-google-grace-hopper-sub-sea-cable-system> et <https://www.lemonde.fr/pixels/article/2020/07/30/google-a-commence-a-deployer-un-nouveau-cable-internet-transatlantique>

La lecture de cette décision soulève nécessairement des questions concernant d'autres accords transatlantiques existants<sup>44</sup> s'agissant des transferts de données en matière de sécurité et de justice.

Or, dans sa recommandation au Conseil en vue de l'ouverture de négociations, la Commission européenne rappelait justement la nécessité de garantir la protection des principes et droits fondamentaux reconnus par la Charte européenne des droits fondamentaux.

Cette décision apparaît d'autant plus intéressante que le 28 juillet 2020, Google annonçait le déploiement d'un nouveau câble sous-marin transatlantique pour le transfert de données internet<sup>45</sup>, tandis que le sujet du chiffrement des





© Fotolia - 118081089

données continue de diviser les autorités en quête d'éléments probants et les citoyens en recherche légitime de protection de leurs données.

### Conclusion

Les débats sur les initiatives de la Commission européenne en matière d'obtention transfrontière de la preuve numérique sont légitimes et souhaitables dans une société démocratique. Le défi de l'Union européenne est d'aboutir à une solution qui facilite le travail des enquêteurs et des magistrats européens dans les enquêtes pénales où l'obtention de la preuve numérique est souvent déterminante, tout en assurant aux citoyens le nécessaire respect de leurs droits et la protection de leurs données.

En l'état du droit, les praticiens français

et européens se heurtent souvent au bon vouloir des fournisseurs de service qui se réfugient derrière la législation étrangère, tout en développant leurs services sur le marché européen.

Si les enquêtes n'avancent pas faute d'éléments de preuve numérique, cela se fait nécessairement au détriment des victimes et au bénéfice, notamment, de la criminalité organisée et transnationale. Si les enquêtes avancent du fait d'une pratique pragmatique qui attend toujours d'être rattrapée par un cadre juridique international clair et efficace, cela peut se faire au détriment des droits des personnes suspectées, alors que la société civile attend une réponse de l'Union européenne qui soit à la hauteur de l'enjeu de la protection des données personnelles et des valeurs démocratiques qu'elle veut porter. C'est entre ces deux



écueils que l'Union européenne doit trouver la réponse juridique adaptée. Elle n'a pas d'autre choix, désormais, que de la trouver afin de protéger les droits et les données des citoyens de l'Union à la hauteur des valeurs qu'elle porte.

Ainsi, à ceux qui s'interrogent sur l'utilité d'un accord UE-US, tandis que les propositions E-Evidence sont toujours en discussion, une question mérite d'être posée : en l'absence d'un accord UE-US protecteur des droits et principes de l'Union, comment les entreprises françaises et européennes, dans un monde globalisé, peuvent-elles protéger efficacement leurs données contre une application extensive, unilatérale et incertaine du Cloud Act ?

## AUTEURE

**Emmanuelle Legrand est actuellement magistrate de liaison française en Europe du Sud Est. Elle a exercé précédemment des fonctions juridictionnelles au parquet de Nanterre où elle a notamment été référente cybercriminalité, puis en qualité de juge d'instruction au pôle financier JIRS de Paris, puis à Nanterre, spécialisée en matière économique et financière et en cybercriminalité.**

**Elle a également exercé au Bureau de l'entraide pénale internationale du ministère de la justice, ainsi qu'à la Commission européenne, en qualité d'experte nationale détachée, où elle a travaillé sur les questions de coopération judiciaire et de preuve numérique. Elle a notamment fait partie de la Task Force E-evidence, et participé aux travaux de la Commission européenne en vue de l'ouverture de négociations avec les Etats-Unis sur la preuve numérique.**

**Elle intervient régulièrement à l'École nationale de la magistrature en formation initiale et continue, comme expert en cybercriminalité pour le Conseil de l'Europe, ou encore dans le cadre de la formation des enquêteurs spécialisés.**

