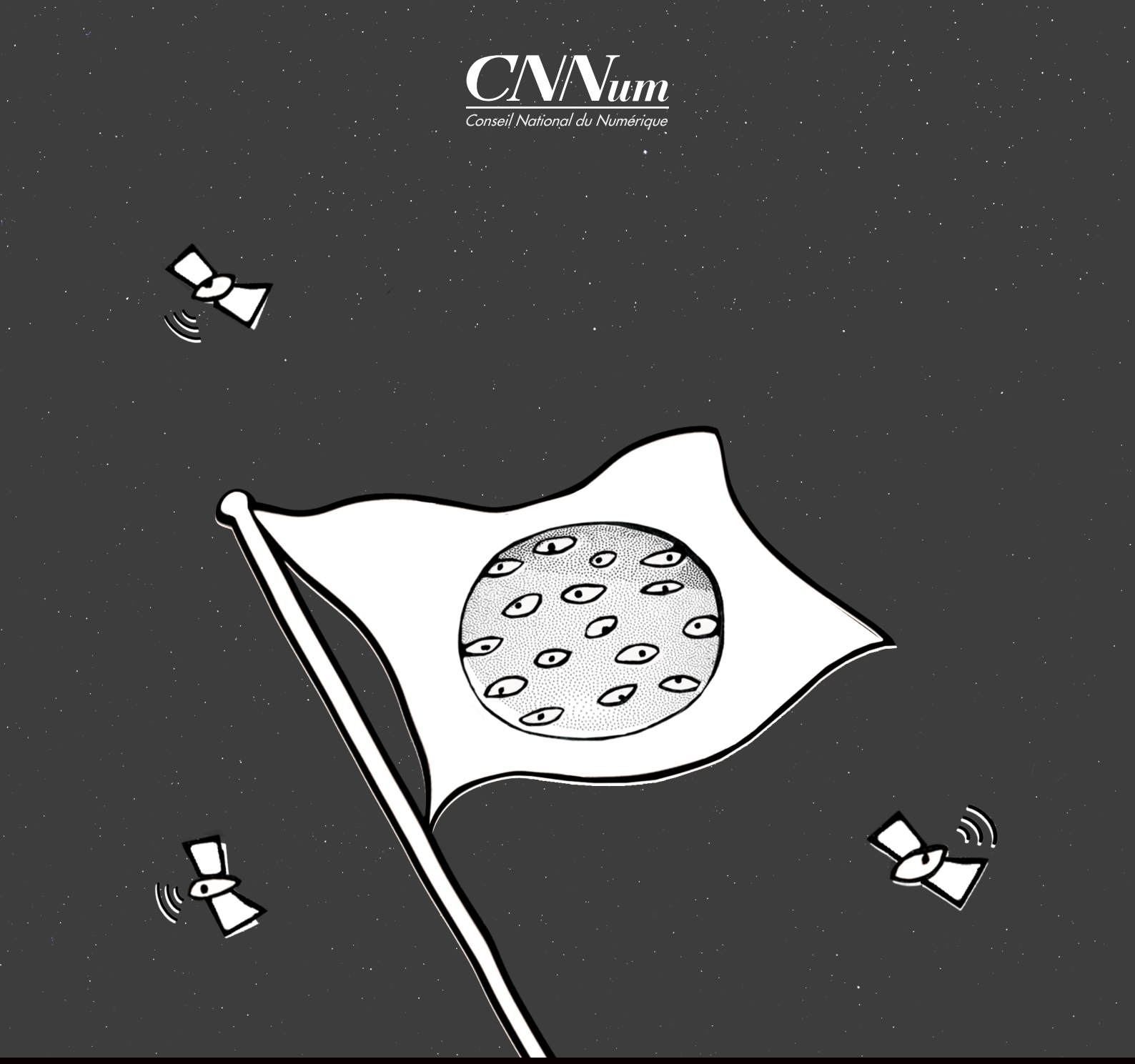
CNNum
Conseil National du Numérique



PRÉDICTIONS CHIFFREMENT ET LIBERTÉS

septembre 2017

PRÉDICTIONS, CHIFFREMENT ET LIBERTÉS

Le Conseil national du numérique s'est saisi à l'été 2016 de la question du chiffrement. Cette autosaisine, pilotée par Rand Hindi, faisait suite aux annonces conjointes de Bernard Cazeneuve, alors ministre de l'Intérieur, et de son homologue allemand Thomas de Maizière, visant à « *armer nos démocraties sur la question du chiffrement* ». Près d'un an plus tard et dans une situation sécuritaire toujours critique, le chiffrement reste au cœur de la tension entre protections des données personnelles, innovation technologique et surveillance. Dans une déclaration commune avec la Première ministre britannique Theresa May, le Président de la République Emmanuel Macron s'est une nouvelle fois prononcé en faveur d'un meilleur accès aux contenus chiffrés, « *dans des conditions qui préservent la confidentialité des correspondances, afin que* [*les*] *messageries ne puissent pas être l'outil des terroristes ou des criminels* ». L'Union européenne doit examiner l'opportunité d'une législation sur le sujet à l'automne. L'occasion, pour le Conseil, d'expliciter sa position et d'élargir la question à la protection des droits et libertés sur Internet, face à une trajectoire sécuritaire qu'il juge préoccupante.

