Published in Criminalité économique et cybercriminalité: mélanges en l'honneur de la professeure Isabelle Augsburger-Bucheli, Helbing Lichtenhahn, 2021, pp. 217-229, which should be cited to refer to this work.

Cybersécurité, et si nous faisions fausse route

Sébastien Jaquier*

* Doyen de l'ILCE (Institut de lutte contre la criminalité économique de la Haute école de gestion Arc, HES-SO // Haute école de Suisse Occidentale, Switzerland).

Bibliographie spéciale

Alexandre Laurent, La guerre des intelligences, Editions JC Lattès, Paris 2017 ; Confédération suisse, Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, avril 2018 (Confédération suisse SN002) ; Lancry Alain, L'ergonomie, Paris 2016 ; Mainardi Michele/Zgraggen Lara/Nussio Michela/Zanetti Alessandro, Minori in internet. Studio longitudinale dell'evoluzione dei comportamenti dei minori in internet e al computer. Project Report Ed. SUPSI/DFA-DSAS, Manno/Locarno 2012 ; Mascheroni Giovanna/Ólafsson Kjartan, Net Children Go Mobile – Risks and Opportunities, 2e éd., Italy: Educatt, Milan 2014 ; Office fédéral de la justice (OFJ), Renforcement de la protection des données, ‹www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html› (19.10.2020) ; Park Seungmin/Kang Minchul/Kim Eunha, Social relationship on problematic Internet use (PIU) among adolescents in South Korea – A moderated mediation model of self-esteem and self-control, Computers in Human Behavior 2014, vol. 38, 349-357 ; PISA 2018, Les élèves de Suisse en comparaison internationale, ‹https://pisa.educa.ch/sites/default/files/uploads/2019/12/pisa2018_fr.pdf› (19.10.2020) ; Rousseau Jean-Jacques, Essai sur l'origine des langues, *in* Fac-similé du manuscrit de Neuchâtel, 1781 ; Union internationale des télécommunications, SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ Sécurité du cyberespace – Cybersécurité – Présentation générale de la cybersécurité, UIT-T, secteur de la normalisation des télécommunications de l'UIT, X.1205 (04/2008) (Union internationale des télécommunications 2008).

Cyber-[1] : (du grec kubernân, gouverner), préfixe servant à former de très nombreux mots relatifs à l'utilisation du réseau Internet.

Cybersécurité[2] : ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants :

– Disponibilité
– Intégrité, qui peut englober l'authenticité et la non-répudiation
– Confidentialité.

Sécurité de l'information[3] : protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. En outre, d'autres propriétés, telles que

1 Larousse.
2 Union internationale des télécommunications 2008.
3 ISO/IEC 27000:2018.

l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.

Les définitions ont ceci d'utile, qu'elles posent un cadre, en l'occurrence, en soulignant la parenté entre les termes de sécurité de l'information et de cybersécurité. Le préfixe cyber- qualifie une multitude de mots relatifs à l'utilisation d'Internet, et ce terme est lui-même une abréviation qualifiant un réseau télématique international ayant pour vocation un échange de données moyennant l'utilisation d'un protocole commun. Rappelons que, selon Larousse, la donnée est la représentation conventionnelle d'une information en vue de son traitement informatique. La boucle est donc bouclée.

A l'heure de la digitalisation, au moment de se préoccuper de sécurisation de l'information, il est bon de revenir à certains fondamentaux qui permettront au lecteur de garder le cap, et surtout les pieds bien ancrés dans le monde réel. La digitalisation n'est autre qu'un synonyme de numérisation. La numérisation est à peu près aussi ancienne que l'informatique. Les débuts d'Internet, dans les années 80 laissaient présager des développements en matière de traitement de l'information. La naissance du web, à l'aube des années 90, a permis d'envisager de nouvelles perspectives en matière d'échange d'informations en ligne.

L'avènement de la société de l'information s'est concrétisé par de nouveaux développements en matière de stockage, traitement et transfert de l'information. Le monde des services était destiné à en bénéficier au premier chef, en quête d'efficacité, de performance et d'ergonomie.

