CNIL.

CNCTR
COMMISSION NATIONALE DE CONTRÔLE DES TECHNIQUES DE RENSEIGNEMENT

air 2024

LA SURVEILLANCE DANS TOUS SES ÉTATS : QUELLE ÉTHIQUE POUR (PROTÉGER) NOS LIBERTÉS

air

AVENIRS
INNOVATIONS
RÉVOLUTIONS

Air est l'acronyme d'Avenirs, Innovations, Révolutions, trois mots-clés qui forment le nom que la CNIL a donné à la mission éthique qui lui a été confiée par la loi pour une République numérique de 2016. Ses objectifs : explorer les avenirs souhaitables, questionner les innovations qui façonnent notre temps et appréhender les révolutions en cours.

Programme de l'édition 2024

Mardi 19 novembre 2024

ALLOCUTION D'OUVERTURE

par Marie-Laure DENIS, *présidente de la CNIL*

« TOUS SURVEILLANTS, TOUS SURVEILLÉS » : LES ENJEUX DE LA SURVEILLANCE PAR LES PAIRS ET INTERPERSONNELLE

Table ronde animée par Charleyne BIONDI, *chercheure associée au Centre de recherches politiques de Sciences Po (CEVIPOF) et à l'institut Montaigne, auteure de « Dé-coder : une contre-histoire du numérique »*

Olivier AÏM, *maître de conférences Sorbonne Université CELSA, auteur de « Les théories de la surveillance »*

Ariane OLLIER-MALATERRE, *professeure à l'Université du Québec à Montréal et auteure de « Living with Digital Surveillance in China »*

Nathalie TEHIO, *présidente de la Ligue des Droits de l'Homme (LDH)*

Stella MORABITO, *déléguée générale de l'Alliance française des industries du numérique (AFNUM)*

OSINT, LE RENSEIGNEMENT D'ORIGINE SOURCES OUVERTES

par Sébastien BOURDON, *vice-président d'Open Facto et journaliste au Monde*

IA ET CAPITALISME DE SURVEILLANCE

par Shoshana ZUBOFF, *professeure émérite à la Harvard Business School, sociologue*

SURVEILLER POUR PROTÉGER : QUELLE ÉTHIQUE AUJOURD'HUI POUR LES SERVICES DE RENSEIGNEMENT ?

Table ronde animée par Amaelle GUITON, *journaliste à Libération*

Pascal MAILHOS, *coordonnateur national du renseignement et de la lutte contre le terrorisme*

Nicolas LERNER, *directeur général de la Sécurité extérieure*

Christian VIGOUROUX, *conseiller d'État honoraire, président du collège de déontologie de la juridiction administrative*

ALLOCUTION DE CLÔTURE

par Serge LASVIGNES, *président de la Commission nationale de contrôle des techniques de renseignement (CNCTR)*

somm

1 *« Tous surveillants, tous surveillés »*

Les enjeux de la surveillance par les pairs et interpersonnelle

naire

2

Surveiller pour protéger

Quelle éthique aujourd'hui pour les services de renseignement ?

3

Épilogue

Édito

« Il est indispensable de s'interroger sur la capacité de l'individu à jouir de ses droits fondamentaux. »

Marie-Laure Denis,
présidente de la CNIL

La Commission nationale de l'informatique et des libertés (CNIL) et la Commission nationale de contrôle des techniques de renseignement (CNCTR) sont toutes deux nées en réaction à la surveillance d'État. En 1978, un projet de fichier central dénommé SAFARI, devant permettre une surveillance généralisée des citoyens par l'administration, aboutissait à la création de la CNIL. La CNCTR, qui succède à la Commission nationale de contrôle des interceptions de sécurité (CNCIS), prend sa source dans la condamnation de la France, en 1990, par la Cour européenne des droits de l'homme dans deux affaires concernant des interceptions judiciaires.

Mais en 2024, nous avons quitté l'univers du *1984* de George Orwell : *Big Brother* a été rejoint par une multitude de « *little brothers* ». L'État n'a plus le monopole de la surveillance. Celle-ci est désormais exercée par une grande diversité d'acteurs, à de multiples échelles et sous différentes formes, de la collecte de nos traces numériques à des fins commerciales à la surveillance des citoyens entre eux… Ces modes de surveillance s'entrelacent, la surveillance horizontale alimente la surveillance verticale. La massification des données et de leur collecte offre aux États un pouvoir d'intrusion dans nos vies privées sans précédent. En France, ce pouvoir est encadré par la loi du 24 juillet 2015 relative au renseignement et contrôlé par la CNCTR et la CNIL, qui veillent à assurer un équilibre entre la sécurité et la liberté.

Grâce au règlement général de protection des données (RGPD), la CNIL et ses homologues européens veillent à protéger les internautes du ciblage et de l'hyperpersonnalisation des publicités, sur lesquels repose le modèle économique des entreprises du Web, notamment des GAFAM, qui aspirent nos données personnelles et dont les algorithmes analysent nos traces numériques pour influencer nos comportements et nos opinions. Pour continuer à faire évoluer les pratiques, la CNIL met en place, après son plan « cookies » déployé depuis 2019, un nouveau plan d'action sur les applications mobiles.

Portée par les objets connectés et les multiples applications, la surveillance interpersonnelle s'invite dans tous les compartiments de nos vies. Dans le monde du travail : avec le contrôle des travailleurs ou la collecte d'informations sur un futur employé. Dans la sphère familiale avec le contrôle parental, la géolocalisation des enfants, ou la télésurveillance des personnes âgées.
Nos raisons de divulguer nos données personnelles et de renoncer en partie à notre droit à la vie privée sont multiples : la sécurité des citoyens au nom de laquelle s'exerce par exemple la surveillance vidéo de l'espace public, l'efficacité des services rendus par les plateformes qui se nourrissent de nos traces de navigation, ou encore la liberté d'expression qui nous conduit à exprimer publiquement des informations et des opinions, qui pourraient ensuite nous nuire.

Dans cet environnement où nous sommes tous à la fois surveillants et surveillés et dans lequel s'estompent les frontières entre monde physique et monde numérique, il est indispensable de s'interroger sur la capacité de l'individu à jouir de ses droits fondamentaux. Si chacun doit arbitrer entre ce qui relève de la sphère privée et du domaine public, de la visibilité numérique et de la protection des données personnelles, la question de la préservation de nos libertés individuelles à l'ère de la surveillance de masse est l'affaire de tous.

Pour revoir l'intégralité des échanges, rendez-vous sur www.cnil.fr/air2024

« TOUS SURVEILLANTS, TOUS SURVEILLÉS »

Les enjeux de la surveillance par les pairs et interpersonnelle

« Tous surveillants, tous surveillés » : cette formule renvoie à une forme de surveillance dont nous sommes à la fois auteurs et cibles passives.

En 2013, Edward Snowden révélait au monde entier les activités de surveillance massive, systématique et indiscriminée auxquelles se livraient les services de renseignement aux États-Unis et en Europe. La surveillance par l'État était alimentée par l'immense flux de données collectées et traitées par les acteurs du numérique et les géants d'Internet, le plus souvent à l'insu des utilisateurs.

Onze ans plus tard, la perspective a encore changé. Le panoptique a cédé la place aux écrans, qui masquent et révèlent à la fois. L'essor des technologies et des outils numériques, ainsi que la massification des données et de leur traitement par l'IA, nous ont fait passer de la surveillance de la masse par quelques-uns à la surveillance de tous par tous. *Big Brother* a cédé la place à « *Big Other* ». Chacun est à la fois l'objet et le sujet de la surveillance, le regardé et le regardeur. La surveillance n'est plus un abus de pouvoir mais bien la forme même de nos existences connectées.
Nos données personnelles sont le prix que nous payons pour notre visibilité numérique, notre existence sur les réseaux sociaux, nos usages des plateformes, des applications, des objets connectés. Mesurons-nous bien le prix à payer ?