AVIS DU CONSEIL _

En bouleversant notre relation au temps, à l'espace, à l'autre, la révolution numérique est à l'origine d'un changement profond de nos sociétés. Le chemin de cette révolution n'est pas tracé à l'avance : l'effet des technologies, tout autant émancipateur qu'asservissant, est toujours issu des choix sociaux et politiques. **Il s'agit donc de veiller à ce que cette révolution, qui porte en elle la promesse d'une refondation démocratique, ne s'accompagne finalement d'une régression des droits et libertés ou de l'État de droit.**

La situation est critique. Il n'est pas question de nier que les nouvelles formes de communication et d'organisation facilitées par le numérique peuvent complexifier la tâche des acteurs en charge de la sécurité publique. C'est particulièrement vrai en matière de terrorisme, qui a fait plusieurs centaines de victimes sur notre territoire. Dans ce climat d'extrême tension, les pouvoirs publics semblent engagés dans une spirale infernale, pour un but — la sécurité absolue — dont l'horizon ne peut jamais être atteint. Chacun est conscient que le risque zéro n'existe pas, pourtant la tentation est forte d'accumuler encore et encore de nouveaux moyens d'action, de privilégier un désir de sécurité au détriment des exigences de l'État de droit et de notre économie. Ainsi le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, actuellement examiné par la nouvelle assemblée, sera **le quinzième texte sécuritaire promulgué depuis 2012**. Certaines des dispositions contenues dans ces différents textes ne sont d'ailleurs toujours pas mises en œuvre. La question de l'efficacité de ces moyens exorbitants mérite d'être posée, en particulier au regard du retour d'expérience américain (voir annexes).

Le Conseil national du numérique a régulièrement pris position dans le débat qui oppose, parfois artificiellement, la sécurité aux libertés individuelles et collectives. Il l'a fait au moment de la loi de programmation militaire de 2013 (collecte en temps réel de données par l'État sans véritable contrôle), la loi renforçant les dispositions relatives à la lutte contre le terrorisme de 2014 (blocage administratif — sans contrôle a priori du juge judiciaire — des sites internet), la loi relative au renseignement en 2015 et, plus récemment à l'occasion de la polémique entourant le fichier des « *titres électroniques sécurisés* » (TES). À chacune de ces occasions, le Conseil a souligné la nécessité d'une **concertation préalable** sur ces sujets aussi complexes que majeurs, qui nous engagent pour les années à venir.

LA SÉCURITÉ EST UN BUT DONT L'HORIZON N'EST JAMAIS ATTEINT.

Dans le discours politique comme dans sa traduction législative, Internet apparaît comme un coupable idéal. Mieux, il sert souvent de terrain d'expérimentation pour le déploiement dans le droit commun des instruments sécuritaires. Pour cause, l'opinion publique s'accommode plus facilement de la surveillance numérique, globalement (et à tort) considérée comme moins intrusive qu'une surveillance physique. Là encore, il n'est pas question de nier le rôle — déterminant — du numérique dans l'accroissement de la menace terroriste, mais cette responsabilité est plus complexe qu'il n'y paraît. Si le web est devenu un terrain favorable à l'endoctrinement, dans la plupart des cas, l'élément déclencheur de la radicalisation reste le contact humain — hors ligne[1].

[1] "Le déclencheur est dans 95% des cas lié à un contact humain" (Unité de coordination de la lutte antiterroriste).

PRÉDICTIONS ET CONTOURNEMENTS DE L'AUTORITÉ JUDICIAIRE

L'objectif de lutte contre le terrorisme aboutit à une multiplication de dispositions qui entérinent l'affaiblissement de l'autorité judiciaire au profit de l'autorité administrative. La loi antiterroriste de 2014 a donné à l'administration le pouvoir de bloquer et de déréférencer des sites Internet, sans contrôle préalable du juge. La loi relative au renseignement de 2015 a renforcé cette tendance à se passer de l'autorité judiciaire, ouvrant la voie à la généralisation de méthodes intrusives, hors du contrôle des juges, pourtant garants des libertés individuelles. De la même façon, le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, porté par le gouvernement actuel, vise à introduire dans le droit commun des dispositions d'exception et contribue, une fois encore, à la marginalisation de l'autorité judiciaire.

Malgré l'urgence et la complexité technique inhérentes aux affaires antiterroristes, le Conseil tient à réaffirmer son attachement au **principe d'une intervention judiciaire** lorsque sont mises en cause les libertés individuelles. Si le passage par le juge ne constitue pas une garantie absolue, il s'apparente à une garantie nécessaire : contrairement à l'administration ou aux services de sécurité, régis par un pouvoir hiérarchique, le juge est indépendant. Il doit ainsi s'assurer, avant que la mesure ne soit mise en œuvre, que celle-ci n'est pas arbitraire, qu'elle est nécessaire et proportionnée à l'objectif poursuivi et qu'elle respecte les droits de la personne. S'il n'est pas question de nier l'importance du contrôle du juge administratif et son rôle historique dans la préservation des libertés individuelles, il faut noter que ce contrôle intervient nécessairement après la mise en cause d'une liberté et suppose la saisine préalable du juge administratif — ce qui en pratique n'arrive que très rarement.