**Elle est également titulaire d'un diplôme d'université en Cybercriminalité obtenu à l'Université de Montpellier 1, ainsi que d'un LL.M. en droit américain obtenu à la University of Texas School of Law. Elle est également auditrice de la 1<sup>ère</sup> session nationale INHESJ-IHEDN sur la Souveraineté numérique et la Cybersécurité, et préside actuellement l'association des auditeurs de la session nationale.**



© AI par melano works

## UNE ÉCOSPHÈRE D'IA REGULÉE POUR CONCILIER L'INNOVATION ET LA CONFIANCE

Les conditions sont réunies pour une évolution généralisée des techniques d'IA : disponibilité et diversité des données, développement des offres et performance des équipements informatiques. L'IA génère des inquiétudes quant aux conséquences sociétales de son emploi dans toutes les activités et sa supposée prépondérance dans la sphère décisionnelle.

Sa gouvernance juridique est considérée par certains auteurs comme impérative. Faut-il encore en cerner le périmètre. Les domaines de la responsabilité, de la propriété intellectuelle et de la protection de la vie privée méritent l'exploration de nouvelles voies juridiques et éthiques pour accompagner ou anticiper les effets de systèmes d'IA complexes et évolutifs.

Cependant, si l'IA est une activité concurrentielle et stratégique, la disparité des régimes légaux régionaux ne préjuge pas d'une norme internationale dans l'immédiat. Cependant, l'Europe dégage naturellement une vision éthique. Un contrôle humain, le respect de la vie privée, la transparence, la non-discrimination et la responsabilisation sous-tendent les recommandations expresses de ses experts. Sur le plan international, L'OCDE milite pour la création d'un écosystème d'AI de confiance et centré sur l'humain régulé par des dispositifs éthiques et réglementaires. La confiance ne pourra résulter à terme que de la construction d'une norme internationale qui, sans entraver l'innovation, préserve les libertés individuelles.

# L'intelligence artificielle

## centrée sur l'humain : droit ou éthique ?

Par Sabine Marcellin

**L**

Les progrès accomplis par l'intelligence artificielle permettent à des machines d'effectuer des tâches cognitives qui étaient réservées aux humains par le passé. L'IA peut contribuer à renforcer la cybersécurité ou assister les médecins dans l'élaboration de leur diagnostic. Les applications sociales de l'IA sont sources de progrès mais aussi de risques. Certains chercheurs, comme Stephen Hawking, ont exprimé la crainte que l'IA ne devienne une menace pour l'humanité. Face à ces risques, de nombreux gouvernements et organi-

sations ont entamé des réflexions sur les principes de cadrage de l'IA. Ces principes prendront-ils la forme de règles juridiques ou éthiques ?



**SABINE MARCELLIN**

Avocat associé  
DLGA

Parmi les nombreuses conceptions de l'intelli-

gence artificielle (IA), la définition de l'OCDE d'un système d'IA est un système automatisé qui, pour un ensemble donné d'objectifs définis par l'homme, est en mesure d'établir des prévisions, de formuler des recommandations ou de prendre des décisions influant sur des environnements réels ou virtuels.

Aujourd'hui, les conditions sont réunies pour une évolution généralisée des techniques d'IA : disponibilité et diversité des données, développement des offres et performance des équipements informatiques.

(1) Un biais algorithmique est le fait que le résultat produit par l'algorithme ne soit pas neutre, loyal ou équitable. Cela peut provenir du fait que les données utilisées reflètent des interprétations et valeurs existantes.

La maîtrise de l'IA représente des enjeux d'innovation et de productivité. Entre fascination et inquiétude, ils s'accompagnent également des risques parmi lesquels la difficile explicabilité des décisions, les effets des

biais des algorithmes<sup>1</sup>, l'atteinte à la vie privée et la dépendance technique de quelques acteurs incontournables. Les nombreuses études françaises et internationales sur le thème de l'IA évoquent également d'autres risques : les accidents, la limitation des emplois, l'automatisation de la prise de décision, le frein à la réflexion, la discrimination et le renforcement de la fracture technologique.