À quoi sommes-nous prêts à renoncer pour rejoindre la société de la surveillance ?

Regards croisés

Régis Chatellier

Chargé des études prospectives au sein du laboratoire d'innovation numérique de la CNIL (LINC)

Charleyne Biondi

Politologue et auteure de *Dé-coder - une contre-histoire du numérique* aux éditions Bouquins

« La généralisation des technologies numériques signe bien l'entrée dans une nouvelle ère de la surveillance. »

En quoi sommes-nous dans une nouvelle ère de la surveillance ?

Régis Chatellier : Ce qui est nouveau, c'est la forme multidirectionnelle prise par la surveillance. Depuis les années 2000, l'essor des outils numériques a provoqué le développement de la surveillance par les pairs, aux côtés de la surveillance des populations par les États, ou des particuliers par des acteurs privés. Ainsi, nous pouvons tous désormais être à la fois surveillés et surveillants.

Charleyne Biondi : La surveillance aujourd'hui ne se limite plus à une logique fonctionnelle de contrôle ou de gestion des populations. Elle s'inscrit dans une transformation épistémique plus large, où le numérique structure notre rapport au monde. La surveillance n'est plus seulement une pratique visant à contrôler ou orienter des comportements, elle est devenue une forme d'organisation symbolique et structurelle de nos sociétés. La généralisation des outils de surveillance à l'âge des GAFAM nous a en quelque sorte sortis du dilemme moral entre surveillance (ou sécurité) et liberté, pour nous faire entrer dans une logique où la collecte et l'analyse de données - la surveillance, donc, est désormais la principale source de production des savoirs et des richesses. C'est un tournant épistémologique essentiel.

Nos vies numériques encouragent-elles la surveillance ?

CB : En traduisant le monde en données, en quantifiant le réel et en le mettant en réseau, le numérique rend tout quantifiable, enregistrable, diffusable. Tous les jours, nous constatons à quel point la technologie organise nos vies individuelles et collectives, et combien elle rythme et ordonne le monde. Nous sommes la matière première nécessaire de cette transformation numérique, et nous en avons parfaitement conscience. Le numérique a fait émerger une forme de culture de la surveillance qui redéfinit la notion de l'intime et fait disparaître l'idée d'une frontière nette et inviolable entre le public et le privé.

RC : Le numérique facilite la surveillance. Nos pratiques, consciemment ou non, nous conduisent à des formes de surveillance. Au-delà de l'exposition de soi sur les réseaux sociaux, il existe une forme de surveillance « *by design* », incorporée aux outils. En indiquant si un message a été reçu et lu, ou si un utilisateur a quitté ou rejoint un groupe, des applications de messagerie créent des microformes de surveillance. Le simple usage de ces applications constitue un regard sur l'autre. Par ailleurs de nombreux outils numériques viennent répondre à des peurs anciennes : c'est le cas des « parents hélicoptères » qui disposent désormais d'outils leur permettant de savoir à tout moment où se trouvent leurs enfants. Dans une très large mesure, les pratiques de surveillance interpersonnelle échappent au cadre règlementaire : le RGPD « ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques ». Ces pratiques peuvent cependant tomber sous le coup de la loi quand elles relèvent du harcèlement ou sont détournées à des fins malveillantes. Mais elles doivent nous interroger. Une connexion permanente avec ses proches est-elle une bonne habitude ? Où commence l'ingérence ? Quelle est notre capacité à accepter l'incertitude ? Comment arbitrer entre les inquiétudes des parents et le droit des adolescents à la liberté et à l'intimité ?

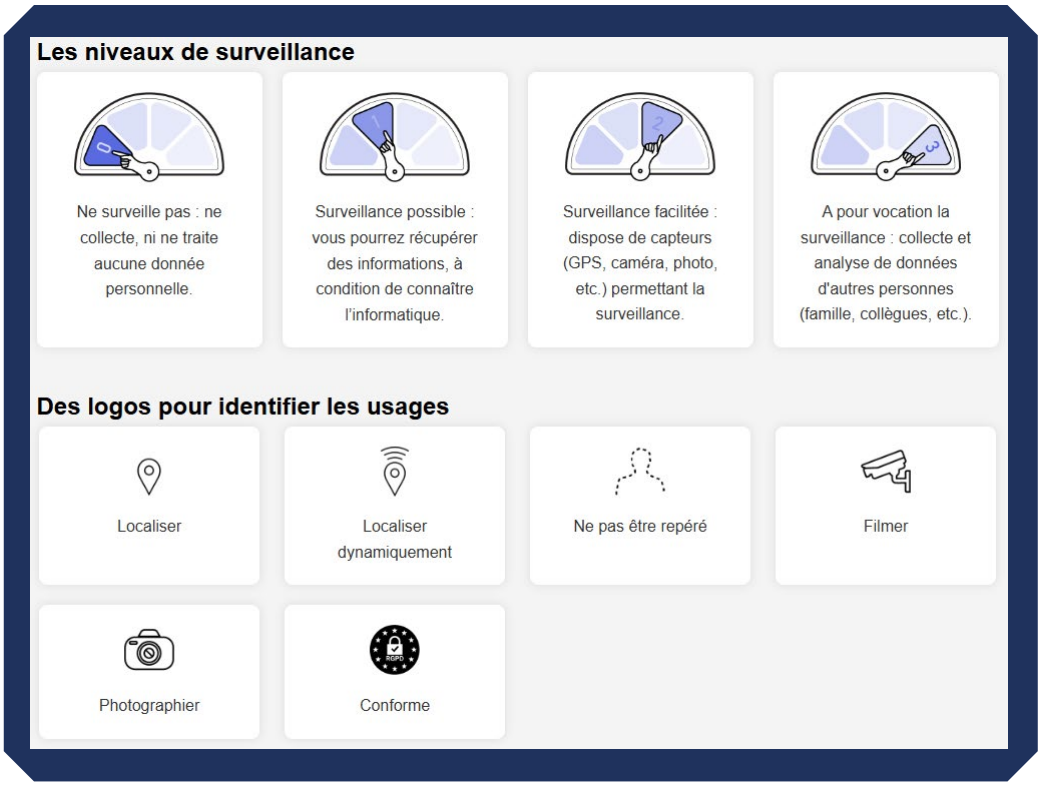
Peut-on aujourd'hui échapper à la surveillance ?

RC : Dans nos grandes villes, il n'est plus possible de sortir dans la rue sans être filmé par une caméra. Il n'est pas non plus possible d'utiliser un service numérique sans partager de données. Mais de même que des dispositions juridiques encadrent la vidéosurveillance, le partage de données avec un service numérique doit faire l'objet d'une relation contractuelle claire et respecter les textes. Chacun doit être attentif aux traces qu'il consent à laisser. Les usages sociaux du numérique font partie de notre vie : nous arbitrons constamment entre notre désir de protection et notre désir de connexion. Une enquête récente du LINC et du pôle d'éducation au numérique de la CNIL montre que les adolescents prennent aujourd'hui mieux en compte les risques liés au partage de contenus en ligne que leurs aînés. Nous sommes tous en train d'apprendre. Peut-être qu'en même temps que l'on cherche à savoir si on peut échapper à la surveillance, il nous faut aussi nous demander si nous acceptons de ne pas savoir.