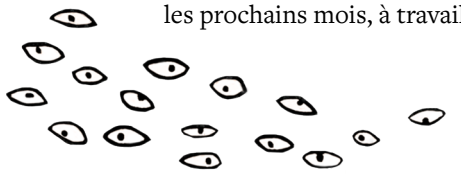
Législations après législations, la logique du soupçon semble l'emporter. La notion de comportement tend à se substituer à celle d'activité : au nom d'une conception prédictive de la lutte antiterroriste, des individus pourraient être contraints non parce qu'ils prépareraient des crimes ou des délits, mais bien parce qu'ils seraient susceptibles d'en commettre. Ce modèle interpelle à plusieurs égards.

De ponctuelles et ciblées, les pratiques de surveillance deviennent permanentes et générales. Les évolutions des usages technologiques, l'augmentation des capacités de calcul, les progrès de l'intelligence artificielle et du *deep learning* associés à la baisse continue des coûts de stockage des données rendent possible l'application de modèles prédictifs aux objectifs de sécurité nationale. L'intention est louable et semble frappée au coin du bon sens. Elle soulève néanmoins des considérations bien spécifiques. En termes de fiabilité, d'abord : quiconque s'intéresse aux modèles prédictifs est forcément confronté à la définition, particulièrement ardue, du seuil

de détection. Le dispositif des « *boîtes noires* » prévu par la loi renseignement illustre cette difficulté. Censé analyser les réseaux pour y repérer les « *signaux faibles* » d'une activité terroriste, cet instrument est naturellement confronté au problème des faux-positifs, ces erreurs qui découlent mécaniquement de l'identification de comportements statistiquement très rares[2]. En matière de renseignement, de telles erreurs peuvent donner lieu à une surveillance abusive parce que décidée sur de mauvais fondements. Malgré les progrès spectaculaires de l'intelligence artificielle, ces algorithmes de traitement de données n'en sont pas moins exempts de biais, notamment sociologiques. Ceux-ci peuvent contribuer à **renforcer les discriminations dont sont victimes certains groupes d'individus au sein d'une population**. Ces dangers, qui commencent à être bien documentés, ont récemment fait irruption dans le débat public autour des questions de police prédictive.

Dès lors, la doctrine du contrôle doit évoluer pour encadrer ces nouvelles réalités techniques. En plus du nécessaire équilibre entre le respect de la vie privée des individus et les impératifs de sécurité, le contrôleur doit s'assurer que les pratiques de surveillance ne contribuent pas à créer de la discrimination. Dans ce contexte, il est probablement nécessaire d'ajuster notre conception juridique et philosophique de la protection des individus face aux traitements de leurs données. Il s'agit de prendre en compte ces modes de profilage qui, mis au service de la prédiction, s'intéressent moins à l'individu en tant que tel qu'au groupe statistique auquel il est rattaché. Un chantier doit être ouvert en matière d'explicabilité de ces algorithmes de traitement de données : le contrôleur doit être en mesure d'ouvrir ces boîtes noires, afin de s'assurer de leur équité, pour organiser une voie de retour démocratique et l'effectivité du droit au recours des individus. Le Conseil se questionne également sur l'opportunité de renforcer les incriminations pénales relatives aux atteintes aux données personnelles sur le fondement de la vie privée. À mesure du développement de l'intelligence artificielle, ces questions sont appelées à devenir majeures. Le Conseil sera amené, dans les prochains mois, à travailler plus avant sur ces sujets.

TEXTES APRÈS TEXTES, LA LOGIQUE DU SOUPÇON SEMBLE L'EMPORTER.



[2] Sur ce dernier point, les chercheurs de l'Inria avaient alerté le gouvernement sur la production systématique d'erreurs même dans un système bien réglé, qui sont d'autant plus nombreuses que la masse de données à traiter est importante. En effet, la difficulté réside en effet dans l'identification fiable de comportement statistiquement très rares. Les chercheurs de l'Inria l'avaient démontré de la façon suivante : supposons que l'on recherche des terroristes dans une population. Tout algorithme de détection a une marge d'erreur, c'est-à-dire va identifier des personnes sans intention terroriste (des « faux-positifs »). Si la marge d'erreur est de 1%, ce qui est considéré à ce jour comme très faible, l'algorithme identifiera quelques 600 000 personnes sur une population totale de 60 millions de personnes. Si le nombre de vrais terroristes est par exemple de 60, ces vrais terroristes ne représenteront que 0,01% de la population identifiée [comme potentiellement suspecte]. De plus, un tel algorithme devra prendre en compte le fait que les individus ciblés par ce dispositif chercheront à adopter un comportement visant à échapper aux *patterns* définis puisqu'ils s'adaptent en permanence pour échapper à la détection.