Qui aurait alors pu dire que l'influence du développement des *bits and bytes* ne se limiterait pas à la dimension de l'information, mais investirait le monde réel, s'immisçant graduellement dans chaque objet, envahissant successivement les secteurs secondaire et même primaire, s'invitant dans toutes les sphères d'activités, notamment privées et associatives.

Soudainement, tout s'accélère. La société n'a pas encore intégré les développements liés à l'Internet des objets que l'intelligence artificielle émerge, de manière tonitruante et néanmoins désordonnée, laissant pourtant présager une concurrence réelle avec le cerveau humain. Il n'est désormais plus complètement farfelu d'envisager que l'intelligence des machines puisse égaler, voire dépasser l'intelligence humaine dans certains domaines, ce qui présage une transformation du rapport de l'Humain à son activité, en commençant par la remise en question d'un système éducatif qui n'aurait pas pris toute la mesure de cette révolution en marche[4]. L'estimation de la courbe d'apprentissage des machines prend désormais l'apparence d'une prédiction.

4 Alexandre.

I. Changement de paradigme pour l'ensemble des acteurs de la société

Ainsi, l'impact des développements du numérique a non seulement dépassé les systèmes d'information ; l'onde de choc touche le mode réel dans tous les secteurs d'activité. Ses effets ne se limitent désormais plus uniquement aux données stockées, traitées ou transférées, ils impactent notre quotidien de manière tangible :

- Dans le secteur public, citons les systèmes de mesure (débits d'eau, d'énergie, etc.), les systèmes d'alarme et de détection d'événements ou encore la gestion des réseaux (énergie, transports, communications, etc.) ;
- Dans le secteur industriel, avec notamment le suivi logistique, l'identification de chaque pièce d'une production et en corollaire le suivi de chaque objet produit avant, voir après sa vente ou sa distribution, tout au long de son cycle de vie ;
- Dans l'agriculture, avec la gestion des véhicules, de certaines activités (p. ex. culture avec pilotage par satellite), le suivi des bestiaux, la surveillance des terrains ;
- Dans le ménage privé et sur chaque individu, la gestion des accès, la gestion de l'énergie, les assistants personnels, les *Wearables*, les moyens de transport individuels, etc.

La liste n'est pas exhaustive, et pour cause ; l'émergence des outils technologiques permettant ce genre de développement, notamment les réseaux de communication, provoque ou du moins soutient un foisonnement d'idées propice à une innovation tous azimuts, même s'il faut admettre que les modèles économiques des objets ainsi développés sont parfois insuffisamment éprouvés, les reléguant ainsi parfois au rôle de feux de paille, parfois à celui d'accélérateur d'innovation.

L'informatique centralisée, matérialisée par de gros serveurs avec lesquels nos systèmes d'information communiquaient, fait partie de l'histoire. L'informatique dans le cloud est en quelque sorte une évolution de ce modèle initial, avec des serveurs permettant un accès facilité, un traitement et un stockage important de l'information. Désormais, l'informatique des objets intègre l'ambition d'échanges de pair à pair et de clouds distribués. Le stockage de l'information lui-même se dématérialise, plus précisément, il se distribue de se multiplie à l'envi si bien qu'il devient complexe de localiser physiquement la donnée[5].

5 A titre d'illustration, la société Storj.io fondée en 2003 déjà ambitionne de fournir la plus grande plateforme de stockage de données décentralisée dans le cloud, de manière participative en utilisant la blockchain.