CB : La surveillance est inhérente à la numérisation des sociétés ; mais, paradoxalement, la quantité de données collectés assure une forme relative d'anonymisation. L'intelligence surveillancielle des GAFAM, par exemple, s'intéresse davantage à l'agrégation de nos données qu'à ce qu'elles révèlent de nos identités, elle porte sur nos échantillons de nos comportements, pas sur nos individualités. On est donc dans une logique d'influence très différente des fictions de « La vie des autres » sous la Stasi, ou de la dystopie d'Orwell où la surveillance visait le contrôle des subjectivités. Il n'en reste pas moins que cette implosion-reconfiguration permanente de nos doubles numériques n'est pas anodine : que reste-t-il de la démocratie quand son plus essentiel fondement - l'idée d'un individu-sujet - est remis en question par la logique (surveillancielle) dominante du temps présent ?

Le surveillanscore

À la manière du nutriscore, ce design fiction du LINC informe, et interroge, sur le potentiel de surveillance intégré à un objet ou service numérique.



www.surveillanscore.fr

Débat

Tous surveillants, tous surveillés : les enjeux de la surveillance par les pairs et interpersonnelle

Imaginez : en signalant aux autorités, vidéo à l'appui, que je ne plaçais pas mes déchets alimentaires dans le bon bac de tri, mon voisin a obtenu des points de crédit social, qui lui permettent d'être considéré comme un bon citoyen et d'attendre moins longtemps à l'hôpital ou à la mairie.

Fiction ? En Chine, les citoyens qui informent la police peuvent, dans certaines municipalités, se voir faciliter l'accès à l'école ou au logement. Mais chez nous aussi, en France, des collectifs de voisins ou de citoyens vigilants surveillent les allées et venues tandis que des parents suivent leurs enfants par géolocalisation. L'ère de la surveillance de tous par tous est-elle une menace pour nos droits et libertés ou une promesse de richesse, de service et de sécurité ?

Big Brother est-il chinois ? La puissance technologique entre les mains d'un État autoritaire : cette combinaison fait de la Chine l'objet de nos fantasmes sécuritaires. Les données individuelles collectées par des acteurs numériques au service du pouvoir central y détermineraient l'accès au logement, à l'éducation et à l'emploi, avec un système de crédit social récompensant les bons comportements et sanctionnant les mauvais. *« Il s'agit largement d'une légende. Il existe bien des plateformes intégrées qui regroupent réseaux sociaux, sites d'achat en ligne, systèmes de paiement, services de téléphonie, de réservation, etc. On trouve aussi des systèmes de récompense et de «* social shaming *», c'est-à-dire d'ostracisation publique de « mauvais citoyens », et un recours massif à la reconnaissance faciale et à la vidéosurveillance, mais il n'y a pas de système unifié de notation de chaque citoyen. En fait, la Chine dispose même d'une réglementation similaire au RGPD, la PIPL (pour Personal information protection law) qui encadre la sécurité et le traitement des données par les entreprises »* tempère Ariane Ollier-Malaterre, titulaire de la Chaire de recherche du Canada sur la régulation du numérique dans la vie professionnelle et personnelle à l'Université du Québec à Montréal (UQAM).

Un fardeau émotionnel

Dans son ouvrage, *Living with Digital Surveillance in China*, l'universitaire s'attache à comprendre en quoi consiste la surveillance en Chine, mais aussi à en mesurer le poids sur les citoyens. *« Lorsqu'on les interroge, ceux-ci ont tendance à défendre le système de surveillance dont ils font l'objet, évoquant un État paternaliste soucieux de leur bien-être et du progrès moral ou encore la fierté liée à la maîtrise technologique. Mais lorsqu'on les questionne sur leur ressenti, ils font alors état de frustration, de colère, de peur. Si le discours rationnel justifie la surveillance, celle-ci représente un fardeau émotionnel qu'on doit interroger »*, souligne la chercheuse.

Sommes-nous si éloignés de l'Empire du Milieu ? N'exerçons-nous pas aussi une forme de surveillance latérale constante sur les réseaux sociaux, en scrutant les publications en ligne d'un collègue ou d'une connaissance, ou encore en analysant le temps d'écran de nos enfants ?

Ariane Ollier-Malaterre

Professeure à l'Université du Québec à Montréal (UQAM) et auteure de *Living with Digital Surveillance in China. Citizen's Narratives on Technology, Governance and Privacy.*

« 3 000 ans de surveillance en Chine ont abouti à une normalisation de celle-ci. De nombreux citoyens se sont habitués à une surveillance centralisée associée à une surveillance à l'échelle du quartier ou de l'immeuble. Mais cette acceptation dans le discours s'accompagne d'un coût émotionnel très lourd. »

Stella Morabito

Déléguée générale de l'Alliance française des industries du numérique (AFNUM)

« Les dispositifs de contrôle parental ou de géolocalisation des enfants sont des formes de surveillance bienveillante, visant à protéger avant qu'à restreindre. Mais est-ce aux parents ou au législateur de déterminer où situer le curseur du bien ? »

Au nom du bien

Et si avec le contrôle parental, *Big Mother* et *Big Father* s'étaient substitués à *Big Brother* ? Depuis le 13 juillet 2024, la loi Studer impose aux constructeurs d'intégrer un système de contrôle parental aux appareils électroniques connectés. En légiférant, l'État fixe un cadre et rappelle aux parents leur devoir de surveillance. Pour Stella Morabito, déléguée générale de l'Alliance française des industries du numérique (AFNUM), l'enjeu de santé publique légitime l'action du législateur. « *Encadrer vaut mieux qu'interdire* » souligne-t-elle, évoquant l'annonce par le premier ministre australien d'interdire l'accès aux réseaux sociaux aux mineurs de moins de 16 ans. *« Le contrôle parental relève d'une surveillance bienveillante, qui vise à protéger les plus vulnérables. Pour être efficace, il doit s'exercer dans la concertation avec l'enfant et ne pas être simplement imposé »* précise-t-elle.

Pouvoir et contre-pouvoir

« Les bonnes intentions peuvent constituer de potentielles menaces » objecte Nathalie Tehio, présidente de la Ligue des droits de l'Homme. Pour elle, la surveillance latérale entre en collision avec l'État de droit. Elle invoque les exemples de « voisins vigilants » s'inquiétant des fréquentations de leurs riverains, avec des biais racistes, et, sur la côte d'Opale, la constitution de groupes de chasseurs s'investissant d'une mission de surveillance et de dénonciation des migrants…

« On assiste à une forme de maillage de la surveillance de tous par tous. Ainsi, par exemple, la loi contre le séparatisme, avec son « contrat d'engagement républicain », impose désormais aux associations de contrôler leurs membres et leurs bénévoles sous peine de sanctions financières. C'est une atteinte à la fois à la liberté d'expression et à la liberté d'association » déplore l'avocate, qui y voit une forme d'organisation de la censure, un instrument de musèlement des associations par les autorités publiques. Selon elle, les outils numériques peuvent permettre l'exercice d'un contre-pouvoir lorsque les manifestants filment les actions des forces de l'ordre. Mais ils, viennent surtout s'inscrire dans ce continuum de la surveillance, comme un instrument de pouvoir, lorsque les forces de l'ordre utilisent ces mêmes outils pour identifier les individus. *« L'ambivalence des outils n'empêche pas une forme de technosolutionnisme qui préfère multiplier les caméras plutôt que les patrouilles, alors même que les bénéfices de ces dispositifs restent à évaluer »* note la présidente de la Ligue des droits de l'Homme, qui redoute aussi une délégation de la surveillance par l'État aux acteurs privés : le recours aux vigiles, notamment à l'occasion des Jeux olympiques et paralympiques de Paris, ou dans les transports, aux salariés d'une entreprise privée et non au service du public. *« Ces transferts de compétences sont inquiétants et contreviennent à l'article 12 de la Déclaration des droits de l'Homme et du Citoyen de 1789, qui prévoit le recours à une force publique »* dénonce-t-elle.