L'IA représente de tels enjeux et génère tant de transformations que sa gouvernance mérite d'être élaborée, alors que des interrogations demeurent quant à la forme de cette gouvernance. Le droit actuel est-il suffisant et faut-il développer des règles juridiques ou éthiques ?

### Le droit actuel peut-il s'appliquer à l'IA ?

L'intelligence artificielle a des incidences profondes et généralisées qui transforment les modes de travail. Comment en assurer un développement maîtrisé sans freiner l'innovation ? Les règles juridiques actuelles peuvent-elles s'y appliquer ? Il existe déjà des normes utiles pour réguler l'IA comme la gouvernance responsable des entreprises et la gestion de la cybersécurité. Cependant, des pans entiers du droit classique sont remis en question par l'IA, parmi lesquels la responsabilité, la propriété intellectuelle et la protection de la vie privée.

Les instruments classiques de la respon-

sabilité semblent pouvoir être exploités. Les parties impliquées peuvent aménager les contours de leur responsabilité par un contrat. Cependant, ces conditions contractuelles ne sont pas opposables, en droit français, ni aux consommateurs ni à un tiers qui subirait un dommage. Si un robot piloté par une IA génère un préjudice, qui sera responsable ? La question de la détermination de la responsabilité sera complexe, comme l'est celle de la chaîne de responsabilité. Du concepteur du système jusqu'à son utilisateur, sans oublier ceux qui vont maintenir et entraîner ce système apprenant, qui seront les acteurs responsables ?

(2) Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur (Dictionnaire Larousse).

L'IA remet aussi en question les principes de la propriété intellectuelle. La protection des composants de l'IA (logiciels, données et algorithmes<sup>2</sup>) est cruciale pour permettre la protection des investissements. Les logiciels sont protégés par le droit d'auteur, à

condition de comporter une part d'originalité. Les données peuvent bénéficier de la protection sui generis des bases de données, à condition de prouver un investissement substantiel du producteur et d'être conformes au droit des données personnelles. Si les algorithmes ne sont pas protégeables en tant que tels, leur mise en forme pourrait être protégée par le

droit d'auteur quand ils sont intégrés à un logiciel. Il faut préciser que les méthodes mathématiques ne sont pas protégeables,

(3) Article L611-10 du Code de la propriété intellectuelle.

(4) Rapport « Donner un sens à l'intelligence artificielle », sous la direction de Cédric Villani, 8 mars 2018.

ni par le brevet ni par le droit d'auteur<sup>3</sup>. La mise en œuvre de ces protections peut se complexifier quand le système d'IA génère lui-même de nouvelles données. A qui appartient l'ensemble

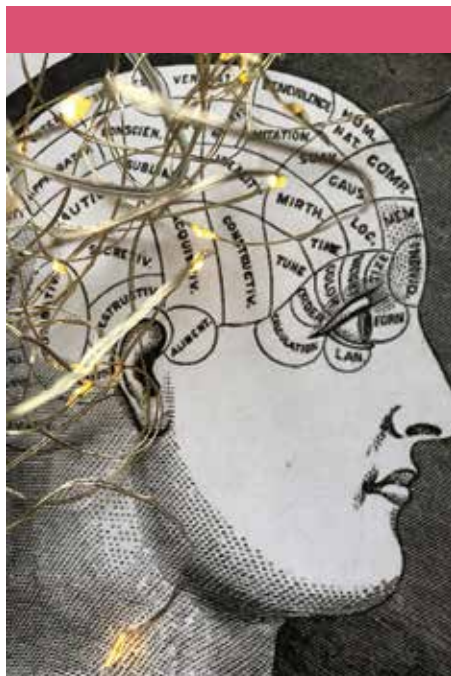
de données générées par une intelligence artificielle ? Et si le système d'IA génère une création artistique, qui est titulaire de cette création ? Ici, l'IA défie les notions juridiques traditionnelles d'originalité et d'auteur. « *Beaucoup de ces enjeux soulevés par les algorithmes constituent aujourd'hui un angle mort du droit* » selon le rapport Villani<sup>4</sup>.