II. Quelques idées préconçues à l'ère du tout numérique

Tous ou presque l'admettent ; l'informatique fait partie intégrante de l'activité humaine, pour le bien commun. Il est plaisant d'envisager que la maîtrise de cette technologie soit l'affaire des techniciens, autrement dit, c'est par l'informatique que l'on résout les défis et les problèmes qui sont liés à son exploitation, notamment en ce qui concerne la sécurité de l'information. Cette idée suppose que l'informatique est une science que nous ne maîtrisons pas encore pleinement, mais dont nous perfectionnons continuellement la pratique. Il y aurait donc un idéal de maîtrise technologique à atteindre. S'agissant d'une science se caractérisant par la production ininterrompue de nouveaux outils, révolutionnant parfois son propre écosystème, confirmant puis infirmant les conjectures de Moore[6] au fil des sauts technologiques, cette idée semble ne pas relater complètement la réalité. Il est vrai qu'à lire la définition du terme informatique[7] la prépondérance du traitement automatique de l'information est évidente. Cependant, le traitement n'a de sens que s'il supporte des échanges d'informations. L'individu est ainsi à la fois initiateur et destinataire des processus informatiques. Or comme le relève Alain Lancry[8] dans l'équation Homme – Tâche – Machine – Situation, la composante humaine est fréquemment assimilée à la variable d'ajustement. Cet élément contribue sans doute à expliquer pourquoi, en informatique, le désormais célèbre facteur humain est à l'origine de tous les maux informatiques et réceptacle de toutes les critiques. Le facteur humain semble bien être le talon d'Achille de la chose informatique.

Quant aux cybercriminels, que faire contre des individus, des organisations, désormais des groupements criminels qui semblent toujours avoir une longueur d'avance ? L'honnête citoyen est condamné à subir leurs assauts. Pour rester sauf, il se fie à la technologie tel un nageur dépassé par la virulence des vagues qui s'accroche à une bouée, car c'est bien de l'informatique elle-même que doit venir la solution à ses maux. Ne le nions pas, ce raccourci simpliste est de nature à satisfaire l'industrie informatique, les concepteurs de matériels et logiciels, nombre de consultants en la matière et même les utilisateurs finaux. Il sert d'accélérateur de ventes pour les uns et de bonne conscience pour les autres.

6 Gordon E. Moore ; docteur en chimie et en physique, co-fondateur de INTEL en 1968, qui mentionnait que la complexité des microprocesseurs doublait tous les deux ans. Plus tard il mit cette évolution en perspective avec la réduction tout aussi importante du coût de production desdits composants.

7 Larousse.

8 Lancry.

III. L'heure n'est pas au fatalisme

Du point de vue de l'utilisateur, cette relative indolence est surprenante, dans une société pourtant tournée vers l'action. Serait-ce parce que, comme le prétendait Rousseau[9], l'homme est naturellement paresseux ? Nous émettons ici l'hypothèse que c'est plutôt le résultat de l'action démagogique, volontaire ou non, de l'industrie informatique qui n'a de cesse de vanter l'incroyable complexité des outils inimaginablement simples à utiliser qu'elle met à la portée de tous. Le fossé entre l'utilisation de l'instrument et la compréhension de ses mécanismes devient abyssal.

Comment considérer la question de la sécurité de l'information dans ce contexte ? Elle fait indéniablement partie de ces thématiques nébuleuses, de ces sujets rébarbatifs auxquels seuls des informaticiens semblent pouvoir s'atteler. Pourtant, l'industrie elle-même peine à embrasser cette problématique, qui, entre course à l'innovation et recherche du rendement (si possible) immédiat, n'a décidément pas encore trouvé son créneau. Ainsi, les révélations de failles informatiques, fuites de données et autres problèmes visant nos compagnons numériques, ou plutôt les informations qu'ils traitent, sont désormais légions. Le *security by design* et ainsi que le *privacy by default* sont de nos jours encore des slogans qui ne relatent que partiellement l'expérience vécue par l'industrie. Tout est probablement question de priorités. Pour survivre ou pour croître, l'industrie doit innover ou proposer une offre concurrentielle attractive. Le premier chemin pousse l'industrie à accélérer son processus de conception et de création afin de réduire le « *time to market* » et ainsi poursuivre sa course face à la concurrence. La seconde voie l'incite à réduire les coûts pour produire moins cher. La finalité n'est pas l'usage de la chose réalisée, mais bien le succès de l'entreprise qui la produit.