De gauche à droite : Charleyn Olivier Aïm.

Nathalie Tehio

Présidente de la Ligue des droits de l'Homme (LDH)

« La montée en puissance de la surveillance n'est pas le seul fait du numérique, même si celui-ci favorise une forme d'habitude et de consentement à la surveillance. »

e Biondi, Ariane Ollier-Malaterre, Nathalie Tehio, Stella Morabito,

Tous vigilants ?

Olivier Aïm, qui enseigne la théorie des médias et la philosophie de la communication au CELSA, relève également l'extension et la normalisation des pratiques de surveillance. Pour l'auteur des *Théories de la surveillance, du panoptique aux Surveillance studies*, la population est aujourd'hui disposée à contribuer à l'effort de surveillance, elle adhère au mot d'ordre de la RATP appelant à la vigilance « attentifs ensemble » : *« La population revendique son droit à prendre part à " l' économie de la visibilité " dont parlait Michel Foucault. Nous avons tous incorporé des pratiques de la surveillance. Celle-ci est devenue participative. Derrière mon écran, je monitore, je* check, *je* stalk, *je* screen *pour suivre les flux d'informations et constituer, le cas échéant, des preuves, des dossiers. La surveillance est devenue une part essentielle de la culture numérique ».*

Stella Morabito abonde dans ce sens : *« Avec le numérique, la surveillance devient attrayante : elle facilite les démarches quotidiennes, avec l'administration ou pour faire ses courses, et bénéficie de la personnalisation, de l'efficacité, de la gratuité et de la simplification rendues possibles par le numérique. Les réseaux sociaux nous proposent de nous mettre en valeur, les objets connectés nous aident à évaluer notre santé, nos performances sportives, notre temps de sommeil, et à partager ces informations ».*
Au risque qu'elles tombent entre de mauvaises mains.

Olivier Aïm

Maître de conférences au CELSA, Sorbonne Université et auteur de *Les théories de la surveillance, du panoptique aux Surveillance studies*.

« Nous avons basculé dans une culture de la surveillance dans laquelle tous souhaitent prendre part à cette nouvelle économie de la visibilité. »

OSINT

Les sources ouvertes : une mine d'informations

Sébastien Bourdon, vice président d'*Open Facto* et journaliste au *Monde*.

Des failles de sécurité au plus haut niveau

En 2018, le *New York Times* fait sensation avec un article expliquant comment la publication sur la plateforme Strava de leurs parcours de footing avait conduit des militaires américains à dévoiler l'existence de bases secrètes en Afghanistan. Sébastien Bourdon, vice-président d'OpenFacto et journaliste au *Monde* a décidé d'utiliser cette faille pour tester la sécurité du président Emmanuel Macron. Dans la série d'articles qu'il co-signe avec Antoine Schirer, il détaille comment, grâce à Strava, il est parvenu à anticiper les déplacements présidentiels.

« À partir des segments de courses laissés dans des lieux stratégiques, tels un départ et un retour depuis l'Élysée ou un parcours dans les jardins de la Lanterne, la résidence d'État du président français, nous avons pu repérer sur Strava une douzaine de membres du GSPR, le groupe chargé de la protection du chef de l'État » raconte Sébastien Bourdon. Une fois ces hommes identifiés, il devenait possible de suivre leurs déplacements, partout où ils couraient. Les journalistes sont ainsi parvenus, uniquement avec ces traces de footing, à identifier les hôtels destinés à accueillir le président lors de ses déplacements, les hommes du GSPR s'y rendant souvent quelques jours plus tôt pour sécuriser les lieux. *« À dix reprises, nous avons ainsi pu découvrir les lieux de séjour du Président avant ses déplacements et obtenir* a posteriori *la confirmation de nos déductions »* précise Sébastien Bourdon qui ajoute avoir facilement découvert, à partir de leurs profils publics sur Strava, les noms et lieux de résidence de certains agents du GSPR. Avec Antoine Schirer, il a reproduit l'exercice sur les gardes du corps de Joe Biden et Vladimir Poutine. Résultat similaire : les journalistes ont identifié 26 agents du Secret Service américain, et, grâce aux traces Strava de 6 membres du FSO, suivi celles du président russe, y compris jusqu'à un palais de la mer Noire qu'il nie posséder.

« Alors que cela fait six ans qu'on connaît l'existence de cette faille de sécurité, elle n'est toujours pas corrigée. Pourtant, deux clics suffisent pour passer son profil en privé, sur Strava, comme sur les autres plateformes. Cela témoigne, pour certains services, ou au moins pour certains agents, d'une véritable méconnaissance des risques numériques » déplore Sébastien Bourdon.

Contactée par les journalistes du *Monde*, l'Élysée continue de minimiser ces risques, estimant que les conséquences de l'utilisation de Strava par des membres du GSPR « sont très faibles et n'ont en aucun cas des impacts sur la sécurité du président de la République ».

Entrevue

Entretien avec Shoshana ZUBOFF

Sociologue, professeure émérite à la Harvard Business School, auteure de L'âge du capitalisme de surveillance.

Que recouvre l'expression « capitalisme de surveillance » ?

J'ai étudié pendant des années l'informatisation progressive de l'environnement professionnel. Autour des années 2000, j'ai réalisé que nous assistions à une numérisation du monde : nous sommes tous devenus des informations numériques. Le capitalisme de la surveillance est né de la volonté de Google, en particulier, de monétariser ces données. Il s'agit de collecter nos traces numériques, nos engagements, nos interactions, nos clics pour se les approprier, les analyser, les transformer en outils de prédiction de nos comportements futurs, et de vendre cette ressource. Un tour de passe-passe qui a conduit à une augmentation de 3 590 % des revenus de Google entre 2001 et 2004 ! Google s'est approprié nos données à notre insu. Il s'agit d'une stratégie volontaire et assumée de dissimulation. Le capitalisme de surveillance trouve donc son origine dans ce qui s'apparente à un vol : prendre quelque chose à quelqu'un, sans son accord et à son insu, afin de l'utiliser à ses propres fins.

Cette exploitation de nos données se limite-t-elle à la publicité ciblée ?

Le trésor que représentent nos signaux comportementaux est convoité dans tous les aspects de notre vie. Le capitalisme de surveillance s'étend à tous les domaines. Aujourd'hui, les automobiles sont conçues comme des dispositifs mobiles de surveillance, les capteurs se généralisent partout, analysant et communiquant sur tous nos comportements : notre activité physique, nos fréquentations, notre temps de sommeil, nos déplacements ou nos consommations. Tous les pans de notre société sont victimes de cette captation de nos signaux comportementaux, avec des conséquences terribles.

Quelles sont ces conséquences ?

La première est la perte de la vie privée. Celle-ci, telle que nous pouvions la connaître il y a vingt ans, n'existe tout simplement plus. La seconde est la corruption de l'information. Les systèmes d'information sont conçus par les GAFAM pour maximiser les volumes et les vitesses de transmission au détriment des contenus. Il faut du clic, de l'attention. Cela conduit à des contenus décorrélés de la réalité, les fameuses fake-news. Aujourd'hui aux États-Unis, la modération de tels contenus est perçue comme de la censure. Selon la Food and Drug Administration, ce droit à la désinformation est désormais la première cause de décès. Enfin la troisième conséquence désastreuse du capitalisme de la surveillance est la concentration, non seulement du pouvoir économique, mais aussi de la connaissance et de sa distribution, aux mains d'une oligarchie aux intérêts commerciaux. Avec le numérique, nous avions la possibilité d'un véritable âge d'or de la connaissance. Internet et l'intelligence artificielle pouvaient être mis au service du bien commun : aider à mieux soigner, mieux éduquer, améliorer l'hygiène, la santé ou la sécurité. Au lieu de ça, Internet est devenu une prison, sans barreaux, mais sous haute surveillance, sans possibilité d'évasion, dans laquelle les contenus les plus outranciers et les plus polarisants sont les plus valorisés.