LE CHIFFREMENT, AU CŒUR DU DÉBAT OPPOSANT LIBERTÉS ET SÉCURITÉ

Dans ce débat, le chiffrement des données semble cristalliser la tension opposant la sécurité aux libertés individuelles. Depuis les révélations d'Edward Snowden et la prise de conscience sur l'ampleur de la surveillance étatique, les entreprises du numérique ont de plus en plus recours à des solutions de chiffrement. Elles sont souvent proposées par défaut aux utilisateurs, avec un chiffrement de bout à bout, c'est-à-dire que ces derniers sont les seuls à détenir les clés de déchiffrement, l'entreprise fournissant le service n'étant pas en mesure d'accéder elle-même aux communications privées de ses utilisateurs.

On parle de **chiffrement de bout à bout** lorsque l'information est chiffrée de bout à bout de la communication, c'est-à-dire lorsque seuls l'émetteur et le destinataire de la communication détiennent la clé permettant de déchiffrer le message. Cette information est donc théoriquement indéchiffrable par des tiers, et notamment par l'intermédiaire qui transporte le message. Ne détenant pas elle même la clé de déchiffrement, l'entreprise est donc dans l'incapacité de répondre aux réquisitions des forces de l'ordre pour accéder aux données chiffrées.

Signal, Telegram, WhatsApp... les messageries sécurisées se sont multipliées ces dernières années. Elles sont aujourd'hui dans le collimateur des forces de l'ordre en raison du chiffrement bout à bout. Dans de nombreux pays, dont la France, les autorités publiques ont fait état de leur préoccupation : ils redoutent de ne pas être en mesure de prévenir une attaque terroriste ou d'enquêter sur des activités criminelles.

Le plan présenté par Emmanuel Macron et Theresa May vise à « *permettre l'accès au contenu chiffré* ». Ce plan précise que « *lorsque les technologies de chiffrement sont utilisées par des groupes criminels, voire terroristes, il doit exister une possibilité d'accès au contenu des communications* ». Cette déclaration peut laisser songeur : comment accéder à des contenus chiffrés dont on n'a pas la clef ?

Une porte dérobée (ou backdoor) est un point d'accès à un système d'exploitation, à un programme ou à un service en ligne. Ces passages secrets sont généralement introduits à l'insu de l'utilisateur. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle. Pour des pirates ou des services de renseignement, l'intérêt réside dans la possibilité de surveiller les activités de l'utilisateur, copier ou détruire des données, prendre le contrôle d'un ordinateur, etc.

Une proposition régulièrement avancée à des fins de sécurité par certains politiques, serait de contraindre les constructeurs et fournisseurs de services et d'applications numériques à introduire délibérément dans leurs systèmes des « portes dérobées » (backdoors). Celles-ci auraient pourtant des conséquences dramatiques pour l'ensemble des utilisateurs. Les cyberattaques récentes et massives ne cessent de démontrer le risque que peut faire courir le maintien volontaire de failles de sécurités, par des agences de renseignement à des fins offensives, pour la sécurité des utilisateurs.

Plus généralement, l'affaiblissement des moyens de chiffrement, aujourd'hui largement diffusés dans les services grand public, aurait sans aucun doute une efficacité très limitée sur l'infime minorité d'utilisateurs qui les utilisent pour cacher des desseins criminels. En effet, le développement de logiciels non contrôlables, faciles à distribuer et offrant un niveau de sécurité très élevé est à la portée de n'importe quelle organisation criminelle. Répétons-le : **il n'existe pas de technique d'affaiblissement systémique du chiffrement qui ne permettrait de viser que les activités criminelles. Limiter le chiffrement pour le grand public reviendrait alors à en accorder le monopole aux organisations qui sauront en abuser**.

Il est utile de rappeler que le chiffrement des données n'est pas un obstacle insurmontable pour accéder aux informations nécessaires aux enquêtes. Il existe de nombreux moyens de le contourner, même s'il est très robuste, en exploitant des failles techniques ou en s'introduisant directement dans l'équipement de la personne ciblée. En outre, si les contenus sont chiffrés, les métadonnées y afférant restent généralement en clair, dans la mesure où elles sont indispensables au fonctionnement du système. Ces métadonnées sont bien souvent suffisantes pour cartographier un réseau ou localiser des individus, sans qu'il y ait besoin pour cela d'entrer dans le contenu des communications privées.

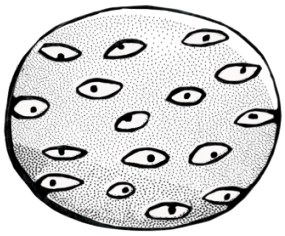
Le Conseil affirme à nouveau que la coopération avec les fournisseurs de produits et de services sécurisés dans l'accès judiciaire aux métadonnées reste l'une des procédures à privilégier. Pour ce faire, le Conseil préconise de renforcer les règles de coopération judiciaire, afin de réduire ces délais de transmission.

UN OUTIL VITAL POUR NOTRE SÉCURITÉ EN LIGNE

Internet est devenu le support de nos communications. Il est essentiel au développement de nos sociétés et de nos économies. Dans le même temps, pas une semaine ne s'écoule sans que l'actualité ne se fasse l'écho d'une faille critique découverte dans un système, de fuites ou de vols majeurs de données personnelles.

Dans ce contexte, **le chiffrement est un élément vital de notre sécurité en ligne. Pour les citoyens, le chiffrement est un levier majeur de confiance dans le monde numérique** : au quotidien, il permet de protéger les communications et les transactions de milliards d'individus contre des cybermenaces qui se font toujours plus redoutables. Le chiffrement est d'ailleurs un outil au service de la protection de la vie privée consacrée par le règlement général sur la protection des données. Pour les entreprises, le chiffrement reste le meilleur rempart contre l'espionnage économique. Il est indispensable pour qui souhaite protéger ses actifs immatériels. Enfin, pour l'État, il s'agit tout simplement d'une condition de sa souveraineté. Les révélations d'Edward Snowden n'ont eu de cesse de le démontrer.

Dans ces conditions, le Conseil se prononce une fois de plus pour une promotion massive du chiffrement, auprès du public, des acteurs économiques et des administrations.



PAR CONSÉQUENT, LE CONSEIL CONSIDÈRE QUE_

Tout projet législatif et réglementaire qui emporte des conséquences importantes sur les libertés doit faire l'objet d'une vaste consultation préalable ;

Le principe de l'intervention d'une autorité judiciaire doit être réaffirmé chaque fois qu'est mise en cause une liberté ;

Les pouvoirs publics doivent refuser la logique du soupçon, qui ouvre la porte à l'arbitraire, dans la mise en œuvre des politiques sécuritaires sur Internet ;

Le chiffrement est un outil vital pour la sécurité en ligne ; en conséquence il doit être diffusé massivement auprès des citoyens, des acteurs économiques et des administrations ;

Le chiffrement – et les libertés fondamentales dont il permet l'exercice – constitue un rempart contre l'éventuel arbitraire des États. Il nous protège aussi contre le contrôle croissant des acteurs économiques sur nos vies ;

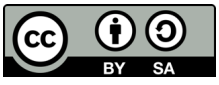
Le chiffrement ne constitue pas un obstacle insurmontable pour les enquêtes. Il est possible de le contourner dans le cadre d'une surveillance ciblée. À ce titre, il est surtout un rempart contre la surveillance de masse ;

Plus généralement, compte-tenu de l'augmentation des pouvoirs des services de renseignement et des incidences importantes sur la vie des citoyens, le Conseil s'interroge sur la nécessité d'établir un droit au recours effectif et, au-delà un droit à l'explicabilité des algorithmes de prédiction. Il se questionne également sur l'opportunité de renforcer les incriminations pénales relatives aux atteintes aux données personnelles sur le fondement de la vie privée.

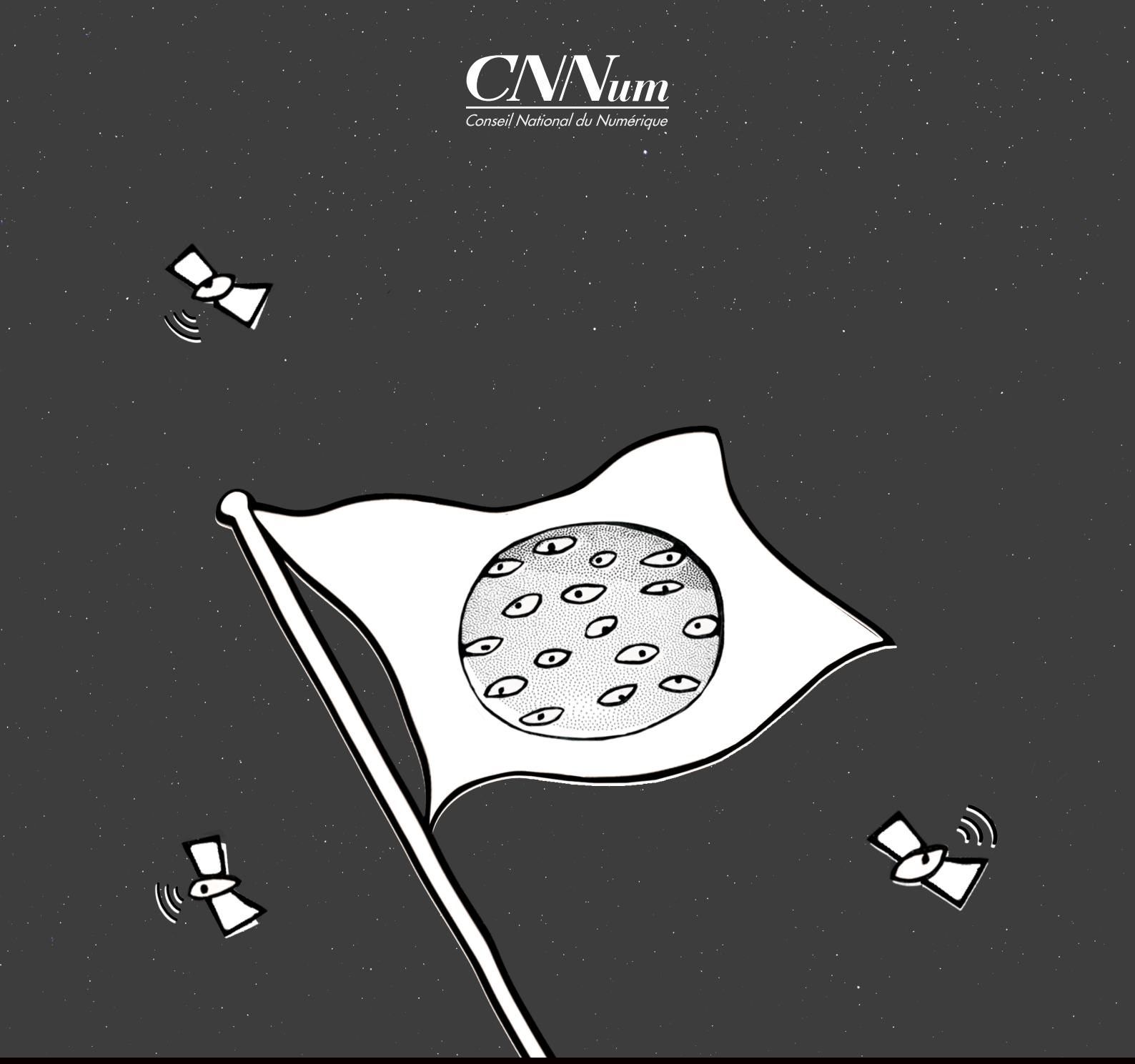
www.cnnumerique.fr

Conseil national du numérique
Bâtiment Atrium
5 place des Vins-de-France
75573 Paris Cedex 12
info@cnnumerique.fr - @CNNum
01 53 44 21 27

CONTACT PRESSE
Yann Bonnet, Secrétaire Général
presse@cnnumerique.fr
01 53 44 21 27



CNNum
Conseil National du Numérique

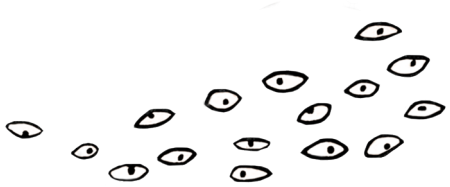


PREDICTIONS ENCRYPTION AND DIGITAL RIGHTS

september 2017

PREDICTIONS, ENCRYPTION AND FREEDOMS

In the summer of 2016, following a joint press conference in which then French minister of the interior Bernard Cazeneuve and his German counterpart Thomas de Maizière called for legislation to "*arm our democracies on the issue of encryption*," the French Digital Council (CNNum) took on the task of addressing the question of encryption. Nearly one year later, and with security still a critical issue, encryption is a key source of friction between personal data protection, technological innovation and surveillance. In a joint statement with British Prime Minister Theresa May, President Macron once again stated his preference for better access to encrypted content "*under conditions which preserve the confidentiality of the correspondence so that these message applications cannot be used as tools for terrorists or criminals.*" The EU is scheduled to examine the relevance of introducing legislation on this matter in the autumn. For the Council, this is an opportunity to spell out its position, and – given worrisome moves to tighten security – to expand the issue to include the protection of rights and freedoms on the Internet.



OPINION OF THE COUNCIL_

The digital revolution has effected thoroughgoing change in our societies, upending our relationship to time, space and other people. The path that this revolution will take is unpredictable: the effect of technologies that both liberate and enslave is always the result of social and political choices. We must ensure that this revolution – which carries with it the promise of profound democratic change – does not ultimately compromise either rights and freedoms or the rule of law.

National security is a vital issue. There is no denying that the new forms of digital-based communication and organisation can make it harder for those tasked with public security to perform their duties. In recent years, terrorism has claimed hundreds of lives in France. In an atmosphere of heightened tension, the authorities appear to be caught in a never-ending spiral where the goal of total security can never be achieved. Everyone knows that there is no such thing as zero risk, and yet there is a strong urge to amass even more means of action, to choose the desire for security over the requirements of the rule of law and our economy. Thus, the Domestic Security and Anti-Terrorism Bill, which is currently being debated in the National Assembly, will be the 15th security-oriented piece of legislation promulgated since 2012. Some of the provisions in these various laws have not yet been implemented. The issue of the effectiveness of this all-pervasive legislation should be addressed, particularly in light of the American experience.

The French Digital Council has regularly stated its position in discussions that pit security against individual and collective freedoms, sometimes artificially. The Council has weighed in on the 2013 Military Planning Act (which allows real-time collection of data by the government without any real control), the Act of 13 November 2014 strengthening anti-terrorism measures (allowing the government to block Internet sites, without prior court supervision), the 2015 Intelligence Act and, most recently, the furious debate over the Secure Electronic Documents file (TES). On each of these occasions, the Council has underscored the need for prior consultation on all of these topics that are as complex as they are important, and which will affect us in the coming years.

In both political discourse and resulting legislation, the Internet is a perfect scapegoat. What is more, it is often used as a testing ground for deploying security measures under ordinary law. Public opinion has more easily accepted digital surveillance, which is generally (and wrongly) considered to be less intrusive than physical surveillance. Once again, the point is not to deny the determining role that digital technology plays in heightening the terrorist threat, but this responsibility is more complex than it appears. Although the web is a propitious venue for indoctrination, in most cases, radicalisation comes through human contact – off-line[1].

[1] "In 95% of cases, the triggering event is human contact" – Anti-Terrorist Coordination Unit.

PREDICTIONS AND CIRCUMVENTION OF JUDICIAL AUTHORITY

The goal of combatting terrorism has led to a host of measures that compound the weakening of the authority of the courts and bolster that of the executive branch. The 2014 Anti-Terrorism Act gives the government the power to block and delist websites without any prior judicial supervision. The 2015 Intelligence Act strengthened this tendency to bypass the courts, paving the way for more widespread intrusive methods outside the control of judges, who are nevertheless the guardians of individual freedoms. In the same way, the Domestic Security and Anti-Terrorism Bill, which was submitted by the current administration, seeks to introduce provisions concerning exceptions into ordinary law, once again undermining the authority of the courts.

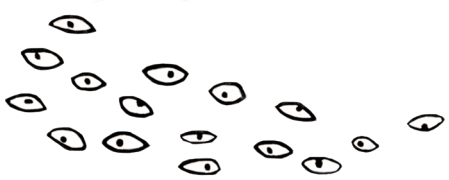
Despite the pressing nature and technical complexity that are inherent to anti-terrorist efforts, the Council would like to restate its commitment to the principle of judicial intervention whenever individual freedom is at stake. Although appearing before a judge provides no watertight guarantee, it amounts to a necessary guarantee: the judge is independent, which is not the case for the government or the intelligence services, which are subject to a hierarchical authority. The judge in a judicial court verifies – *prior* to its being implemented – that a measure is not arbitrary, that it is necessary and commensurate with the objective pursued, and that it respects human rights. While we do not wish to deny the importance of oversight by administrative court judges and their historic role in upholding individual freedoms, it should be pointed out that this oversight comes into play *after* a freedom has been called into question, and presupposes a prior referral to an administrative court, which in practice is quite rare.

In law after law, a mindset of suspicion appears to carry the day. The concept of behaviour is substituted for one of actual activity – in the name of a predictive view of the fight against terrorism, individuals can be detained not because they were preparing to commit crimes or misdemeanours, but simply because they would be likely to do so. This model raises a number of questions.

Surveillance practices have gone from being occasional and targeted to being permanent and widespread. Changes in how technology is used, greater processing capacities and progress in both artificial intelligence and deep learning, combined with ever-lower costs of data storage make it possible to apply predictive models to national security objectives. This move is well-intentioned and appears to make sense. Nevertheless, it raises very specific questions, the first of which concerns reliability. Anyone interested in predictive models will necessarily deal with the particularly thorny issue of defining a detection limit. The "*black boxes*" provided for in the Intelligence Act are a good illustration of this problem. These instruments are intended to anal-

yse networks to pick up "*weak signals*" of terrorist activities, but naturally run into the problem of false positives – errors that automatically result from the process of identifying behaviour that is statistically extremely rare . When it comes to intelligence, false positives can lead to abusive surveillance decided on skewed grounds. Despite amazing leaps forward in artificial intelligence, algorithms for processing data are not exempt from bias, particularly sociological bias. This in turn can contribute to bolstering the discrimination suffered by certain groups of individuals within a population. These dangers, which are beginning to be well-documented, have recently surfaced in public discussions around issues of predictive policing .

In these circumstances, the "*control*" paradigm must change to incorporate these new technological realities. In addition to the vital balance between respect for individuals' privacy and security needs, those with oversight must ensure that surveillance practices do not create discrimination. As part of this, it will likely be necessary to adjust our legal and philosophical notions of the protection of individuals when processing their data. The idea is to factor in these profiling methods which, when used for the purposes of prediction, focus less on the individual than on the statistical group to which he or she belongs. Efforts should be made in terms of the explainability of these algorithms – those with oversight must be able to open the black boxes to ensure they are fair, and to organise democratic feedback and effective legal remedies for individuals. The Council is also considering the issue of stronger criminal sanctions with respect to breaches of private data to uphold privacy. This and the growth in artificial intelligence are set to become critical issues in the near future. The Council will explore these topics more in depth in the coming months.



[2] With respect to this last point, researchers at Inria have alerted the government to the systematic appearance of errors, even in a well-regulated system, which are all the more numerous as the dataset being processed is extremely large. The difficulty resides in reliable identification of behaviour that is statistically quite rare. The researchers gave the following example: Let us assume that we are searching for terrorists within a given population. Every detection algorithm has a margin of error; that is, it will pick out individuals with no terrorist intentions (false positives). If the margin of error is 1%, which is currently considered to be a very low rate, the algorithm will pick out some 600,000 individuals out of a population of 60 million people. If the number of real terrorists is, let us say, 60, then the real terrorists will represent only 0.01% of the population identified (as potential terrorists). Moreover, the algorithm should factor in the idea that the individuals being targeted will attempt to adapt their behaviour to avoid being profiled and to escape detection. The "inherent biases" of predictive policing methods are also a source of discrimination.

ENCRYPTION ON THE FRONT LINE IN THE BATTLE BETWEEN FREEDOM AND SECURITY

In this discussion, data encryption is the embodiment of the tension that pits safety against individual freedoms. Since the revelations of Edward Snowden and the awareness of the scope of government surveillance, digital firms are increasingly turning to encryption solutions.

End-to-end encryption is often offered to users as a default. This means that only users hold the decryption keys, and not even the company supplying the service is able to access their private communications.