Dans l'industrie, les méthodes, outils, cadres de référence méthodologiques soutenant le processus de création dans l'entreprise ont évolué. Ils tendent désormais à généraliser une pratique qui était le propre du secteur du développement logiciel à l'ensemble des activités de l'entreprise, signe, s'il en fallait encore, de la pénétration de l'informatique dans tous les secteurs d'activité économique. C'est notamment le cas avec la méthode Agile[10]. Ce faisant, l'industrie promeut un cadre de référence méthodologique en matière de gestion de projets qui favorise l'émergence de produits pour lesquels l'idée entre le point de départ et le rendu final est susceptible d'avoir sensiblement évolué. Au fil des itérations, le produit est optimisé en accord avec les principes de la méthodologie Agile, dont le premier est la satisfaction client. Cependant, le manque

9 Rousseau.

10 Voir notamment « Manifesto for Agile Software Development », ‹https://agilemanifesto.org› (19.10.2020).

parfois criant d'inclusion du secteur de la sécurité de l'information dans le processus de création, ou plutôt le manque d'expérience dans son implication conduit à des résultats certes ergonomiques, mais peu sécurisés, ou sécurisables. Ce n'est pas ce type de méthodologie qui est remis en cause d'un point de vue sécuritaire, mais plutôt la prise en compte de cette composante dans sa mise en œuvre. On peut ainsi se demander si l'excellence technologique visée est compatible avec l'excellence en matière de sécurité de l'information.

De même, il y a lieu de se demander si cette question pourra réellement être résolue tant que les aspects liés à la sécurité de l'information et à la protection des données personnelles ne feront pas partie intégrante de la proposition de valeur.

Ce constat va d'ailleurs de pair avec celui qui fait du facteur humain le talon d'Achille de la sécurité de l'information. En effet, il semble qu'au niveau de la conception même des produits informatiques, on veuille gommer l'impact de l'humain, au lieu de l'intégrer dans la réflexion liée à l'ergonomie du produit. L'apparition de la serrure à l'âge du bronze répondait à un besoin, celui de pouvoir sécuriser en un lieu des biens ou personnes. La serrure s'accompagnait d'une clé manipulable par l'individu qui comprenait son principe de fonctionnement et pouvait choisir ce qu'il souhaitait sécuriser et dans quelles conditions il voulait le faire. Si l'on se hasarde à une analogie avec l'informatique actuelle, le verrou existe toujours, mais la serrure et la clef ne sont plus à portée de l'utilisateur moyen. Leur fonctionnement est réglé par le système auquel l'utilisateur fait confiance par défaut (pour s'en convaincre, il suffit d'observer les paramètres de configuration proposés par les fournisseurs de logiciels). A défaut, c'est le spécialiste informatique qui maîtrise ces composants. La situation est somme toute confortable puisqu'elle permet à l'utilisateur final de ne plus se préoccuper de cette question qui, par ailleurs, ne fait en général pas partie de son cahier des tâches.

De fait, l'utilisateur se complait dans cette « dynamique » et tend à perpétuer d'anciens réflexes développés l'apparition de l'informatique destinée au grand public. La confiance accordée aux ordinateurs, smartphones routeurs, pare-feu et autres composants informatiques en matière de sécurité est proportionnelle à l'ignorance de leurs principes de fonctionnement. Ce qui, dans tout autre domaine semblerait une aberration est ici un fait accompli. Cette ignorance est le fruit d'une stratégie industrielle qui a voulu rendre accessible au plus grand nombre et sans apprentissage particulier l'utilisation de systèmes d'information dont les traitements ne cessent de se complexifier. Force est d'ailleurs de constater que, même de nos jours, acheter de la sécurité de l'informatique ne fait pas rêver l'utilisateur lambda. La notion de responsabilité n'a ici pas sa place.