(5) Loi du 30 juillet 2018 sur le secret des affaires.

(6) Loi pour une République numérique du 7 octobre 2016 et décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique.

Pour protéger ces résultats, la protection par la loi sur le secret des affaires<sup>5</sup> peut être une solution mais les exigences de transparence prévues par la protection des données personnelles peuvent se heurter à ce mécanisme. De plus, la loi pour une République numérique<sup>6</sup>

prévoit que les codes sources des algorithmes utilisés par l'administration soient des documents communicables. Entre protection de l'innovation



© Marcelin

L'IA s'inscrit naturellement dans une sphère éthique du fait de la protection des données, du régime de la responsabilité et de son impact algorithmique discriminatoire. La perception variable de son périmètre juridique et la disparité des approches tant scientifiques que politiques rendent nécessaire mais délicate l'émission d'une norme internationale.

et transparence des algorithmes, l'équilibre est à construire.

Les règles de protection des données personnelles sont également mises à l'épreuve face au développement de l'IA. Le RGPD et la « Loi Informatique et Libertés modifiée » encadrent l'usage des données personnelles et interdisent la prise de

décision par la seule machine. La loi pour une République numérique s'inscrit dans la même logique que le RGPD, dès lors qu'elle renforce l'obligation faite à ceux qui déploient des algorithmes d'en informer les personnes concernées. En effet, face aux biais pouvant entraîner une discrimination, comment exploiter l'IA tout en maintenant l'impératif de protéger les libertés individuelles, permettre un droit d'accès dans un système dont la complexité peut échapper à la compréhension humaine et enfin appliquer le principe de transparence quand les systèmes sont complexes et évolutifs ?

La question se pose de l'obligation de normer par anticipation ou de prendre le temps d'observer si la mise en œuvre opérationnelle de l'IA nécessite une évolution des régimes actuels du droit ?

### **La gouvernance de l'IA doit-elle se structurer autour de règles juridiques ou éthiques ?**

La confrontation des nouveaux usages de l'IA aux règles juridiques classiques a ouvert un large débat et encouragé les réflexions de différents organismes autour de la normalisation de l'IA. Jamais un thème n'a autant suscité d'études et de discussions. Il est vrai que le caractère disruptif de l'IA suscite de nombreux questionnements. Les systèmes cognitifs, demain basés sur des neurones artificiels, modifient la façon dont les organisations innovent et fonctionnent.

Comment encadrer ce courant d'innovation sans le brider ? Le débat sur la prééminence de l'éthique ou du droit pour encadrer l'IA est ouvert.

Rappelons que l'éthique est la science des principes moraux qui interviennent dans l'action humaine. A la différence du droit, l'éthique n'impose pas de sanctions. La norme éthique, sans caractère obligatoire, est néanmoins une préfiguration de la norme juridique. La réflexion philosophique et morale peut inspirer l'élaboration de normes à caractère obligatoire. De plus, le caractère éthique influe sur l'attrait des consommateurs pour un produit ou service.

Quant au droit, c'est l'ensemble des dispositions qui, à un moment et dans un État déterminés, règle le statut des personnes et des biens, ainsi que les rapports que les personnes publiques ou privées entretiennent. Le droit, de par son caractère contraignant, pourrait-il freiner les travaux de recherche en IA ? Sachant que les régimes juridiques varient entre les États et régions du monde, il est possible de penser que l'encadrement juridique pourrait influencer sur le développement de l'IA dans un État plutôt qu'un autre. Comme l'IA est une activité par nature internationale et concurrentielle, une normalisation juridique mondiale semble utopique au regard des disparités des régimes légaux régionaux. L'IA fait l'objet d'enseignements et de recherches

dans de nombreux pays, et les technologies qui en sont à la base y sont similaires. Les algorithmes représentent un langage universel et les États veulent conserver l'équilibre entre innovation et gouvernance.