Quelles sont les solutions ? Une meilleure régulation ?

Il n'est pas trop tard pour que nous nous réapproprions nos données. Les droits des travailleurs ont été obtenus au prix de combats en réponse à la révolution industrielle. L'Europe avec le RGPD, et la Chine avec son PIPL, ont montré la voie à suivre. Les législateurs américains, qui ont été défaillants, doivent suivre ces exemples.

Mais, alors que nous commençons à mesurer les dégâts causés par le capitalisme de surveillance, nous devons oser nous demander si la régulation est suffisante. Celle-ci représente toujours un compromis : comme s'il s'agissait de donner un cadre au vol des données personnelles à des fins commerciales. Je propose de désigner ce vol pour ce qu'il est : un crime. Je veux prononcer le mot « abolition ». C'est le seul terme approprié face à une activité catastrophique pour nos démocraties, inacceptable moralement et politiquement. Comme on a su le faire face au travail des enfants ou à l'esclavage, il est temps de commencer à refermer la fenêtre de la régulation. Aucune démocratie ne peut résister au capitalisme de la surveillance. Nous n'en voulons pas, nous n'en voulons plus. Abolition.

Shoshana Zuboff en direct de New-York lors de l'événement Air2024.

SURVEILLER POUR PROTÉGER

Quelle éthique aujourd'hui pour les services de renseignement ?

Quelles sont les règles quand on agit hors des cadres ?
Les agents des services de renseignement sont, en particulier lorsqu'ils interviennent à l'étranger, parfois amenés à enfreindre la loi. Quand il s'agit de recruter une source, d'intercepter une communication, de suivre un suspect, d'infiltrer une organisation, de mener une opération clandestine sur le sol étranger, quelles sont les limites ? Qui les fixe ? Que se passe-t-il lorsqu'elles sont franchies ? Comment, en France, le droit, les procédures et la déontologie s'articulent-ils pour contrôler les services de renseignement ?

Débat

Qui surveille ceux qui nous protègent ?

De gauche à droite : Amaelle Guiton, Pascal Mailhos, Nicolas Lerner et Christian Vigouroux

La nécessité de contrôler les activités des services de renseignement français est née de la condamnation de la France par la Cour européenne des droits de l'homme (CEDH) dans deux affaires d'interception des communications réalisées à des fins judiciaires. En réponse le législateur a adopté la loi du 10 juillet 1991 relative au secret des correspondances et créé la Commission nationale de contrôle des interceptions de sécurité (CNCIS) à laquelle la CNCTR a succédé. La mission de la CNCTR : exercer une action continue de contrôle sur l'utilisation des techniques de renseignement en veillant au respect des dispositions fixées la loi relative au renseignement du 24 juillet 2015.

Un cadre juridique

Cette loi donne un cadre juridique aux opérations d'écoute et d'interception des communications en précisant, dans le Livre VIII du Code de la sécurité intérieure les conditions dans lesquelles elles peuvent être autorisées. *« L'article L801-1 de ce Code donne une définition positive de l'action des services de renseignement : celle-ci doit procéder d'une autorité compétente, résulter d'une procédure conforme, respecter les missions confiées aux services et enfin être justifiée par une menace »* résume Christian Vigouroux, qui rappelle que ce sont les services de renseignement eux-mêmes qui ont poussé à l'adoption de lois encadrant leurs pratiques : *« la loi protège l'institution et ceux qui la servent. Légiférer sur les services les renforce »*.

Christian Vigouroux

Conseiller d'État honoraire, président du collège de déontologie de la juridiction administrative.

« Nous avons basculé dans une culture de la surveillance dans laquelle tous souhaitent prendre part à cette nouvelle économie de la visibilité. »

Nicolas Lerner

Directeur général de la Sécurité extérieure et ancien directeur général de la Sécurité intérieure.

« Nos valeurs nous guident et fixent les limites de nos actions.»

Contrôler les services

La CNCTR exerce un contrôle préalable à la mise en œuvre des techniques de renseignements mais aussi un contrôle a posteriori. Elle agit comme un tiers de confiance, informant le Parlement et le public sans révéler les méthodes opérationnelles des services qu'elle contrôle. En 2023, les avis défavorables de la CNCTR représentaient un taux de 1,2 % du nombre total de demandes. Un chiffre qui témoigne des efforts accomplis par les services de renseignement pour se conformer aux exigences qu'impose le cadre légal en matière de techniques de renseignement, et d'une volonté de progrès. *« À l'issue d'échanges avec la coordination nationale du renseignement et de la lutte contre le terrorisme, les directions des services de renseignement et la présidence de la république, la CNCTR va bientôt pouvoir accéder à distance, depuis ses propres locaux, à l'ensemble des données issues de la technique du Recueil de données informatiques (RDI) mises en œuvre par les services de renseignement. La conservation de ces données sera centralisée par le Groupement interministériel de contrôle (GIC) »* annonce Pascal Mailhos, coordonnateur national du renseignement et de la lutte contre le terrorisme, qui se réjouit de ces évolutions.

Même s'il opère dans l'ombre, le renseignement est un service d'État qui n'échappe ni à la loi ni au contrôle. Un contrôle à la fois externe et interne, que détaille Nicolas Lerner : CNCTR, CNIL, parlementaires, inspection des services de renseignement (ISR), Cour des comptes, juge pénal, inspections et audits internes veillent au grain… *« Nous consacrons d'importants moyens à la satisfaction des autorités de contrôle, avec un dialogue constant sur leur étendue et leurs modalités. Au moins 5 % de notre personnel est affecté à des missions de contrôle »* révèle Nicolas Lerner, directeur général de la sécurité extérieure.

Déontologie interne

Le contrôle interne repose sur des procédures mais aussi des valeurs. Nicolas Lerner reconnaît que les activités d'espionnage conduisent, par définition, à s'affranchir des lois des pays dans lesquelles elles se déroulent. *« La DGSE conduit les actions que lui prescrit le gouvernement. Mais nous nous posons des questions. Pour chaque opération nous évaluons l'intérêt, le risque, les moyens et la conformité à nos valeurs et principes : la loyauté, l'exigence, la discrétion et l'adaptabilité. Nous disposons d'un déontologue et d'un code de déontologie propres aux services ainsi que de procédures de concertation pour toutes les décisions : nul ne peut décider seul, il faut gravir une dizaine d'échelons pour passer d'une intention opérationnelle à sa mise en œuvre. Ce processus de décision est lourd, mais il garantit la qualité du travail et le respect des exigences démocratiques ».*

Pour Christian Vigouroux, la déontologie professionnelle des services de renseignement est construite sur trois échelons : celui du droit, celui de la déontologie commune à tout agent public qui impose probité, impartialité et efficacité, et enfin celui des règles propres à la profession. *« Le médecin s'attache au soin,* primum non nocere. *Le professeur d'école au respect des enfants, le policier à un usage proportionné de la force, les agents de renseignement à la loyauté et à la discrétion… »* explique le conseiller d'État honoraire.

