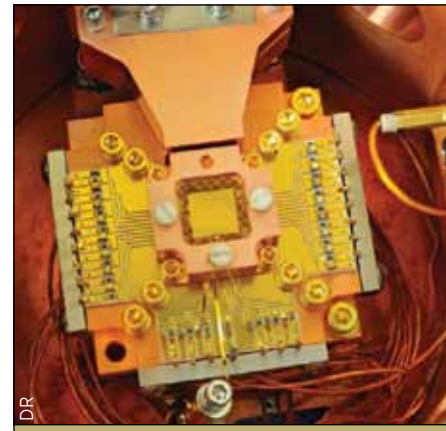
L'homme au cœur de la souveraineté numérique

Après avoir fait toute sa carrière dans la Gendarmerie, le général Marc Watin-Augouard se consacre maintenant aux enjeux que génère la transformation numérique du monde. Fondateur du Forum international de la cybersécurité, il est l'un des trois membres de son comité directeur tout en étant le directeur du centre de recherche de l'école des officiers de la Gendarmerie nationale. C'est donc en expert qu'il livre ici ses conseils sur la façon de répondre à ces nouveaux défis pour la défense et la sécurité.



DR

La taille des microprocesseurs tend vers celle de l'atome

La crise de la Covid-19, au-delà de ses aspects sanitaires, a mis en exergue les heurs et malheurs liés à la transformation numérique. La surface d'attaque a été démultipliée en quelques heures, conséquence d'un télétravail généralisé mais non sécurisé. Jamais sans doute les prédateurs n'ont été aussi actifs. Mais jamais aussi sans doute la conversion au numérique n'a été autant accélérée, tant il a fallu s'adapter, innover.

« La transformation numérique a des caractéristiques dimensionnantes qui échappent à nos repères spatio-temporels, à la vitesse de notre pensée »

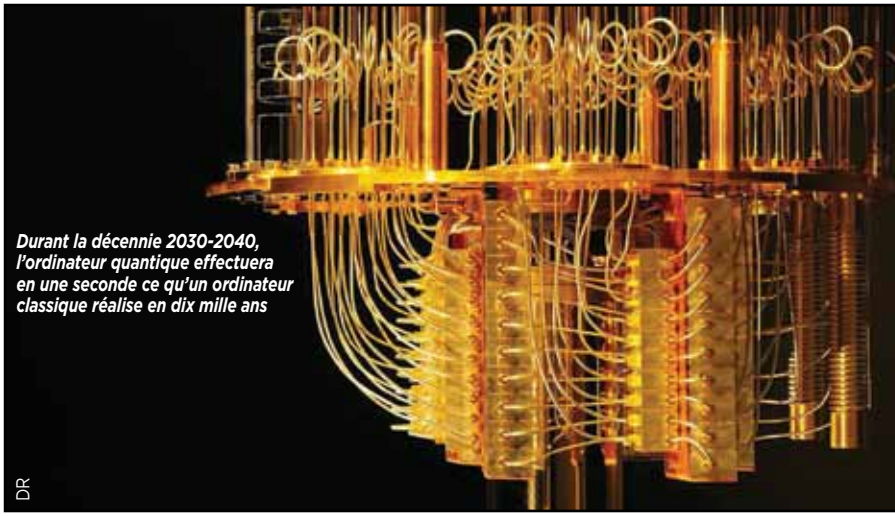
Cette transformation n'est pas une mutation, une évolution, ni même une révolution. Au vrai, il s'agit d'une « métamorphose » qui reformate notre société en bouleversant les paradigmes, sur lesquels se fondaient notre monde, pour nous conduire vers l'immatérialité. La transformation numérique échappe à nos repères habituels, tant elle s'inscrit dans l'infiniment rapide, l'infiniment grand ou l'infiniment petit. Les « nouvelles technologies » se conjuguent, exploitant l'irruption de la data et sa croissance exponentielle. Le « substrat numérique » n'est pas un espace à part, comme l'imaginaient les pionniers ; il s'intègre dans les espaces terrestre, maritime, aérien et extra-atmosphérique au point d'y imposer sa propre régulation. Dans un monde modelé selon les principes westphaliens de souveraineté, le numérique met les modes de gouvernance classiques à l'épreuve. L'État semble dépassé, voire remis en cause, mais demeure en première ligne pour lutter contre des prédateurs qui exploitent les opportunités de l'espace numérique.