Quant aux cybercriminels, on ne cesse de s'étonner du fait qu'ils aient une longueur d'avance dans leur domaine de compétences. Rappelons ici que la

cybercriminalité c'est avant tout de la criminalité ! Les individus ainsi que les organisations qui en font leur fonds de commerce se comportent à l'image de l'industrie, en recherchant en permanence l'innovation afin d'atteindre leurs buts, ce qui est en somme une attitude pragmatique. En revanche, il est surprenant que l'on n'intègre pas ce facteur de manière plus active et didactique dans le raisonnement lié à la sécurité de l'information. Pourtant, l'avance des criminels, mise en exergue précédemment est de nature à contredire la prépondérance du facteur technologique en tant que solution face à la cybercriminalité, puisqu'elle est constamment prise de court. Notre propos n'est pas de nier l'importance de cette composante dans la lutte contre la criminalité informatique, mais plutôt de mettre en exergue le fait qu'elle doit faire partie d'un arsenal et qu'à ce titre elle est, à elle seule, insuffisante.

IV. Les leviers

Pour constituer un arsenal digne de ce nom, il est donc nécessaire d'inclure d'autres composants qui agiront comme autant de leviers susceptibles de contribuer à réduire la fracture entre des utilisateurs infantilisés, une industrie qui a longtemps été infantilisante afin de déjouer les actions des criminels, qui n'ont jamais cessé d'exploiter toutes les opportunités pour arriver à leurs fins.

V. La loi

On a coutume de dire que les législations ont constamment un temps de retard face à la criminalité en matière informatique. Il s'agit cependant ici d'un propos simpliste. Les mécanismes juridiques nationaux et internationaux existent et tissent une toile dont le maillage est certes perfectible, mais qui a d'ores et déjà le mérite de poser les fondamentaux et de tracer des lignes claires en matière de compréhension et d'appréhension des phénomènes.

Au niveau helvétique, la législation ne peut pas être considérée comme lacunaire. Elle s'applique d'abord à bien définir la criminalité liée à l'informatique en distinguant d'une part les infractions dont l'objet est un système d'information, infractions informatiques au sens strict[11] des infractions dites ordinaires commises au moyen d'un ordinateur[12]. Cette distinction permet de souligner le fait que la criminalité liée à l'informatique est en grande partie de la criminalité ordinaire, le numérique est bien souvent un outil ou un

11 Notamment CPS art. 143, soustraction de données ; 143bis, Accès indu à un système informatique ; 144bis, Détérioration de données ; 147, Utilisation frauduleuse d'un ordinateur.

12 Notamment CPS art. 135, Représentation de la violence ; 146, escroquerie ; 148, Abus de cartes-chèques et de cartes de crédit ; 150, Obtention frauduleuse d'une prestation ; 179^{septies}, Utilisation abusive d'une installation de télécommunications ; 179^{novies}, Soustraction de données personnelles.

moyen permettant aux criminels d'arriver à leurs fins. Cet arsenal juridique, qui permet une qualification au plan pénal des infractions liées à l'informatique est complété par des législations spécifiques. Citons principalement la loi sur la concurrence déloyale, donc l'objet principal n'est certes pas l'informatique, mais qui la prend en considération, en particulier pour ce qui est des pratiques déloyales notamment l'envoi de courriels en masse. Enfin, la loi sur la protection des données (LPD) devient un élément charnière dans l'arsenal juridique, puisqu'elle détermine l'utilisation non pas des outils, mais des informations qu'ils traitent. Cette dernière législation est soumise à une certaine pression depuis quelques années, avec le développement de nouvelles règlementations au niveau international, en particulier la règlementation générale sur la protection des données (RGPD) émise par l'Union européenne. La révision en cours vise notamment à la rendre compatible avec la directive européenne relative à la protection des données dans le cadre de poursuites pénales[13]. Relevons que le projet de LPD révisée a été adopté par le Conseil National et le Conseil des Etats le 25 septembre 2020[14], soit plus de trois ans après le projet[15] proposé par le Conseil fédéral, laissant augurer une entrée en vigueur à l'horizon 2022.