The term end-to-end encryption is used when data is encrypted from one end of the communication to the other, i.e. when only the sender and the recipient of the communication hold a key allowing them to decrypt the message. The information is thus theoretically indecipherable by third parties, and particularly by the intermediary that transmits the message. Since it does not hold the decryption key, the company is thus unable to respond to requests from law enforcement to access encrypted data.

Signal, Telegram, WhatsApp – in recent years, there has been an explosion in secure messaging services. Today, they are the focus of scrutiny by law enforcement agencies due to end-to-end encryption. In many countries, including France, public officials have expressed their concern: they worry that they will not be in a position to prevent a terrorist attack or to investigate criminal activities.

The plan presented by Emmanuel Macron and Theresa May aims to “allow access to encrypted content”. It goes on to state that “when encryption technologies are used by criminal groups, and terrorists, it must be possible to access the content of communications”. This statement begs the question: how can one access encrypted content without a key?

One proposal that is regularly tabled by certain politicians in respect of security is to compel manufacturers and providers of services and digital applications to build in backdoors to their systems. Doing so would, however, have drastic consequences for all users. Recent and large-scale cyberattacks are proof of the risks to users’ security when intelligence services voluntarily maintain security flaws for offensive purposes.

A backdoor provides a point of access to an operating system, an application or an online service. These secret entries are generally introduced unbeknownst to the user. An individual with knowledge of a back door can use it to monitor how an application is used, and even take control of it. For both hackers and the intelligence community, the interest lies in the possibility of monitoring users’ activities, copying or destroying data, taking control of a computer, etc.

More generally, weakening the means of encryption – which today are extremely widespread in services for the general public – would doubtless be of limited effectiveness with respect to the extremely tiny minority of users who employ encryption to hide criminal activity. Indeed, it is within the grasp of any criminal organisation to develop opaque applications that are easy to distribute and which provide a very high level of security. Let us be clear: no technique for weakening encryption can be used solely for targeting criminal activities. Restricting encryption for the general public is equivalent to granting a monopoly to organisations that will abuse this power.

It is worth pointing out that data encryption is not an insurmountable barrier for accessing data necessary to investigations. There are a number of ways to get around it, even if it is very robust, by exploiting technical flaws or by directly operating the equipment of the individual in question. Moreover, although content may be encrypted, its related metadata is generally not, in that it is critical to the operation of the system. This metadata is often sufficient to sketch out a network and localise individuals without having to access the content of private communications.

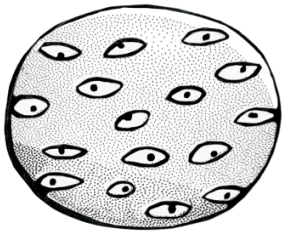
The Council would like to once again state that cooperating with suppliers of secure products and services for the purposes of judicial access to metadata is a possible solution. To do so, the Council recommends bolstering regulations governing judicial cooperation in a bid to reduce delays in supplying this data.

A CRITICAL TOOL FOR OUR ONLINE SECURITY

The Internet has become the pathway for our communications. It is vital to the growth of our societies and our economies. At the same time, however, barely a week goes by without news reports of critical flaws discovered in systems, leaks and large-scale thefts of personal data.

Given the situation, encryption is a critical part of our online security. For citizens, encryption is a major source of trust in the digital world: on a daily basis, it protects the communications and transactions of billions of individuals against increasingly formidable cyber-threats. Encryption is also a tool to foster the privacy that is enshrined in the General Data Protection Regulation. For companies, encryption is the best rampart against economic espionage, and is essential for anyone wishing to protect intangible assets. Finally, for the State, encryption is a sina qua non of sovereignty – the revelations of Edward Snowden provide constant proof of this.

In light of the foregoing, the Council would like to reiterate its support for a large-scale rollout of encryption for the general public, economic stakeholders and government departments.



AS A RESULT,
THE COUNCIL BELIEVES THAT_

Any bill or regulation that has significant implications for individual freedoms must be the subject of a large-scale prior consultation

The principle of court intervention must be reaffirmed whenever a freedom is called into question

The public authorities must set aside the mindset of suspicion, which paves the way for arbitrary treatment, when implementing Internet-related security policies

Encryption is a critical tool for online security – as a result, it must be rolled out on a large scale to citizens, economic stakeholders and government departments

Encryption – and the fundamental freedoms that it protects – are a rampart against the arbitrary power of states. It also protects us against the growing control over our lives exercised by economic stakeholders

Encryption is not an insurmountable barrier to investigations. It can be circumvented as part of a targeted surveillance operation. As such, it is a foil to mass surveillance.

More generally, given the increasing powers exercised by intelligence services and the significant impact that this has on the life of citizens, the Council is interested in the need to establish an effective right to remedy as well as a right to the explainability of predictive algorithms. The Council is also considering the issue of stronger criminal sanctions with respect to breaches of private data to uphold privacy.

www.cnnumerique.fr

Conseil national du numérique
Bâtiment Atrium
5 place des Vins-de-France
75573 Paris Cedex 12
info@cnnumerique.fr - @CNNum
01 53 44 21 27

CONTACT PRESSE
Yann Bonnet, Secrétaire Général
presse@cnnumerique.fr
01 53 44 21 27