« Les contraintes et le contrôle qui pèsent sur leurs services de renseignement font l'honneur des démocraties. »

Pascal Mailhos

Coordonnateur national du renseignement
et de la lutte contre le terrorisme

La responsabilité des agents

Depuis 2022 la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) a la responsabilité, avec l'appui d'une quinzaine de conseillers, d'harmoniser les pratiques de recrutement et de gestion de carrières des services de renseignement. Pour Pascal Mailhos, *« le garant de l'intégrité des services de renseignement c'est leur matière humaine, ce sont les 20 000 hommes et femmes qui font la richesse du renseignement et qui tous, pour leur habilitation, ont fait la démonstration de leur non-vulnérabilité et de leur équilibre personnel. Le contrôle des services de renseignement, c'est leur assurance vie ».*

Sur la place publique

Certaines affaires font la une des journaux, se retrouvent devant les tribunaux. *« Une part significative de ces affaires sont initiées par les services eux-mêmes. Nous sommes intransigeants à chaque fois que nous constatons une dérive individuelle ou un mésusage des moyens de l'État. À quelque niveau que ce soit, le dévoiement de nos principes n'est pas acceptable »* martèle Nicolas Lerner.

Le droit européen continue de faire bouger les lignes. Plus d'une douzaine de requêtes contre la loi du 24 juillet 2015 introduites par des avocats et des journalistes sont en cours d'examen par la Cour européenne des droits de l'homme. Elles portent notamment sur une règle régissant les relations entre services de renseignement, la règle du tiers service : un service de renseignement qui a reçu une information d'un service étranger ne peut la communiquer à un service tiers sans l'accord du service émetteur. Cette disposition rend impossible le contrôle de ces informations. Alors qu'il existe une jurisprudence au travers deux arrêts rendus par la CEDH le 25 mai 2021 (Big Brother Watch et autres c. Royaume-Uni et Centrum för rättvisa c. Suède), la Cour estimant que le partage d'information entre services de renseignements étranger devait être encadré par des règles et soumis à un contrôle indépendant.

La CNCTR estime qu'une évolution du cadre légal français est inévitable. *« Lorsque la CEDH aura rendu sa décision sur les affaires françaises pour lesquelles elle a été saisie, nous entendons bien respecter ses décisions et la jurisprudence »* relève le coordonnateur national du renseignement et de la lutte contre le terrorisme [NDLR : postérieurement au colloque, la Cour européenne des droits de l'homme (CEDH) a rendu le 16/01/2025 une décision déclarant irrecevables ces requêtes mais retient le caractère effectif du dispositif de recours incluant la CNCTR et le Conseil d'État mis en place par la loi française[1]].

2023
Chiffres clés

94 902 demandes de techniques de renseignement présentées à la CNCTR par les services de renseignement (+ 6 % par rapport à 2022).

24 209 personnes ont été surveillées par ces techniques (+ 15 % par rapport à 2022).

Le nombre d'avis défavorables a concerné 1,2 % des demandes (-20 % par rapport à 2022).

136 contrôles sur pièces et sur place ont été réalisés, ce qui représente le plus grand nombre de contrôles *a posteriori* réalisés depuis la création de la CNCTR.

1 D. CEDH, n°49526/15 et autres, Association confraternelle de la presse judiciaire contre la France et autres, 16/01/2025

Entrevue

3 questions à Nicolas Lerner

Directeur général de la Sécurité extérieure et ancien directeur général de la Sécurité intérieure.

En quoi le contrôle des services de renseignement est-il une bonne chose, pour les services comme pour la démocratie ?

L'émergence du renseignement en tant que politique publique, marquée par différentes étapes (livre blanc de 2008, loi renseignement de 2015 et ses suites, publication de la Stratégie nationale du renseignement en 2019), a permis aux services de sortir de l'ombre. C'est une bonne chose, même si cette mise en lumière est également due à des évènements plus tragiques (otages, prégnance de la menace terroriste, bouleversements géopolitiques majeurs…). Comme toute politique publique, le renseignement doit être contrôlé.

Dans un système démocratique tel que le nôtre, le contrôle des services de renseignement, interne et externe, est à bien des égards la condition nécessaire à leur activité car elle conditionne leur acceptabilité. Les services de renseignement se voient reconnaître par la loi des prérogatives exorbitantes du droit commun (techniques de renseignement, constitution de fichiers…) et il est donc nécessaire qu'ils soient contrôlés afin de rendre tout abus inenvisageable et de créer un climat de confiance.

J'ajouterais que l'existence d'un cadre légal, dont le corollaire est le contrôle, était une demande pressante des membres des services de renseignement eux-mêmes. D'une part, parce qu'il les protège - qui accepterait d'agir, et donc parfois prendre des risques, sur ordre, sans avoir la garantie que ses actions sont couvertes par la loi ? - et, d'autre part, parce qu'il constitue un ensemble de garde-fous qui garantissent l'ancrage démocratique de nos services. À la DGSE, ce contrôle interne fait intervenir des entités dédiées (service juridique, inspection…) et a impliqué la mise en place de processus de formation et de conformité auxquels nos agents sont formés.

Il est donc faux d'affirmer, comme on l'entend parfois, que les services seraient par nature réticents à tout contrôle. Le temps du « vivons heureux, vivons cachés » est bel et bien derrière nous. Bien sûr ces contrôles ne doivent pas nous amener à brider nos ambitions opérationnelles, au risque de nous empêcher d'accomplir nos missions, essentielles pour la sécurité de la nation et la défense de notre souveraineté. Ils doivent être proportionnés et accompagner les évolutions technologiques. Pour permettre cela, c'est aux services de savoir créer un climat de confiance et faire œuvre de pédagogie vis-à-vis de leurs contrôleurs comme de l'échelon politique. J'estime que nous avons atteint en France un juste équilibre entre l'efficacité du contrôle et la préservation des marges opérationnelles des services de renseignement.

La montée en puissance de la menace cyber, demande-t-elle des évolutions législatives ou règlementaires ou les dispositifs d'encadrement en vigueur sont-ils adaptés ?

On note effectivement une augmentation du nombre d'opérations informatiques de déstabilisation, à visée d'influence et de sabotage, mais également à but lucratif (attaques par rançongiciel). Dans le cadre de l'accroissement des tensions internationales, des attaquants étatiques qui ont la capacité de se prépositionner sur des réseaux critiques (énergie, transport, logistique, télécommunications) pourraient être amenés à conduire des actions de sabotage. En France, les actions de déstabilisation ont principalement pris la forme d'attaques par déni de service (DDoS) conduites par des groupes d'hacktivistes très réactifs à l'actualité. Si elles ont principalement des conséquences médiatiques et réputationnelles, certaines attaques par DDoS de grande ampleur peuvent perturber significativement les réseaux de télécommunications.

Face à cette montée en puissance, la France a progressivement renforcé ses moyens de prévention, de détection et d'analyse des cyberattaques, sous l'autorité de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui est l'autorité nationale en matière de cybersécurité et de cyberdéfense. Les services de renseignement ont évidemment un rôle à jouer en matière de détection et d'analyse des différentes cyberattaques et c'est la raison pour laquelle nous avons proposé une extension de la technique de renseignement dite de l'algorithme à la détection des menaces pour la défense nationale, parmi lesquelles les cyberattaques.

Cette possibilité a été ouverte par la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France, à titre expérimental pour une durée de quatre ans. Il nous revient désormais de la mettre en œuvre, ce qui suppose d'identifier et de modéliser des comportements correspondant à des cyberattaques, de les appliquer aux données sur lesquels la technique peut être mise en œuvre et de traiter les alertes générées par le dispositif. Nous nous y attelons et fournirons au Parlement des rapports d'étape et d'évaluation, afin que les représentants de la Nation puissent juger de l'utilité et de la proportionnalité de ce nouveau dispositif de détection de la menace cyber.