Cette préconisation de se garder d'une contrainte juridique trop forte sur la recherche en IA, est présente dans différentes études. Par exemple, dans son document de réflexion relatif à l'IA dans

(7) ACPR, « Intelligence artificielle : enjeux pour le secteur financier », Document de réflexion, décembre 2018.

(8) L'ACPR (Autorité de Contrôle Prudentiel et de Résolution) est chargée de la supervision des secteurs bancaires et d'assurance. Elle veille à la préservation de la stabilité du système financier et à la protection des clients.

le secteur financier<sup>7</sup>, l'ACPR<sup>8</sup> indiquait, en 2018 : « *Il peut y avoir un risque à édicter trop tôt des normes qui fassent obstacle au développement de certains usages de l'IA dans le secteur financier. Inversement, il apparaît toutefois important que le développement de l'usage de l'IA s'accompagne d'une réflexion pratique*

*sur les formes adaptées de leur gouvernance, au regard d'objectifs réglementaires technologiquement neutres.* »

Par ailleurs, le temps du législateur n'est pas celui du chercheur en IA. Les normes envisagées doivent assez souples pour s'adapter à une technologie en rapide mutation.

Pour accompagner l'IA en plein développement, faut-il légiférer ou promouvoir

l'éthique ? Cette question est au centre des réflexions de nombreuses institutions publiques en France, au plan européen et international. Quelles sont les réflexions majeures ?

### Les travaux français

Dès 2014, le Conseil d'État consacre son étude annuelle au numérique et aux droits fondamentaux. L'étude invite notamment à « repenser les principes fondant la protection des droits fondamentaux ».

Le Sénat publie, le 29 mars 2017, un rapport intitulé « *Pour une intelligence artificielle maîtrisée, utile et démystifiée* ». Les principes majeurs énoncés sont de favoriser des algorithmes et des robots sûrs, transparents et justes.

Fruit d'un débat public animé par la CNIL, en décembre 2017, une publication explore les promesses et les risques associés à ces technologies. Les recommandations de la CNIL sont de rendre les systèmes compréhensibles en renforçant le droit existant, de promouvoir le design des algorithmes au service de la liberté humaine, de construire une plate-forme nationale d'audit et d'encourager le développement de l'éthique.

Le 28 mars 2018, le Parlement propose un autre rapport : « Une stratégie pour la France en matière d'IA ». Selon Cédric Villani, son rapporteur : « *La France doit réaffirmer sa souveraineté et définir un cadre*



*de confiance pour l'utilisation de l'IA au bénéfice de ses citoyens, en tenant compte du cadre européen.* » Le rapport formule diverses recommandations notamment celles de penser des droits collectifs sur les données et de promouvoir une gouvernance spécifique de l'éthique en IA.

Pour le secteur de la banque et de l'assurance, l'ACPR publie en juin 2020 un document de réflexion :

« Gouvernance des algorithmes d'intelligence artificielle dans le secteur financier ». Sa rédaction, soumise au débat public, encourage à s'assurer de la fiabilité des algorithmes et à définir une gouvernance appropriée.

### Les réflexions européennes

Le Conseil européen propose, le 3 décembre 2018, une Charte éthique sur l'utilisation de l'IA dans les systèmes judiciaires.

Une résolution du Parlement européen sur une Politique industrielle quant à l'IA et la robotique est rendue publique le 12 février 2019. Le Parlement veut promouvoir un environnement réglementaire favorable au développement de l'IA et envisager avec précaution toute loi ou réglementation globale de l'IA.

Le 8 avril 2019, c'est la Commission européenne, au travers de son groupe d'experts en intelligence artificielle

(AI HLEG) qui partage ses lignes directrices sur l'éthique de l'IA. La Commission encourage notamment le contrôle humain, la sécurité et la robustesse, le respect de la vie privée, la transparence, la non-discrimination et l'équité ainsi que la responsabilisation.

(9) High-Level Expert Group on Artificial Intelligence (CAHAI).

Le Conseil de l'Europe a décidé de la création d'un Comité IA ad hoc<sup>9</sup> pour examiner l'opportuni-

té de développer des règles propres à l'IA, au sein de ses 47 États membres.

L'objectif de ce comité est d'« *examiner la faisabilité et les éléments potentiels, sur la base de larges consultations multipartites, d'un cadre juridique pour le développement, la conception et l'application de l'intelligence artificielle* ».

### Les initiatives internationales

Comme chaque rupture technologique, l'IA aura des implications majeures sur le plan

international. Elle constitue déjà une zone de compétition<sup>10</sup>, tout particulièrement entre les États-Unis et la Chine. Et l'Europe reste dans la course.

(10) Julien Nocetti, « Intelligence artificielle et politique internationale : les impacts d'une rupture technologique », Études de l'Ifrri, Ifri, novembre 2019.

(11) Recommandation du Conseil sur l'intelligence artificielle. <https://unesco.delegfrance.org./Intelligence-Artificielle-des-initiatives-et-normes-international-3405>

L'OCDE a publié, en juin 2019, une Recommandation du Conseil sur l'intelligence artificielle<sup>11</sup>, à l'occasion du sommet d'Osaka. Il s'agit de la



première norme intergouvernementale sur l'IA.

Son objectif est de stimuler l'innovation et de renforcer la confiance dans l'IA en promouvant une approche responsable. La Recommandation indique que : « *si elle présente des avantages, l'IA ne va pas sans poser aux sociétés et aux économies un certain nombre de défis, notamment en termes de mutations économiques et d'inégalités, de concurrence, de transitions sur les marchés du travail et de conséquences sur la démocratie et les droits de l'homme.* »

Le texte de cette recommandation énonce cinq principes majeurs : une croissance inclusive, des valeurs centrées sur l'humain, l'explicabilité, la robustesse et la responsabilité. Ces principes s'accompagnent de recommandations pour une IA digne de confiance, à savoir :

- investir dans la recherche et le développement en matière d'IA,
- favoriser l'instauration d'un écosystème numérique pour l'IA,
- façonner un cadre d'action favorable à l'IA,
- renforcer les capacités humaines et préparer la transformation du monde du travail,

- et favoriser la coopération internationale au service d'une IA digne de confiance.

L'OCDE publiera ensuite en juillet 2020, un rapport « Examples of AI National

(12) Examples of AI National Policies, Report for the G20 Digital Economy Task Force, July 2020.

Policies »<sup>12</sup> qui présente l'état des travaux dans une vingtaine de pays, dont la France. La plupart des politiques nationales

sont récentes, avec pour volonté de construire un écosystème d'AI de confiance et centré sur l'humain. Certaines questions reviennent régulièrement sur les thèmes d'accès aux données et d'écosystème de l'IA. L'OCDE relève que peu de politiques semblent mettre l'accent sur les principes de robustesse, de sécurité et de responsabilité. L'OCDE encourage l'innovation en IA tout en exigeant des garanties de protection des droits humains, par des dispositifs éthiques ou réglementaires.

(13) Organisation des Nations Unies pour l'éducation, la science et la culture.

De par sa dimension internationale, l'UNESCO<sup>13</sup> affiche également

son ambition de définir les principes éthiques fondamentaux qui encadreront les développements de l'IA. Dans le cadre d'une conférence, « Principes pour l'IA : vers une approche humaniste ? » organisée à Paris le 4 mars 2019, Audrey Azoulay, directrice générale de l'institution, prend position : « *Il est certainement prématuré de vouloir réglementer l'IA au niveau mondial, mais il est plus que*

*temps de définir un socle de principes éthiques qui encadreraient cette disruption* ». L'Unesco annonce être prête à élaborer des règles éthiques sur l'IA et deux réunions intergouvernementales sont prévues en 2021 pour finaliser le texte de cet instrument normatif.

Aujourd'hui, la gouvernance de l'IA est à un stade expérimental mais actif dans de nombreux pays. Au cœur des discussions politiques internationales, cette gouvernance se construit essentiellement autour de dispositifs éthiques.

## **AUTEURE**

**Sabine Marcellin est avocat associé au sein du cabinet DLGA, en charge du droit de la cybersécurité et du numérique.**

**Elle est lieutenant-colonel (RC) dans la Réserve de Cyberdéfense de la Gendarmerie et chargée de cours à HEC.**

## DIRECTEUR DE LA PUBLICATION

Général de brigade **Laurent BITOUZET**

## RÉDACTION

Directeur de la rédaction :

Général d'armée (2S) **Marc WATIN-AUGOUARD**,  
directeur du centre de recherche de l'EOGN

## RÉDACTEUR EN CHEF

Colonel (ER) **Philippe DURAND**

## MAQUETTISTE PAO

Maréchal des logis-chef **Anne PELLETIER**  
SDG

## COMITÉ DE RÉDACTION

- Général de corps d'armée **Bruno JOCKERS**,  
major général de la Gendarmerie nationale
- Général de corps d'armée **Thibault MORTEROL**,  
Commandant des écoles de la Gendarmerie nationale
  - Général de brigade **Laurent BITOUZET**,  
Conseiller communication du directeur général  
de la Gendarmerie nationale - chef du Sirpa-gendarmerie

## COMITÉ DE LECTURE

- Général de corps d'armée **Alain PIDOUX**,  
Inspecteur général des armées – gendarmerie
- Général de corps d'armée **Bruno JOCKERS**,  
Major général de la Gendarmerie nationale
- Général de corps d'armée **Thibault MORTEROL**,  
Commandant des écoles de la Gendarmerie nationale
- Général de corps d'armée **François GIERÉ**,  
Directeur des opérations et de l'emploi
- Général de brigade **Laurent BITOUZET**,  
Conseiller communication du directeur général  
de la Gendarmerie nationale - chef du Sirpa-gendarmerie
  - Colonel **Laurent VIDAL**,  
délégué au patrimoine – DGGN
- Lieutenant-colonel **Édouard EBEL**,  
département gendarmerie au sein  
du service historique de la Défense

## DÉPOT LÉGAL

Raison sociale de l'éditeur :

CREOGN, avenue du 13<sup>e</sup> Dragons,  
77010 Melun cedex

Général (2S) Watin-Augouard

**Imprimerie :** SDG - 11 rue Paul Claudel  
87000 Limoges  
Janvier 2021

101001111010110000001100101111  
010 NOUVELLE SESSION NATIONALE 101  
111101001010111110100111101000  
110000000011010000100111000100  
100111101110101001001000101010  
01000010001101011001011110010  
100011111010011011100100000000  
000100010101000010011010101010  
**MAJEURE**01000101001001111110  
**SOUVERAINETE NUMERIQUE**  
**& CYBERSECURITE**1011010001  
100101011000110011011101101000  
101001111010110000001100101111  
01000000010011111010001011101  
111101001010111110100111101000  
110000000011010000100111000100  
100111101110101001001000101010  
01000010001101011001011110010  
100011110010011011100100000000  
001010010101011101100000100110

Période de formation **septembre 2021 à juin 2022**

**NOUS CONTACTER**

Pour toutes questions relatives au contenu de la majeure  
[sncyber@ihedn.fr](mailto:sncyber@ihedn.fr)

Pour toutes questions relatives au processus de recrutement  
01 44 42 47 06 – [recrutement.auditeurs@ihedn.fr](mailto:recrutement.auditeurs@ihedn.fr) – [www.ihedn.fr](http://www.ihedn.fr)