La transformation numérique a des caractéristiques dimensionnantes qui échappent à nos repères spatio-temporels, à la vitesse

de notre pensée. En 1969, quatre machines étaient connectées. On en dénombrait plus de quatre-vingts milliards en 2020 avec une perspective de mille milliards en 2030, du fait des possibilités offertes par la norme *5G*. À cette date, la production annuelle de données correspondra à un contenu équivalent à mille milliards de disques durs d'un téraoctet. Grâce à la migration vers le standard *IPV6*, ce sont près de sept cents millions de milliards d'objets par mm^2 qui pourraient être connectés : chaque grain de sable du désert en quelque sorte ! En 25 ans, le trafic internet a été multiplié par sept cent mille, la taille des microprocesseurs a été réduite, selon la loi de *Moore*, pour se rapprocher du milliardième de mètre et tendre vers celle de l'atome. L'échelle des temps est remise en cause par la puissance de calcul qui va atteindre prochainement l'exaflops, c'est-à-dire un milliard de milliards d'opérations par seconde. Cette vitesse vertigineuse n'est rien, comparée à celle de l'ordinateur quantique qui, dans la décennie 2030-2040, effectuera en une seconde ce qu'un ordinateur classique réalise en dix mille ans. Ces chiffres donnent le vertige. Ils soulignent le découplage de la transformation numérique par rapport à nos modes de pensée et d'action. Nos organisations, nos process ne sont plus adaptés. La transformation numérique impose vitesse, agilité, transversalité, qualités qui ne sont pas encore partagées par des élites trop souvent déconnectées et confrontées à internet qui *« dérange l'ordre établi*[1] *»*, pour reprendre l'expression de Laure Belot. Dans ce contexte, le leadership s'appuie sur une approche « galactique » et non plus verticale. Les forces armées sont sans doute mieux à même de s'inscrire dans ce « reformatage ». Les entreprises, les administrations qui n'épouseront pas cette rupture historique sont appelées à disparaître.

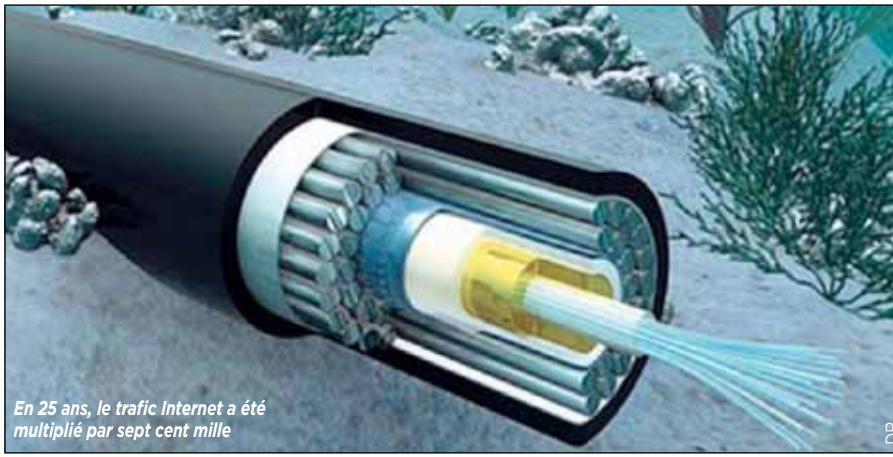
La géographie du nouveau monde n'est plus conditionnée par les distances, par les délais. Désormais la connexion, notamment grâce

1/ Laure Belot, *La déconnexion des élites, Comment internet dérange l'ordre établi*, Les Arènes, 2015.



Durant la décennie 2030-2040, l'ordinateur quantique effectuera en une seconde ce qu'un ordinateur classique réalise en dix mille ans

DR



En 25 ans, le trafic Internet a été multiplié par sept cent mille

DR

aux câbles sous-marins, crée l'immédiateté, et rapproche les territoires et les humains ou les maintient à distance, en raison d'une fracture numérique. Internet est un « réseau des réseaux » que l'on dit sans frontière[2], avec une architecture complexe, systémique. Les stocks *(datacenters)* comme les flux qu'il génère échappent au principe de territorialité sur lequel repose la souveraineté de l'État, telle qu'elle était conçue depuis les traités de Westphalie. L'atomisation du monde numérique conduit à s'interroger sur sa gouvernance. Le premier réflexe devrait inciter à rechercher auprès de l'ONU la réponse universelle. Malheureusement pour les mondialistes, les échecs successifs[3] mettent en évidence la coupure du monde en deux blocs : d'un côté celui qui veut la gouvernance de l'internet, de l'autre, celui qui revendique une gouvernance sur internet. Les seconds entendent pouvoir contrôler le bon fonctionnement, mais aussi la nature des contenus véhiculés au nom de la sécurité nationale. Faute d'unanimité, la recherche d'une gouvernance régionale[4] peut apparaître comme une alternative, dont l'efficacité se heurte cependant à l'absence d'universalité. Les associations « historiques », telles l'*ICANN*, l'*ISOC* et le *W3C*[5] , apportent des réponses utiles mais partielles et très « américano-centrées ». Faute d'une solution « publique », des acteurs privés, tel *Microsoft*, imaginent une Convention de Genève du numérique portée par des entreprises. L'Appel de Paris, lancé le

2/ Ce qui n'est pas tout à fait exact, en raison des protocoles de frontière entre les réseaux et la tendance de certains États (Russie, Chine, Iran) à créer un internet « national » pour garantir la sécurité nationale.

3/ L'échec du sommet de l'Union internationale de télécommunications (UIT), à Dubaï en 2012, et celui du Groupe d'experts gouvernementaux (GGE), en 2017.

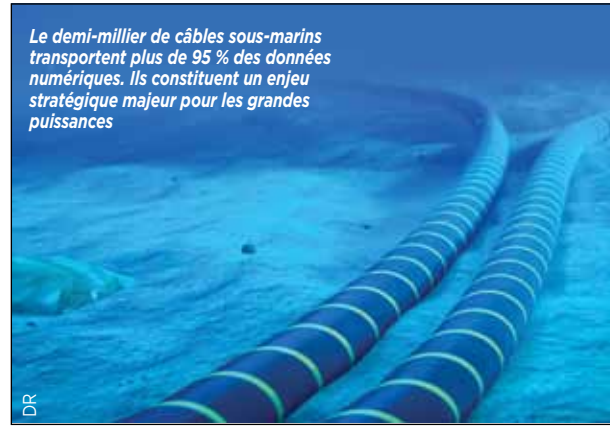
4/ Par l'Organisation de la coopération de Shangaï (OCS), le Conseil de l'Europe (Convention de Budapest), la Convention du Caire (Pays arabes), la Convention de Malabo (Union africaine).

5/ *Internet Corporation for Assigned Nales and Numbers (ICANN),* association créée notamment pour gérer les noms de domaine, *Internet Society (ISOC)*, association qui avec l'*Internet Engineering Task Force (IETF)* fait progresser les normes, *World Wide Web Consortium (W3C)*, association qui régule l'architecture du web.

12 novembre 2018 par le président Macron semble offrir une solution « multi-acteurs » qui soit susceptible de rapprocher les parties prenantes. Mais les États les plus importants (États-Unis, Russie, Chine) ne l'ont pas signé. Faute de gouvernance, ce sont les géants du Net[6] qui donnent le la, eux dont le chiffre d'affaires dépasse le PIB de nombreux États. La conception classique de l'État[7] est remise en cause : le pouvoir de conduire la diplomatie se heurte à la diplomatie des *GAFAM* et des *ATBXH*, le pouvoir de battre monnaie est concurrencé par les cryptoactifs. Le pouvoir de créer le droit cède devant des normes d'origine externe, la plupart anglo-saxonnes, qui sont subies à défaut d'avoir été inspirées[8]. Le pouvoir de rendre justice est contraint par la compétence spatiale du juge à laquelle s'oppose l'extra-territorialité de nombreux contentieux de nature pénale, civile ou commerciale. Enfin, des groupes non-étatiques s'emparent du pouvoir de « faire la guerre ».

« L'État est cependant en première ligne, car c'est vers lui que se tournent les victimes de plus en plus nombreuses des prédateurs »

L'État est cependant en première ligne, car c'est vers lui que se tournent les victimes de plus en plus nombreuses des prédateurs. Comme nous l'avons annoncé, en 2007[9], *« la cybercriminalité est la criminalité du XXIe siècle »*. L'augmentation très sensible du nombre de cyberinfractions depuis le début de la crise sanitaire confirme cette prévision. L'espace numérique subit une double migration. Celle des délinquants qui profitent des opportunités du Net : jamais ils n'ont été aussi près de leur victime et jamais aussi loin de leur juge, pourvu qu'ils opèrent depuis un État «cyber-voyou ». Le rapport gain escompté/risque pénal est optimisé. Dans le même temps, les États comprennent que le cyberespace est un territoire idéal pour une cyberconflictualité qui permet d'agir à faible coût et à faible risque. La « banderille numérique » remplace la politique de la canonnière. États et groupes criminels se rejoignent, les seconds étant souvent des



Le demi-millier de câbles sous-marins transportent plus de 95 % des données numériques. Ils constituent un enjeu stratégique majeur pour les grandes puissances

DR

6/ *GAFAM (Google, Apple, Facebook, Amazon, Microsoft)* et bientôt les *ATBXH (Ali Baba, Tencent, Baidu, Xiaomai, Huawei)*.

7/ *« Communauté d'hommes, fixée sur un territoire propre et possédant une organisation d'où résulte pour le groupe envisagé dans ses rapports avec ses membres une puissance suprême d'action, de commandement et de coercition »*, Carré de Malberg, Contribution à la théorie générale de l'État (1921).

8/ *« Code is law »* écrit en 2000 Lawrence Lessig, professeur de droit à Harvard.

9/ Marc Watin-Augouard, discours introductif du FIC 2007 : *« La cybercriminalité, criminalité du XXIe siècle »*.

« tiers attaquants » agissant au profit des premiers. Si les cyberattaques visent principalement les systèmes connectés, c'est-à-dire la « couche logicielle » du Net, la vulnérabilité de la « couche sémantique » est sans aucun doute la plus préoccupante à moyen terme. La « couche des données » est porteuse de sens, de non-sens, de contresens. Les systèmes visés à travers elle, ce sont nos esprits, notre intimité, notre vie privée, notre autodétermination. Demain ce ne sont pas les territoires qu'il conviendra de conquérir, mais les humains qu'il importera d'asservir.

« Les acteurs régaliens doivent renforcer leur coopération »

Un continuum défense-sécurité s'observe dans l'espace numérique[10], car il existe une très grande porosité entre le délinquant et le « combattant ». Tant que les conditions ne sont pas réunies[11] pour qualifier une cyberattaque d'agression armée, au sens du droit international public, toute action entre dans le champ infractionnel et donc du droit commun. La difficulté est bien là : sans pouvoir relever de la guerre, *stricto sensu*, beaucoup de cyberattaques prennent une dimension et ont des conséquences sans comparaison avec la délinquance classique. Ainsi apparaît une zone grise qui emprunte la qualification des faits au droit pénal et l'objectif poursuivi au champ de la conflictualité. C'est précisément cette brèche, cette zone hybride qu'exploitent les cyberdélinquants. Le droit classique est aujourd'hui mis à l'épreuve. Pour surmonter cette difficulté, les acteurs régaliens doivent renforcer leur coopération : l'enquête menée par un cybergendarme peut pénétrer le « terrain d'action » de COMCYBER[12] et inversement. Mais la puissance publique ne peut rien sans une coopération public/privée inédite, car les acteurs privés possèdent une grande parte des clefs de la réussite. L'ouverture du « Campus cyber » à la Défense témoigne de cette exigence.

Depuis 2008, une prise de conscience des enjeux de défense et de sécurité a conduit l'État a développer une stratégie de cybersécurité qui conjugue la lutte contre la cybercriminalité et la cyberdéfense. Mais cette montée en puissance doit être accélérée, au risque de perdre la légitimité. En effet, si l'État n'a pas la capacité de protéger les personnes et les biens et de venir en aide aux victimes, son existence même est en cause. L' « ubérisation » de l'État n'est pas une hypothèse à exclure. Sa souveraineté interne va dépendre de son « reformatage » à l'ère du numérique.
Sa souveraineté externe s'appuie encore sur les principes westphaliens, mais elle doit être revisitée à l'ère du numérique. Pour comprendre il suffit d'emprunter l'image des « poupées russes »[13] qui s'emboîtent depuis la plus petite. Celle-ci nous représente. La souverai-

---

10/ Marc Watin-Augouard , *« Le continuum défense-sécurité dans le cyberespace »*, *Huffington Post* 2013, *Res Militaris* 2015.

11/ Il faut en effet que la cyberattaque produise des effets physiques au moins équivalents à ceux que l'on observe lors d'une attaque cinétique. Par ailleurs, l'agression armée doit pouvoir être attribuée, ce qui est rarement possible, du moins dans un premier temps, lors d'une cyberattaque.

12/ La création récente d'un commandement de la Gendarmerie du cyberespace, COM/CYBERGEND est annonciateur d'une coopération renforcée entre les forces armées (armées et Gendarmerie).

13/ Le lecteur ne verra dans cet emprunt aucun « clin d'œil » au nouveau tsar de Russie, dont on connaît le penchant pour la « guerre informationnelle ».

neté collective est vaine si nous ne sommes pas nous-mêmes souverains, maîtres de notre « moi-numérique ». Mais la souveraineté des personnes physiques est tributaire de celle des personnes morales (entreprises, administrations, collectivités territoriales, associations, etc.). Cette dernière dépend de celle de l'État. Mais l'État ne peut être aujourd'hui souverain dans l'espace numérique si l'Europe n'est pas souveraine. Sans renoncer aux obligations régaliennes dans une « Europe des nations », nous devons construire une Europe numérique forte. Nous sommes, en effet au milieu d'un étau, dont les deux mâchoires qui se resserrent sont constituées par les États-Unis et la Chine. Si l'Europe ne s'affirme pas, nous serons écrasés, sauf si nous décidons d'être « américains » ou « chinois ». Entre le mercantilisme numérique, illustré par les *GAFA*M, et le totalitarisme numérique d'une société de surveillance, il y a une troisième voix, une troisième voie. L'Europe doit porter un discours « gaullien » vis-à-vis du reste du monde pour construire une société numérique qui place l'humain en son cœur. La présidence française de l'Union européenne[14] est une belle opportunité pour donner du souffle à une Europe qui en a grand besoin.

Les enjeux de défense et de sécurité à l'heure de la transformation numérique exigent de répondre à la question « comment ? », celle qui inspire le choix des voies et moyens. Mais cette démarche est vaine sans la réponse à la question « pourquoi ? » qui nous invite à nous appuyer sur les valeurs trop souvent oubliées ou combattues par ceux-là mêmes qui savent qu'elles sont notre force. *« En notre temps, la seule querelle qui vaille est celle de l'homme »*. Le général de Gaulle, sans le savoir, a écrit pour la génération d'aujourd'hui qui devra replacer l'humain au cœur du débat, sauf à devenir une colonie de zombis, à l'âge de la multitude qui sera en fait celui de la solitude.

Marc WATIN-AUGOUARD
Officier général (2s)

14/ À compter du 1er janvier 2022.

15/ Nicolas Colin, Henri Verdier, *L'âge de la multitude*, Armand Colin, 2015.

L'empreinte numérique

La liberté individuelle, mais aussi la souveraineté nationale, reposent sur la maîtrise de l'empreinte numérique que chacun laisse inévitablement sur Internet. Ces traces étant exploitées majoritairement par des multinationales américaines, il existe cependant des moyens techniques et juridiques permettant d'échapper à leur emprise.

DR

Chaque connexion à Internet oblige à y laisser des données personnelles

Toute personne qui se connecte à Internet, avec quelque appareil que ce soit, y laisse des traces. Elle peut penser que sa navigation sur le Web est noyée dans la masse, et qu'elle ne sera pas remarquée puisqu'elle n'a pas d'importance particulière. Cette croyance très répandue est malheureusement inexacte. Même si la personne n'a, selon elle, « rien à cacher », son comportement intéresse les grandes sociétés.

Chaque connexion à Internet oblige à y laisser des données personnelles, de manière généralement involontaire. Les sites relèvent systématiquement l'adresse *IP*[1] du périphérique informatique connecté. Celle-ci est unique, et lui permet d'être reconnue sur le réseau Internet afin que les serveurs distants puissent lui envoyer l'information demandée. Attribuée par le fournisseur d'accès, elle constitue une trace inévitable de l'activité de l'internaute sur le Web. Elle est enregistrée sur les serveurs contactés au gré de la navigation et permet la localisation de l'appareil utilisé. Le serveur relèvera en même temps le nom du navigateur, la résolution d'écran et le système d'exploitation utilisés, ainsi que l'adresse du dernier site visité. Ces données constituent le profil de base. La probabilité que deux internautes aient le même étant très faible, ils sont donc parfaitement identifiables. Les serveurs conserveront les journaux de connexion pendant une certaine durée (un an en France, illimitée aux États-Unis).

Simultanément, des codes informatiques, les *« cookies »*, sont déposés sur le disque dur de l'ordinateur via le navigateur. Ceux-ci ont d'abord un but pratique : lors de la connexion suivante, l'internaute retrouve l'affichage tel qu'il a été paramétré, notamment la langue. Ils permettent aussi à l'éditeur du site Internet de savoir quelle est son audience, ainsi que le comportement de ses utilisateurs. Un maximum d'informations est donc recueilli : pages vues, temps passé sur la page, etc. Mais au-delà de cet intérêt pratique, l'envoi de *« cookies »* a des objectifs plus pernicieux.

1/ *Internet Protocol*.

Après regroupement et analyse par des sociétés spécialisées, ces codes informatiques permettent de définir le profil de l'internaute en cernant ses centres d'intérêt, son environnement privé, social et professionnel, pour lui envoyer des publicités de mieux en mieux ciblées. Ce sont donc de véritables outils d'influence.

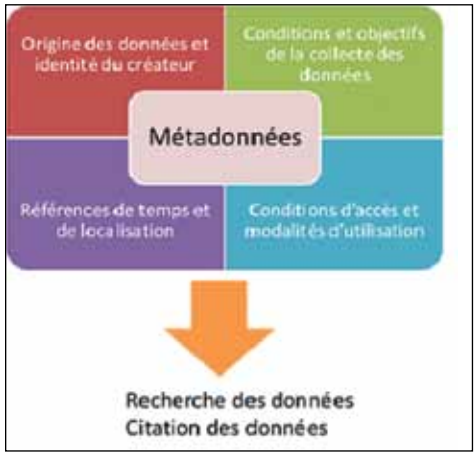
« La récolte massive des *cookies* constitue, pour l'instant, le moteur principal du modèle économique d'Internet »

La récolte massive des *« cookies »* constitue, pour l'instant, le moteur principal du modèle économique d'Internet. La consultation des sites étant gratuite, la réception de publicités, sur lesquelles il est proposé de cliquer, est la contrepartie de cette gratuité, car ce sont elles qui financent les sites Internet. Les profils sont commercialisés, les données étant « l'or noir » de l'économie du XXIe siècle. Les renseignements laissés sur les réseaux sociaux permettent de dresser un profil encore plus complet de l'internaute. D'après le site officiel d'*Instagram*, les renseignements suivants sont recueillis quand l'internaute se connecte à *Instagram*, *Facebook* ou *Messenger* :

- les métadonnées[2] du fichier fourni ;
- des informations sur les personnes, les pages, les comptes et les groupes avec lesquels il est en relation, ainsi que la manière dont il interagit avec eux ;
- les données concernant ses achats et ses transactions ;
- des activités d'autres personnes et les informations qu'elles fournissent le concernant ;
- des informations techniques sur les appareils utilisés et leur environnement ;
- des données issues des paramètres de l'appareil (dont la localisation *GPS*) ;
- des informations provenant des partenaires d'*Instagram*, *Facebook* et *Messenger* ; c'est ainsi que le site du journal *Le Monde* comporte des « mouchards » de *Facebook*, *Twitter* et *Google*, que le lecteur ait un compte sur ces réseaux ou non.

Ces informations peuvent être partagées avec d'autres à l'insu de la personne concernée : sur un réseau social, on mène une vie… sociale. Il est donc illusoire de penser y mener une vie privée.

Les ordiphones (« *smartphones* ») sont beaucoup plus indiscrets que les ordinateurs classiques et sont considérés comme de véritables aspirateurs à données. En effet, de nombreuses applications mobiles exigent, pour pouvoir les utiliser, de leur octroyer des permissions très intrusives.



DR

2/ Les métadonnées contiennent des informations sur la source du document, sa nature, son contenu et sa localisation physique ; elles ont pour effet d'améliorer l'efficacité des recherches d'information.

C'est ainsi que *Strava* permettait de suivre l'entraînement sportif des agents de la DGSE autour de la caserne Mortier[3]. De même, il est souvent étonnant de constater qu'un simple jeu demande aussi l'accès au carnet d'adresses de l'ordiphone pour fonctionner…

« L'empreinte numérique générée par l'activité Internet de chaque internaute peut grossir très vite »

Même si une application ne demande pas de permission particulière, ce qui est rare, le simple fait de la télécharger sur *Google Play* ou l'*Appstore* fournit à ces plateformes des renseignements précieux. *Google* et *Apple* connaîtront ainsi, grâce au gouvernement…, le nom des citoyens qui ont téléchargé l'application *Tousanticovid* et ajusteront les publicités envoyées en conséquence.

L'empreinte numérique générée par l'activité Internet de chaque internaute peut grossir très vite, faisant peser des risques non-négligeables sur sa vie privée et sa vie professionnelle. La réception quotidienne de publicités qui, comme par hasard, correspondent généralement aux goûts, aux désirs, aux recherches de l'intéressé voire à sa localisation, en est la conséquence la plus visible.

Mais les conséquences peuvent être aussi beaucoup plus graves, les empreintes numériques pouvant être compromises par le piratage du serveur où elles se trouvent et être utilisées dans des buts malveillants, voire criminels. Et les piratages ne sont pas rares : ainsi, des données personnelles, concernant 500 millions de comptes *Facebook*, dont potentiellement 20 millions en France, sont actuellement diffusées sur un site de « *hackers*[4] ». Ces piratages peuvent donner lieu à l'usurpation de l'identité de l'internaute à des fins frauduleuses, ou à la mise en cause de sa réputation. Le réalisme des courriels de « hameçonnage » est renforcé par l'exploitation des empreintes numériques.

Les photos peuvent contenir des balises indiquant où et quand elles ont été prises. Ces informations pourraient être utilisées pour localiser la maison de l'internaute, l'endroit où ses enfants vont à l'école. Ainsi, les photos publiées sur *Instagram* par un militaire en opération extérieure peuvent être rapprochées de celles déjà prises en France, révélant d'emblée que l'intéressé est absent de son domicile.

« Des actions simples permettent de limiter le pistage »

Des actions simples permettent de limiter le pistage :

- le choix du moteur de recherche est la plus efficace ; ainsi, il convient de bannir *Google*, *Yahoo*, au profit de moteurs qui ne pistent pas leurs utilisateurs comme *Qwant* ;
- celui du navigateur en est une autre ; *Chrome* ou *Edge* sont à délaisser au profit de *Firefox*, navigateur libre qui dispose de nombreuses extensions de protection : dans tous les cas, il est prudent d'effacer l'historique de navigation à la fin de chaque session ;
- des choix plus radicaux comme l'utilisation d'un *VPN* (réseau virtuel privé) permettent d'avoir une protection plus complète ;
- pour la messagerie, prenant acte du fait que *Gmail, Hotmail, Outlook*…, lisent les courriels à livre ouvert, il convient de privilégier les ap-

3/ *BFM TV*, 12/01/2018.

4/ *Le Point*, 03/04/2021.

DR

Il faut recourir le plus souvent possible au socle interministériel de logiciels libres (data.gouv.fr)

plications chiffrées de bout en bout comme *Protonmail* ou *Tutanota* pour avoir une confidentialité totale ;

• pour les ordiphones, il vaut mieux utiliser de préférence ceux équipés d'un système d'exploitation libre comme *E*[5] (qui est français), sinon privilégier les téléchargements sur une plateforme ne pistant pas ses utilisateurs, comme *F-DROID*[6] ;

• il existe aussi des alternatives libres aux réseaux sociaux américains.

« Il est souhaitable de se connecter en priorité à des sites européens localisés en Europe »

Il est souhaitable de se connecter en priorité à des sites européens localisés en Europe, car les données personnelles sont ainsi protégées par le RGPD[7]. Ce n'est pas le cas des données médicales confiées à *Doctolib* car elles sont hébergées sur les serveurs d' *Amazon Web Services*, société soumise, de par sa nationalité, au *Cloud Act*[8] et donc susceptible de répondre à toute demande des services officiels américains, même si les données sont en Europe. Ce n'est pas le cas non plus des solutions de visioconférence à la mode comme *Zoom* et *Viméo*, trop souvent utilisées, y compris par des organismes officiels, alors qu'il s'agit d'applications américaines, donc soumises aussi au *Cloud Act*. Le socle interministériel de logiciels libres préconise l'emploi de l'application *Jitsi Meet*[9].

Les profils réalisés à partir des *« cookies »* permettent de mieux cibler les internautes afin de les pousser à effectuer une action (achat ?, vote ?) qu'ils n'auraient peut-être pas faite autrement. Sauf à voir la liberté individuelle se réduire comme une peau de chagrin sous la pression de ce contrôle social insidieux, la limitation de l'empreinte numérique laissée sur Internet doit être une préoccupation quotidienne.

Le fonctionnement de la démocratie est également impacté puisque la connaissance étendue des empreintes numériques peut en fausser l'expression légitime, comme l'a démontré le scandale de la société *Cambridge Analytica*, accusée d'avoir exploité les données de 87 millions d'utilisateurs de *Facebook* afin de favoriser le *Brexit* et l'élection de Donald Trump.

La maîtrise des données personnelles est une condition essentielle, non seulement de la liberté individuelle mais aussi de la souveraineté nationale.

Jacques TABARY
Commissaire en chef de 1ère classe (er)
Membre de l'ASAF

5/ https://e.foundation/fr/?lang=fr

6/ https://fr.wikipedia.org/wiki/F-Droid

7/ Règlement général pour la protection des données.

8/ https://fr.wikipedia.org/wiki/CLOUD_Act

9/ https://framatalk.org/accueil/fr/