Comment s'assurer que le respect de l'éthique et des principes démocratiques ne constitue pas un handicap face à un ennemi qui s'en affranchit volontiers ?

Durant la guerre froide, le combat était âpre, mais il y avait néanmoins un certain nombre d'usages qui étaient respectés, y compris au niveau des services de renseignement. Nous vivons désormais dans un monde où un grand nombre d'acteurs s'affranchissent en effet des règles qui ont longtemps prévalu dans la compétition internationale. Plusieurs tabous, comme l'emploi de la force militaire et l'équilibre nucléaire, ont sauté. Cette brutalité s'exprime également sous le seuil des conflits armés. L'une de ses manifestations les plus visibles a trait aux manipulations de l'information, qui produisent des dommages sérieux dans nos sociétés démocratiques, non seulement en promouvant les positions de tel ou tel acteur, mais aussi en semant la discorde à l'intérieur de nos sociétés, jusqu'à nous faire douter de la pertinence de notre propre modèle.

Face à ces agressions, le premier écueil serait de nier la réalité et de refuser de voir la portée du phénomène : nous n'en sommes plus là. Le second serait de se résoudre à une certaine impuissance. Le troisième, peut-être le plus terrible, serait d'adopter les méthodes de nos compétiteurs non démocratiques, au risque de nous perdre en nous éloignant de nos valeurs. Or, notre rôle est de défendre la pérennité de notre modèle démocratique, « le pire des systèmes à l'exclusion de tous les autres », qui reste fort envié dans le monde. Je crois qu'une autre voie, qui permet l'action ciblée et proportionnée, dans le respect de nos valeurs, existe.

Il s'agit de ne pas se laisser imposer des narratifs mensongers et donc d'avoir la capacité de détecter, de dénoncer et d'attribuer ces attaques, et de riposter le cas échéant. L'État s'est par exemple organisé en structurant un écosystème qui gagne chaque jour en maturité. VIGINUM, créé en 2021, est ainsi chargé de détecter et de caractériser tout phénomène de propagation suspecte de contenus mensongers ou hostiles sur les plateformes numériques, impliquant des acteurs étrangers, dans le but de nuire à la France et à ses intérêts. La DGSE lui apporte son concours grâce notamment à ses capacités d'expertises techniques. Mais nos adversaires affinent leur arsenal de désinformation, et délaissent les procédés les plus grossiers, comme les myriades de faux comptes automatisés, pour se tourner vers des techniques plus subtiles.

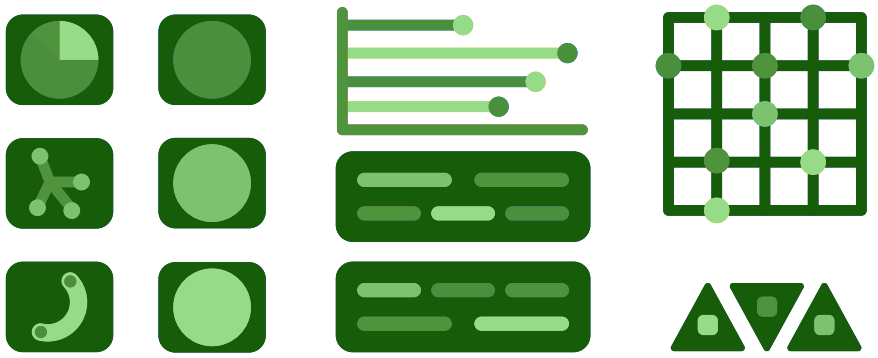
Par ailleurs, une fois que le mal est fait, c'est-à-dire une fois qu'une « infox » a largement circulé, il est très difficile d'en limiter les effets. Il est donc extrêmement difficile de lutter contre un mensonge lorsqu'il s'est déjà répandu. La seule solution, c'est d'agir le plus en amont possible. Si le renseignement a alors un rôle à jouer, d'autres secteurs tels que l'éducation aux médias, la montée en puissance du *fact-checking* par une presse libre, le maintien de mécanismes de modération puissants sur les réseaux sociaux, tout cela encadré par une législation sur laquelle l'Europe est en pointe, sont essentiels.

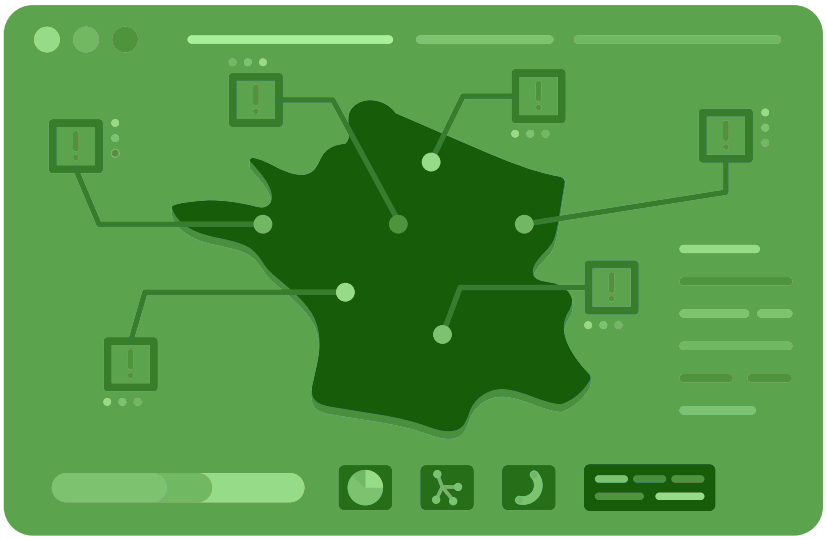
Focus

Les algorithmes au service du renseignement

L'utilisation de caméras de surveillance augmentées, couplée à un dispositif automatisé d'analyse des images en temps réel, fait actuellement l'objet d'une expérimentation, amorcée avec les JOP2024 et qui court jusqu'au 31 mars 2025. Si cette expérimentation, qui n'intéresse pas particulièrement le renseignement administratif, repose en partie sur des algorithmes, l'utilisation de ces « traitements automatisés » par les services de renseignement fait l'objet d'un encadrement spécifique.

Ainsi, la loi du 24 juillet 2015 relative au renseignement, a autorisé, à titre expérimental, le recours à cette technique dite de l'algorithme, qui consiste en un traitement automatisé des données de connexion et de navigation sur Internet, avec la coopération des fournisseurs d'accès. Cette loi a été complétée par plusieurs textes pour tenir compte de l'évolution des technologies. Ainsi, la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement a pérennisé la technique de l'algorithme et l'a étendue aux adresses (URL) de connexion.





Par ailleurs, à titre expérimental et jusqu'au 30 juin 2028, la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France élargit le recours à ces traitements automatisés, au-delà des menaces terroristes, pour détecter des connexions susceptibles de révéler des ingérences étrangères ou des menaces pour la défense nationale.

La CNCTR exerce un contrôle préalable sur l'ensemble de ces techniques de renseignement sur le territoire national et indique, dans son rapport d'activité 2023, avoir autorisé les services à recourir à la technique de l'algorithme à cinq reprises depuis 2015.

Dans son avis de 2021 sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, la CNIL relevait que le recours aux techniques de traitement algorithmique « *porte une atteinte particulièrement forte à la vie privée des individus et au droit à la protection des données à caractère personnel, puisqu'elle ne présente pas de caractère ciblé mais procède de l'analyse de l'ensemble des données de connexion de la population* ».

ÉPILOGUE

Serge Lasvignes : l'éternel retour de la surveillance

Serge Lasvignes

Président de la Commission nationale de contrôle des techniques de renseignement (CNCTR)

La culture de la surveillance n'est pas née avec les technologies numériques et n'est pas réservée aux services de renseignement. Dans le village ariégeois d'où je viens, du temps de mes grands-parents, une partie importante de l'activité sociale consistait à surveiller ses voisins. Aujourd'hui sommes-nous plus ou moins avides de surveillance que nos ancêtres ?