Au plan international la convention sur la cybercriminalité[16] émise par le Conseil de l'Europe et les Etats signataires, dont la Suisse depuis 2012, vise à renforcer la collaboration internationale en matière de lutte contre la cybercriminalité. Cette convention qui date de 2001 a son importance dans l'arsenal juridique national. Chacun sait en effet que les phénomènes cybercriminels ont fréquemment une dimension internationale. Le fait que cette convention soit actuellement ratifiée par 65 Etats auxquels s'ajoutent trois Etats signataires n'ayant pas pour l'instant ratifié le texte ainsi que huit états ayant été invités à ratifier le texte[17] lui donne un certain poids et fournit à la poursuite pénale une base sans doute appréciable en matière de collaboration internationale.

L'arsenal législatif est certes perfectible, la jurisprudence en tant que source du droit est une illustration de l'évolution du droit. Il faut cependant veiller à ne pas codifier de manière trop contraignante le champ de l'utilisation des systèmes d'information afin de ne pas nuire à l'innovation et potentiellement à la position concurrentielle de notre économie dans le monde.

13 Office fédéral de la justice (OFJ).

14 ‹www.parlament.ch/centers/eparl/curia/2017/20170059/Texte%20pour%20le%20vote%20final%203%20NS%20F.pdf› (19.10.2020).

15 ‹www.admin.ch/opc/fr/federal-gazette/2017/6565.pdf› (19.10.2020).

16 ‹www.admin.ch/opc/fr/official-compilation/2011/6297.pdf› (19.10.2020).

17 Convention sur la cybercriminalité, Etat des signatures et ratifications du traité 185, ‹www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Rw8znr7H› (19.10.2020).

VI. La culture

Selon la définition de l'UNESCO, « La culture, dans son sens le plus large, est considérée comme l'ensemble des traits distinctifs, spirituels et matériels, intellectuels et affectifs, qui caractérisent une société ou un groupe social. Elle englobe, outre les arts et les lettres, les modes de vie, les droits fondamentaux de l'être humain, les systèmes de valeurs, les traditions et les croyances. »[18].

L'histoire de l'informatique et de son rôle dans la société s'écrit pour l'instant sur quelques décennies. Le rythme de l'innovation technologique lié à l'informatique semble ne pas être appelé à ralentir. Dans ce contexte on peut à juste titre se demander si notre société a déjà pris la mesure culturelle de la digitalisation. Pour tenter de trouver une réponse à cette question, il est opportun de se demander si l'une des raisons expliquant le fait que le facteur humain soit invoqué de manière récurrente comme maillon faible de la sécurité de l'informatique n'est pas justement la jeunesse de l'ancrage culturel de l'informatique dans notre société. Cette dernière n'aurait ainsi pas encore complètement intégré la dimension cyber dans son propre fonctionnement. C'est un peu comme si nous n'avions pas encore appris à utiliser ces nouveaux outils de manière responsable face à notre propre société.

La culture est sans doute le levier le plus diffus, tant il semble difficile de concevoir des outils concrets permettant de la développer. Pourtant, le fait de la positionner dans ces propos après la loi et avant l'éducation soutient l'idée que l'évolution culturelle puisse notamment être induite par les initiatives en matière de législation et d'éducation.

VII. L'éducation

En 2006, la population helvétique adoptait à une très large majorité de nouveaux articles constitutionnels visant à harmoniser la scolarité obligatoire en Suisse. Le concordat intercantonal sur l'harmonisation de la scolarité obligatoire (HarmoS)[19] est entré en vigueur le 1er août 2009. Les objectifs nationaux de formation ont été intégrés aux plans d'études régionaux. En Suisse romande, le Plan d'études romand (PER)[20] a été adopté dès la rentrée 2013-2014. Ce plan, relativement récent, aborde l'informatique de manière transversale, par l'enseignement des disciplines traditionnelles. En 2007 déjà, la CDIP[21] adoptait une stratégie en matière de technologies de l'information et de la communication

18 Déclaration de Mexico sur les politiques culturelles. Conférence mondiale sur les politiques culturelles, Mexico City, 26 juillet – 6 août 1982. Repris du site de l'OFC, ‹www.bak.admin.ch/bak/fr/home/themes/definition-de-la-culture-par-l-unesco.html› (19.10.2020).

19 Accord intercantonal du 14 juin 2007 sur l'harmonisation de la scolarité obligatoire (concordat HarmoS) ‹http://edudoc.ch/record/24710/files/HarmoS_f.pdf› (19.10.2020).

20 ‹www.plandetudes.ch/per› (19.10.2020).

21 Conférence suisse des directeurs cantonaux de l'instruction publique.

(TIC)[22]. Notons qu'au niveau des gymnases, l'enseignement de l'informatique devrait revêtir un caractère obligatoire à partir de la rentrée 2022-2023[23]. L'étude PISA 2018[24] permet de se faire une idée du positionnement de notre pays par rapport aux autres pays participant à l'étude en matière de TIC. Ces éléments indiquent une volonté politique d'inclure les TIC dans l'enseignement. Cependant, comme le relève l'étude PISA précitée, « De nombreuses études ont montré qu'une utilisation excessive ou inappropriée des appareils numériques peut être liée à des risques tels que des résultats scolaires négatifs ou des problèmes dans la sphère sociale (Park, Kang & Kim, 2014), à des risques de cyber-intimidation (Mascheroni & Olafsson, 2014) et plus généralement à la sécurité dans l'utilisation d'Internet (Mainardi, Zgraggen, Nussio et Zanetti, 2012). ». Force est de constater que les stratégies, plans et programmes consultés n'abordent pas explicitement les aspects sécuritaires liés à l'utilisation de l'informatique. Nos enfants, nos jeunes apprennent donc à utiliser l'informatique en tant qu'outil permettant d'accéder à de l'information ou à entrer en communication avec d'autres, mais ils n'apprennent pas à gérer ces outils de manière sûre.

D'aucuns pourraient argumenter que la sécurité de l'information est un sujet trop compliqué pour un jeune public. Ils feraient bien de réviser leur point de vue. N'apprend-on pas aux enfants des classes primaires les rudiments de la circulation routière en vue d'assurer qu'ils circulent à vélo de manière sûre ?

De fait, l'enseignement de l'informatique devrait être intégré à l'enseignement général, dans le but d'acquérir des compétences spécifiques en lien avec l'informatique, sachant que ces compétences revêtent dorénavant une dimension transversale, la plupart des disciplines faisant désormais appel à l'informatique.

Connaissances :

- Principes de fonctionnement d'un ordinateur
- Représentation de l'information
- Fondamentaux de la communication informatique

Savoir-faire :

- Bases de programmation
- Modélisation des données
- Bonnes pratiques en matière de sécurité de l'information, notamment
  - Sécurisation des échanges
  - Sauvegarde et chiffrement des données

22 Stratégie de la CDIP en matière de technologies de l'information et de la communication (TIC) et de médias (1er mars 2007), ‹http://edudoc.ch/record/30021/files/ICT_f.pdf?version=1› (19.10.2020).

23 ‹www.edk.ch/dyn/31440.php› (19.10.2020).

24 PISA 2018.

– Identifiants et mots de passe
– Réaction en cas d'incident

Ce programme, très schématique devrait s'articuler sur plusieurs niveaux, en fonction des âges des publics cibles et ainsi se compléter.

L'informatique concerne l'ensemble de la population, et pas uniquement les plus jeunes. A ce titre, il est essentiel d'offrir à tous les groupes de population la possibilité de développer les connaissances et savoir-faire susmentionnés.

La Confédération l'a bien compris en adoptant la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022[25]. Dans le cadre de cette stratégie, une série de mesures concrètes s'inscrivant dans le champ d'action « acquisition des compétences et connaissances »[26] sous le paquet de mesures intitulé « Extension et encouragement des compétences en matière de recherche et de formation »[27] ont été énumérées. Elles ont débouché sur l'élaboration de mesures concrètes au niveau des cantons, dont une mesure ayant pour objectif de former l'ensemble des personnels des administrations cantonales et communales en matière de sécurité de l'information, mesure décrite en particulier dans l'annexe au Plan de mise en œuvre de la SNPC[28], dans l'annexe 1[29] sous le titre suivant « Développement d'un concept de formation continue et d'un module pour les administrations cantonales ».

Cette approche sectorielle n'est pas nécessairement la seule qui soit adaptée, mais elle a le mérite d'être concrète. Reste à espérer que d'autres initiatives, publiques et privées permettent de couvrir l'ensemble des secteurs.

VIII. Quelques éléments en guise de conclusion

A l'heure du réalisme, chacun doit prendre sa part de responsabilités dans une société, désormais multiculturelle, mise au défi de l'évolution rapide du secteur de l'informatique et de son intégration dans l'ensemble des domaines de vie.

Il est plaisant, pour ne pas dire facile de faire preuve de fatalisme en matière de sécurité de l'information. C'est le meilleur moyen de se décharger de sa responsabilité, de la responsabilité individuelle en la matière. Ou serait-ce, comme le relevait Hubert Reeves lors d'une interview radiophonique pour France Culture[30], le PFH, ou « putain de facteur humain » qui pousse en résumé les individus à se comporter, en fonction des circonstances, de manière irrationnelle parce que ça les arrange, acceptant ainsi une situation qui ne l'est pas.

25 Confédération suisse SN002.
26 Confédération suisse SN002, chapitre 4.1.
27 Confédération suisse SN002.
28 Confédération suisse SN002.
29 Confédération suisse SN002, Annexe 1.
30 ‹www.youtube.com/watch?v=bI-y743v6ss› (19.10.2020).

Dans les faits, chacun des acteurs de notre société doit endosser le rôle qui lui est dévolu en matière de sécurité de l'information et assumer ses responsabilités. L'industrie doit se réinventer et inclure cette composante dans sa proposition de valeur. L'Etat doit garantir les conditions-cadres afin de garantir que la gestion de l'information à l'ère du numérique se fasse dans le respect des règles nationales et internationales. L'individu enfin doit sortir de son apathie en la matière et admettre qu'il a lui aussi une responsabilité en la matière.

Si chacun des acteurs de la société est désormais appelé à prendre ses responsabilités, ce serait faire preuve d'angélisme que de penser que cette évolution puisse permettre d'empêcher la menace cybercriminelle de s'en prendre à l'information, à notre information.

Les situations de crise ne peuvent être empêchées, ce qui ne signifie pas que l'on doive adopter une attitude fataliste. Au contraire, c'est à la société civile qu'il appartient de se préparer à leur émergence, pour mieux les gérer et les surmonter, l'enjeu est sociétal.

Alors que certaines entreprises de services et autres équipementiers informatiques susurrent depuis des années une réconfortante berceuse à l'attention de leurs clients, leur instillant un message à la fois simple et agréable car garant du moindre effort : il suffit de s'équiper correctement pour être en sécurité sur la toile, notre propos ici est d'éveiller les consciences afin que chacun réalise qu'en la matière, la voie du moindre effort est également la plus périlleuse. Nul doute que des infrastructures informatiques, matérielles et logicielles, à jour sont un ingrédient essentiel de la sécurité de l'information, mais ce composant à lui seul est incapable de garantir l'atteinte de l'objectif sécuritaire. L'implication de la composante humaine est inéluctable. Pour y parvenir, l'accent doit impérativement être mis sur la prévention et la sensibilisation.

En effet, si les outils adéquats sont mis à disposition, encore faut-il les exploiter à bon escient, apprendre à percevoir l'environnement informationnel et les dangers qu'il peut receler, développer une saine vigilance à même de déclencher un réflexe de survie au bon moment.