Une culture de la surveillance

Avec les outils numériques, nous sommes tous à la fois des surveillants et des surveillés. La métropole anonyme est redevenue un village. Nous sommes tous voisins. Nous avons tous désormais la possibilité de filmer nos proches, de géolocaliser nos enfants, de lire ce que postent nos collègues sur les réseaux sociaux…

Interrogeons-nous sur nos usages des technologies de surveillance. Le contrôle parental doit-il être laissé au seul arbitrage des parents ? Je suis encore ému quand ma voiture m'appelle par mon prénom, sans forcément me demander ce que ça entraîne. J'ai été amusé de voir s'afficher ma photo sur un écran géant quand j'ai traversé hors des clous lors d'un séjour en Chine. Mais est-ce amusant ? La réglementation parvient-elle à réguler ces nouveaux usages ? Quand l'État en appelle à la vigilance citoyenne, articule sa surveillance sur celle exercée par des citoyens, des dérives sont possibles, des précautions sont nécessaires. Lorsque nos sociétés démocratiques libérales font le choix de mobiliser pour leur sécurité des organisations autres que l'État, quel risque faisons-nous peser sur l'État de droit ?

Le rempart de la loi

Paradoxalement, les services de renseignement font partie des organismes les plus contrôlés pour leur utilisation des technologies de surveillance : les interceptions de communication, aussi anciennes que le téléphone, s'étendent désormais aux données de connexion, aux données informatiques, aux communications électroniques… La loi du 24 juillet 2015 fixe un cadre légal pour l'usage de ces techniques. Celui-ci repose sur trois piliers.

Premier pilier : on ne peut utiliser les techniques de renseignement que si les « intérêts fondamentaux de la nation » sont en cause. La loi définit de manière exhaustive ces intérêts : se protéger contre les ingérences étrangères, défendre et promouvoir les intérêts de l'économie et de la recherche françaises, prévenir les actes terroristes et les violences collectives, la délinquance et la criminalité organisées.
Deuxième pilier : la loi fixe également, de manière exhaustive, la liste des techniques légalement utilisables – accès aux données de connexion, interceptions téléphoniques, géolocalisation en temps réel, sonorisation de locaux ou de véhicules, captation d'images, recueil de données informatiques, recours à un algorithme…
Troisième pilier : la loi soumet donc le recours aux techniques de renseignement à un double contrôle. Celui du Premier ministre, et selon la technique employée, à l'accord du ministre sous l'autorité duquel le service de renseignement est placé.

La décision du Premier ministre est précédée de l'avis d'une autorité indépendante :
la Commission nationale de contrôle des techniques de renseignement (CNCTR). Ses avis ont jusqu'à présent toujours été suivis lorsqu'ils étaient défavorables.

Un large contrôle

Mais ce cadre légal a des limites : il ne concerne que ce qui se passe sur le territoire national. Les opérations menées à l'étranger, notamment par la DGSE, n'entrent pas dans le champ du contrôle et relèvent de l'éthique des services. La loi de 2015 ne régit pas l'ensemble des activités de renseignement mais le seul usage de certaines techniques. Pour autant, les services de renseignement n'échappent pas à d'autres contrôles : la CNIL veille à la protection des données personnelles, la délégation parlementaire au renseignement (DPR), commune aux deux assemblées, évalue l'ensemble de la politique du renseignement, la Commission de vérification des fonds spéciaux (CVFS) examine la bonne utilisation des crédits… Ceux qui nous surveillent sont très surveillés.

Ce contrôle doit être dynamique. De nouvelles menaces doivent pouvoir conduire à l'adoption de nouveaux outils. Il faut pouvoir enrichir les moyens techniques des services mais sans jamais renoncer à la protection de la vie privée. La capacité de contrôle et de régulation doit rester en phase avec le développement de nouvelles capacités de surveillance telles que le recours à l'intelligence artificielle pour le traitement des données, notamment biométriques.

S'interroger sur l'éthique du renseignement ne revient pas à opposer liberté et sécurité. La défense de la démocratie ne peut aujourd'hui se passer du renseignement, et d'un renseignement efficace. Son contrôle en est le garant.

Mais le contrôle depuis l'extérieur, pour indispensable qu'il soit, ne suffit pas. Il est également nécessaire que les services de renseignement s'interrogent en interne, sur l'usage des techniques dont ils disposent, s'approprient le cadre dans lequel ils agissent, non seulement du point de vue de la stricte légalité, mais aussi des implications de la vie dans une société démocratique. Cette forme d'acculturation doit les conduire à définir plus qu'une simple déontologie professionnelle : une véritable éthique du service.

Serge Lasvignes lors de son discours de clôture.

Hommage à Serge Lasvignes

C'est avec une profonde tristesse que les membres et agents de la CNIL ont appris le décès de Serge Lasvignes, survenu le 15 février 2025. Éminent serviteur de l'État, il a occupé des fonctions de premier plan, notamment en tant que Secrétaire général du gouvernement de 2006 à 2015, puis Président du Centre Pompidou de 2015 à 2021.

Depuis 2021 et jusqu'à récemment, Serge Lasvignes présidait la Commission nationale de contrôle des techniques de renseignement (CNCTR). Son engagement sans faille visait à concilier sécurité et libertés, tout en protégeant les droits fondamentaux des citoyens.

Le 19 novembre 2024, lors du colloque co-organisé par la CNIL et la CNCTR, intitulé « La surveillance dans tous ses états : Quelle éthique pour protéger nos libertés ? », il avait brillamment conclu les travaux en mettant en lumière les enjeux complexes de la surveillance dans nos sociétés modernes. Son intervention avait soulevé des questions éthiques cruciales sur l'équilibre entre sécurité et liberté dans les démocraties.

Les membres et agents de la CNIL tiennent à saluer sa mémoire et adressent leurs plus sincères condoléances à sa famille, ses proches et ses collaborateurs.

A

Lexique

Z

Cookie

Petit fichier informatique stocké par un serveur sur le terminal d'un utilisateur et lu par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile afin, par exemple de mémoriser son identifiant ou son panier ou encore de tracer sa navigation à des fins statistiques ou publicitaires.

GAFAM

Instruction rédigée en langage naturel - et non en code info matique - qui sert à commander les IA génératives.

OSINT (open source intelligence) ou ROSO *(renseignement d'origine source ouverte)*

Renseignement obtenu par le croisement et l'analyse de données en accès libre.

Patriot Act

Loi antiterroriste adoptée aux États-Unis à la suite des attentats du 11 septembre 2001, renforçant fortement le pouvoir des agences de renseignement, notamment en les autorisant à exploiter massivement les données issues de surveillance électronique.

RGPD

Le règlement général sur la protection des données, entré en application le 25 mai 2018 encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Services spécialisés du renseignement

(nommés également services du premier cercle)

DGSE : Direction générale de la sécurité extérieure
DGSI : Direction générale de la sécurité intérieure
DNRED : Direction nationale du renseignement et des enquêtes douanières
DRM : Direction du renseignement militaire
DRSD : Direction du renseignement et de la sécurité de la défense
TRACFIN : Service du traitement du renseignement et de l'action contre les circuits financiers clandestins

Surveillance studies

Champs d'étude pluridisciplinaire consacré à la surveillance née au début des années 2000 (son réseau international, le Surveillance Studies Network voit le jour en 2006).

Commission nationale de
l'informatique et des libertés
3 place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
Tél. 01 53 73 22 22

www.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS