Sécurité et numérique

François Pellegrini

Sécurité et numérique – Entre fantasmes d'efficacité et violations avérées des droits fondamentaux

François Pellegrini

Université de Bordeaux, LaBRI & Inria Bordeaux - Sud-Ouest, 351 cours de la Libération, 33405 Talence cedex, France

{francois.pellegrini@labri.fr}

L'ouverture des espaces numériques a naturellement conduit à l'extension de la problématique sécuritaire en leur sein. Cette extension possède deux versants. Le premier concerne la sécurité des outils numériques proprement dits, ainsi que des conditions de leur usage, regroupés sous le terme générique de « cybersécurité ». Avec la numérisation croissante des sociétés modernes, la cybersécurité représente un enjeu majeur en termes économiques, de souveraineté mais également de protection des biens et des personnes, du fait des possibilités accrues de perturber à distance le fonctionnement de dispositifs critiques (1). Le second versant concerne l'usage spécifique des outils numériques pour la mise en œuvre des politiques sécuritaires. Ces outils incluent les moyens de surveillance ciblée ou de masse, dans un but de contrôle des individus mais aussi potentiellement de populations entières (2). Les risques majeurs inhérents à cette dernière catégorie d'outils doivent amener à s'interroger sur leur proportionnalité, ainsi que sur les garde-fous techniques qui doivent être mis en place lors de la constitution de grands fichiers des populations, les garde-fous juridiques étant inopérants face à un responsable de traitement devenu malveillant (3).

1 Numérique et sûreté

1.1 La sécurité des systèmes d'information

Les problématiques cyber-sécuritaires ne sont pas récentes puisque, dès le 6 janvier 1978, la loi « informatique et libertés » disposait que : « Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage [...] à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés »[1]. Cependant, le non-respect de ces obligations ne pouvait conduire qu'à sanctionner le responsable de traitement lui-même, pour ses négligences. C'est avec la loi « Godfrain » de janvier 1988 qu'a été effectivement mis en place un volet répressif vis-à-vis des auteurs d'infractions informatiques telles que l'intrusion au sein d'un système de traitement automatisé de données (STAD), la perturbation du fonctionnement d'un tel système, ou encore « le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient »[2].
Il est à noter que, jusqu'à sa modification par une loi de novembre 2014 « renforçant les dispositions relatives à la lutte contre le terrorisme », l'article 323-3 du code pénal ne sanctionnait pas l'extraction, la détention, la reproduction ou la transmission frauduleuses de données. Ceci à conduit les juridictions répressives à prendre de grandes libertés avec la loi pénale, censée être d'interprétation stricte, pour sanctionner l'extraction de données d'un STAD. L'artifice, employé *contra legem*, a consisté à qualifier celle-ci de « vol », ce qui est absurde du fait que l'information est un bien informationnel non rival[3].

1 Ces dispositions, initialement présentes dans l'article 29 de la loi, n'ont été amendées qu'à la marge, au sein de l'article 34 de la loi actuellement en vigueur : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »
2 Article 323-3 du code pénal, créé par la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique. Voir : https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000875419&pageCourante=00231 .
3 Il ne faut pas confondre l'information et son support. Ainsi le violon et la musique que l'on en tire sont-ils régis par deux droits radicalement différents, même si la seconde ne peut exister sans le premier. Assimiler l'information à l'électricité est donc erroné. L'électricité peut effectivement être volée, car la puissance électrique consommée est un bien rival : la même puissance électrique ne peut alimenter à la fois deux équipements, et trop en consommer fait « sauter les plombs ». Son coût marginal est non nul, car lié à la quantité d'énergie primaire (charbon, uranium, masses d'eau issues de barrages, etc.) à injecter dans les centrales pour la produire. Poursuivre une personne ayant extrait des informations, au motif du vol du support de données ayant servi à cette extraction, est donc peu opérant, car le coût unitaire d'une feuille de papier ou d'une clé USB ne peut conduire à considérer que le préjudice qui en a résulté serait significatif en tant que tel. Voir par exemple : François PELLEGRINI, « La portabilité des données et des services », RFAP, 2018, à paraître.

À l'image de la sécurité dans le monde physique, mais plus encore du fait de la rareté des compétences techniques nécessaires, la cyber-sécurité nécessite l'implication de tous les tiers susceptibles d'y apporter leur concours, ne serait-ce qu'en alertant les responsables et/ou les autorités quant à l'existence de failles exploitables. Ce n'est que depuis l'entrée en vigueur de l'article L. 2321-4 du code de la défense, créé par l'article 47 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, qu'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information (ANSSI) une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données, n'est pas susceptible de poursuites. Cette exonération de poursuites était pourtant demandée depuis de nombreuses années par la communauté de la sécurité informatique. Face à la complexité toujours croissante des systèmes informatiques, seule la protection effective et certaine de ces personnes contre la mise en œuvre de mesures répressives (et non la seule inapplication discrétionnaire des peines) est à même d'éviter l'auto-censure et de permettre la mobilisation de l'intelligence collective ainsi que la détection et le renforcement des talents.

1.2 La loyauté de la cryptographie

La cryptographie est un domaine technologique essentiel au fonctionnement de la société numérique. Elle structure l'ensemble de l'infrastructure informationnelle publique et privée. C'est grâce à elle que le réseau public Internet peut être utilisé par chacun pour y faire transiter les communications relatives à ses activités domestiques et professionnelles, tant pour garantir la confidentialité des échanges que l'authentification des interlocuteurs[4]. La préservation de la société numérique impose donc la loyauté absolue des briques cryptographiques.

Or, sous la pression sécuritaire, certains gouvernements ont pu être tentés d'obliger les acteurs à insérer des « portes dérobées » dans les protocoles et logiciels cryptographiques. Il s'agit généralement de faire en sorte que le concepteur du logiciel de chiffrement dispose d'une « clé maître » permettant d'affaiblir la robustesse des échanges[5], mais la vulnérabilité peut également concerner l'algorithme proprement dit[6]. L'histoire de la puce cryptographique à clé maître Clipper, conçue dans les années 1980 dans le cadre d'un projet gouvernemental étasunien[7], l'a déjà démontré : personne n'investira jamais dans un système déloyal, d'autant qu'il est extrêmement facile de mettre en œuvre ses propres outils cryptographiques exempts de vulnérabilités connues. Une telle obligation ne pourrait donc conduire qu'à l'affaiblissement global de la sécurité en cas de découverte de la porte dérobée par des tiers, comme ce fut d'ailleurs également le cas pour le dispositif Clipper.

Les tentatives des gouvernements d'obtenir, pour les services de police, des accès quasiment instantanés à des masses considérables d'informations, pose la question de la surveillance globale. Si ces services doivent bien évidemment disposer des moyens les plus perfectionnés afin de pouvoir surveiller de façon ciblée les personnes réputées dangereuses, il n'est aucunement souhaitable de faciliter la surveillance automatisée de masse de l'ensemble de la population.

2 La surveillance par les outils numériques

2.1 La massification de la collecte des traces

La généralisation des outils numériques conduit à une explosion des traces numériques produites par les personnes. Ces témoignages numériques de l'activité des personnes, constitutives de leurs identités numériques, appartiennent à trois grandes catégories : ce que les personnes déclarent d'elles-mêmes, ce qu'elles montrent d'elles-mêmes, et ce que l'on peut en déduire. Nombre de ces traces ont été produites de façon incidente (comme par exemple les données de géo-localisation que les ordiphones peuvent attacher aux photos prises), sans action explicite des personnes, et constituent des « informations qui sont plus abandonnées que cédées, des traces laissées et non des données transmises »[8].

Les forces de l'ordre ont très vite utilisé ces gisements de données dans le cadre de leurs enquêtes. Avant l'âge des réseaux, il s'agissait principalement de collectes *a posteriori*, par le biais de réquisitions auprès des divers responsables de traitement (banques, relevés mensuels d'opérateurs téléphoniques, etc.). La généralisation des réseaux numériques et l'augmentation de leurs performances a progressivement permis la captation des informations au vol, quasiment en temps réel par rapport à leur génération. Parce que plusieurs de ces méthodes de captation nécessitent le concours actif des opérateurs de réseaux numériques, la loi a organisé leur collaboration effective. En particulier, l'article 5 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement a

4 Le coût rédhibitoire des liaisons privées restreint leur usage à quelques acteurs étatiques ou commerciaux. Cependant, du fait que ces liaisons empruntent également le domaine public, le chiffrement des échanges au sein de « réseaux virtuels privés » (VPN) constitue la plus élémentaire des prudences.

5 La clé maître est alors utilisée pour chiffrer les clés des usagers avant de les envoyer intégrées au corps des messages échangés. Ainsi, l'autorité disposant de la clé maître et interceptant ces messages est en théorie la seule à pouvoir obtenir la clé des usagers, permettant de déchiffrer leurs messages.

6 Kim ZETTER, « How a Crypto 'Backdoor' Pitted the Tech World Against the NSA », Wired, 24 septembre 2013, https://www.wired.com/2013/09/nsa-backdoor/ .

7 Wikipedia, article « Clipper chip », https://fr.wikipedia.org/wiki/Clipper_chip, consulté le 20 juin 2018.

8 Antoinette ROUVROY et Thomas BERNS, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », Réseaux 2013/1 (n° 177), pp. 163-196, DOI 10.3917/res.177.0163 .

ajouté au code de la sécurité intérieure (CSI) un florilège de dispositions légales permettant d'obtenir ces informations, légalisant parfois a posteriori des pratiques existantes.
Il en est ainsi notamment de la communication par les opérateurs des données ayant transité par les réseaux de communication (L. 851-1 CSI), de la communication en temps réel par les opérateurs des données transitant sur les réseaux (L. 851-2 CSI), de la communication en temps réel par l'opérateur de la géo-localisation des terminaux (L. 851-4 CSI), de la mise en œuvre d'un dispositif d'interrogation de l'équipement destiné à obtenir ses caractéristiques et sa géo-localisation (L. 851-6 CSI). Les moyens directement mis en œuvre par les autorités sont également concernés, tels que de la mise en œuvre de balises autonomes de géo-localisation (L. 851-5 CSI) ou d'espiongiciels (706-102-1 CPP). Ces derniers permettent d'intercepter les interactions d'une personne avec son équipement, telles que, notamment, les frappes au clavier ou les données affichées à l'écran. Ces mécanismes de captation (appelés génériquement « keylogging », en anglais) visent à contourner la cryptographie de bout en bout éventuellement utilisée par les personnes au moyen d'applications telles que les messageries chiffrées (de type « Telegram »), en captant les informations saisies au clavier avant leur chiffrement, et celles affichées à l'écran après leur déchiffrement.
D'autres dispositifs ainsi légalisés appartiennent au domaine bien plus problématique des outils permettant la mise en œuvre d'une surveillance de masse. Il en est ainsi des dispositifs de leurrage et d'interception de téléphonie mobile, dits « *IMSI catchers* » (L. 852-1 CPI). Ces « imposteurs de réseaux[9] », transportables dans une mallette, simulent le fonctionnement d'une borne de réseau téléphonique mobile, à laquelle sont invités à se connecter tous les équipements personnels des alentours. Les « IMSI catchers » mettent donc en œuvre une surveillance indiscriminée des communications téléphoniques dans leur périmètre de fonctionnement, méconnaissant la protection que la loi apporte à certaines catégories de personnes (avocats, journalistes, etc.) ; en effet, les communications sans rapport avec l'enquête sont détruites « dès qu'il apparaît qu'elles sont sans lien avec l'autorisation délivrée », c'est-à-dire après avoir été écoutées. Cet usage indiscriminé est d'autant plus dommageable que, lors de l'élaboration de la loi, un amendement avait été proposé afin que ces équipements ne captent que les conversations de numéros déterminés. Les travaux parlementaires montrent au contraire que le gouvernement de l'époque a délibérément refusé l'ensemble des garde-fous ayant pu permettre une utilisation ciblée du dispositif, au motif de découvrir des téléphones utilisés par des personnes sans que la ligne soit à leur nom[1011] ; un filtre basé sur la reconnaissance biométrique vocale pour les communications audio, et des mots-clés pour les SMS, serait pourtant à même d'apporter un service équivalent sans écoute humaine. L'interception des communications peut également être mise en œuvre au sein des antennes-relais elles-mêmes, pour obtenir en temps réel une copie de leur trafic de données. L'usage d'une surveillance indiscriminée « de zone » est donc pleinement acté.
La surveillance de masse à l'échelle du pays entier a pour sa part été légalisée par les dispositions relatives aux analyseurs automatiques de trafic internet, pudiquement appelés « boîtes noires » (L. 851-3 CPI), mais dont le principe de fonctionnement relève de l'analyse comportementale de l'ensemble des internautes. Nulle évaluation de l'effectivité de ces dispositifs n'a été effectuée.
La collecte de masse des informations de trafic est, en France, relativement ancienne, puisque c'est la loi n° 2001-1062 du 15 novembre 2001 « relative à la sécurité quotidienne » qui, au sein de l'article L. 32-3-1 du code des postes et communications électroniques, impose aux opérateurs de télécommunications de conserver pendant un an l'intégralité des données de connexion de leurs abonnés. Cette pratique fut généralisée à l'ensemble des États-membres de l'Union européenne par la directive 2006/24/CE[12], avant que cette dernière ne soit invalidée par la CJUE le 8 avril 2014 au motif que la collecte systématique et indiscriminée des traces des personnes n'était pas proportionnée[13]. En dépit de l'arrêt « Tele 2 » de la CJUE du 21 décembre 2016[14], qui confirme cette interprétation, rien n'a été fait en France pour limiter l'usage des données ainsi recueillies, le gouvernement ayant au contraire défendu devant la CJUE la nécessité de cette collecte généralisée, au nom de la toujours opportune et serviable « lutte contre le terrorisme »[15].

9 Contrairement à ce que leur nom laisse supposer, ces équipements ne servent pas qu'à intercepter les numéro des abonnés (dits numéros « IMSI », pour « *International Mobile Subscriber Identity* » se trouvant à portée de l'équipement, mais bien l'ensemble des flux de données transitant entre les équipements mobiles et celui-ci : contenu des communications, des SMS, etc. Voir : Marc REES, « Réforme pénale : la petite farce de l'IMSI catcher », NextINpact, 31 mars 2016, https://www.nextinpact.com/news/99292-reforme-penale-petite-farce-imsi-catcher.htm .
10 Voir le compte-rendu intégral des débats du 3 juin 2015 relatifs à l'amendement n° 24 rectifié du sénateur Claude MALHURET, http://www.senat.fr/seances/s201506/s20150603/s20150603017.html#amd_2014_461_24_rect_1 .
11 Guerric PONCET, « Loi renseignement : après le 7 janvier, "nous sommes prêts à tout accepter" », Le Point, 4 juin 2015, http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/loi-renseignement-apres-le-7-janvier-nous-sommes-prets-a-tout-accepter-03-06-2015-1933306_506.php .
12 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE
13 Arrêt de la cour (grande chambre), affaires jointes C-293/12 et C-594/12, du 8 avril 2014, « Digital Rights Ireland Ltd », C-293/12 et C-594/12, EU :C :2014 :238
14 Arrêt de la cour (grande chambre), affaires jointes C-203/15 et C-698/15, 21 décembre 2016, http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492 .
15 Marc REES, « Le gouvernement défend le Privacy Shield et la conservation généralisée des données », NextINpact, 28 février 2018, https://www.nextinpact.com/news/106063-le-gouvernement-francais-defend-privacy-

2.2 L’extension du fichage de la population

On distingue deux grandes catégories de fichiers : les fichiers administratifs et les fichiers de police. Ces deux catégories ont toujours fait l’objet d’un encadrement différencié. Les fichiers de police sont considérés comme plus intrusifs, car ils contiennent des informations plus détaillées sur les personnes, leur passé, leurs habitudes. Ils visent essentiellement à faciliter la détection et la punition accélérées de la récidive.

2.2.1 Des fichiers administratifs dopés à la biométrie

En France, on constate depuis les années 1980 une pression continue de l’administration en faveur de l’intensification du fichage des personnes. La numérisation croissante de l’administration s’accompagne de la constitution de fichiers administratifs de plus en plus riches, cernant de plus en plus d’aspects de la vie des personnes. Ces fichiers font l’objet d’une interconnexion croissante, au motif de la simplification des procédures pour l’usager. Parallèlement, leur exploitation dans le cadre d’enquêtes de police est rendue de plus en plus simple.

Tel est le cas du fichier TES (« Titres électroniques sécurisés »), le fichier administratif des détenteurs de titres d’identité. Initialement destiné à stocker les informations relatives aux passeports, il a été par la suite étendu aux cartes d’identité. Au prétexte de « sécuriser leur délivrance » et « faciliter leur renouvellement », ce fichier a été transformé en un fichier biométrique centralisé de l’intégralité de la population française, contenant à la fois les photographies et les empreintes digitales des personnes. Les risques pour la population sont considérables. En effet, la biométrie n’est pas révocable : en cas de compromission des informations biométriques liées à une personne, aucune remédiation n’est possible.

La biométrie a deux usages : l’authentification et l’identification. L’authentification vise à déterminer si une personne est bien celle qu’elle prétend être. Pour cela, on compare les données biométriques de la personne avec celles qui ont été préalablement collectées de façon contrôlée auprès de la personne ayant cette identité. Si les données correspondent, la personne est bien celle ayant cette identité, aux faux positifs près ; sinon, aux faux négatifs près, c’est une autre personne, ayant une autre identité, sans que l’on puisse connaître laquelle. L’identification, pour sa part, vise à retrouver l’identité associée à une trace biométrique que l’on possède, qu’elle ait été collectée sur une scène de crime ou qu’elle ait été prélevée sur un cadavre inconnu ou une personne amnésique. On va alors comparer ladite trace avec l’ensemble des données biométriques contenues dans une base de référence, centralisée, dans l’espoir de trouver une correspondance. Si une telle correspondance est trouvée, l’identité de la personne ayant laissé la trace est révélée ; sinon, c’est que ladite personne n’est pas présente dans le fichier.

De fait, seule la fonctionnalité d’authentification est nécessaire à la mise en œuvre des passeports biométriques. Lors d’un contrôle aux frontières, la personne présente au dispositif de contrôle son passeport, qui contient, sur une puce électronique incorporée audit document, le gabarit biométrique calculé lors de la fabrication de celui-ci. Ce gabarit est comparé à l’empreinte des doigts de la personne et permet de déterminer, avec une probabilité plus ou moins forte selon le degré de spécificité de la méthode de comparaison, si la personne qui se présente est bien la titulaire du document.

Le Conseil constitutionnel avait censuré la loi de mars 2012 relative « à la protection de l’identité », qui visait à mettre en place une base centralisée des identités biométriques, au motif que le projet de loi prévoyait que cette base pourrait servir à l’identification des personnes. Il n’a cependant pas censuré le décret créant le fichier TES[16], au motif que les dispositions de l’article 4 dudit décret ne mentionnent pas la finalité d’identification. En prétendant ignorer que toute base centralisée peut être détournée et que le pouvoir qui interdit peut être remplacé à brève échéance par un pouvoir qui autorise, comme l’histoire l’a déjà prouvé[17], il n’a pas joué son rôle protecteur des libertés.

2.2.2 Des fichiers de police en nombre et volume croissants

Le même phénomène inflationniste s’observe pour les fichiers de police, dont le nombre a explosé depuis une vingtaine d’années. Outre l’effet psychologique des attentats du World Trade Center de 2001, on peut avancer comme explication le changement du mode de contrôle de la création de ces fichiers par la CNIL. En effet, depuis 2004, les avis de cette dernière ne sont plus conformes mais seulement consultatifs, ce qui a conduit à ce que ses réserves soient ignorées dans certains cas.

Le fichier emblématique de cette dérive est le FNAEG (« Fichier national automatisé des empreintes génétiques »). Ce fichier, créé en 1998[18], avait pour finalités de faciliter l’identification et la recherche des auteurs d’infractions à l’aide de leur profil génétique, et de personnes disparues à l’aide du profil génétique de leurs descendants ou ascendants. Au cours du temps, son périmètre a été successivement étendu aux principaux crimes d’atteintes aux personnes et aux biens et aux délits tels que vol, tag, arrachage d’OGM, etc. L’inclusion de simples suspects fut rendue possible, ainsi que la facilitation de son utilisation dans les enquêtes. En 2015, le FNAEG contenait près de 5 % de la population, soit 3 006 991 profils génétiques, répartis comme suit : 472 505

shield-et-conservation-generalisee-donnees.htm .

16 Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d’un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d’identité, voir : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345 .

17 Sebastian HAFFNER, *Histoire d’un allemand - souvenirs 1914–1933*, Actes Sud, coll. Babel, 2004.

18 Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu’à la protection des mineurs, voir : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000556901 .

personnes condamnées (16 % du total), 2 280 448 personnes mises en cause (76 %) et 254 038 traces de personnes inconnues. Les réserves du Conseil constitutionnel et de la CEDH quant à la taille et aux usages du fichier n'ont pas conduit à la remise en cause de ces pratiques. Bien au contraire, dans le cadre d'une affaire particulièrement sordide[19], les modalités d'usage du fichier furent étendues en 2011, sans aucun cadre juridique, à la « recherche en parentèle directe en aveugle »[20]. À la différence de l'usage traditionnel d'un tel fichier, qui consiste à savoir si une personne correspondant à la trace recueillie est présente ou non dans le fichier (mode appelé « *hit* / *no hit* »), la recherche en parentèle directe en aveugle vise à déterminer si la personne à l'origine de la trace est un ascendant ou descendant direct de l'une des personnes présentes dans le fichier. La recherche en parentèle indirecte en aveugle, concernant la recherche de possibles frères et sœurs, fut pour sa part mandatée en 2012, toujours sans aucune base légale.
Ces actions ne sont pas anodines. Elles conduisent à la transformation du FNAEG en fichier de « gens honnêtes », puisque les personnes fichées n'ont pas commis le crime faisant l'objet de la recherche en parentèle. Le FNAEG n'est ici utilisé que comme un fichier « de circonstance », dont l'illicéité de l'usage sera moins contestée parce qu'il contient des « réprouvés » (dont 76 % ne sont pourtant que des « mis en cause »). Or, la recherche en parentèle étend considérablement la portée du fichier, au moins d'un facteur 5. C'est donc près d'un quart de la population française, le plus souvent des personnes issues des catégories sociales les moins favorisées, qui sont ainsi fichées de façon directe ou indirecte[21].
Plus généralement, on constate une volonté, de la part de nombre d'États, de collecte massive des données biométriques de leurs citoyens, des personnes souhaitant entrer sur leur territoire[22], voire de l'intégralité de la population mondiale. Il ne s'agit, dans ce dernier cas, de rien moins que de se doter de la capacité d'identifier toute personne d'après ses traces biométriques, qu'elles soient corporelles ou psychiques. Les révélations d'EDWARD SNOWDEN ont ainsi mis en lumière des programmes tels que CIA/ExpressLane (collecte en sous-main des données biométriques récupérés par les services de renseignement « alliés »), NSA/PRISM ou encore NSA/MUSCULAR, ces derniers ayant par exemple apparemment permis d'identifier les personnes se cachant derrière le pseudonyme « Satoshi Nakamoto », créateur de la cyber-monnaie Bitcoin, au moyen de la stylométrie (biométrie du style d'écriture)[23]. Ces données sont également collectées par la « donation » à nombre de pays en développement, majoritairement africains, d'équipement biométriques de contrôle aux frontières, dont les données biométriques collectées ne sont pas hébergées dans le pays récipiendaire.

3 Plaidoyer pour un cahier des charges démocratique

La réglementation de l'usage des technologies numériques reste un défi pour le droit. Alors que la révolution numérique impose au législateur de maintenir une cohérence doctrinale forte au sein de l'édifice normatif (statut de la donnée, promotion de la sécurité des systèmes d'information, régulation des effets monopolistiques, etc.), devant en particulier conduire à étendre les droits et libertés fondamentaux au sein des nouveaux espaces numériques[24], le mirage sécuritaire dérègle la boussole des droits fondamentaux. La fascination technicienne fait exister ce qui est possible, et non ce qui est souhaitable[25,26], la très grande vitesse du progrès technique dans le monde numérique empêchant la prise du recul nécessaire.
Les décisions hâtives prises au prétexte d'un émoi populaire qui prétendrait ne pas comprendre que « rien ne soit fait » conduisent à un risque majeur de mésusage de ces technologies à l'encontre des populations. Quelle Résistance serait possible dans un tel environnement ? Comme il a été fort justement relevé par YUVAL NOAH HARARI[27], les principaux dommages des attaques terroristes aux démocraties occidentales sont ceux qu'elles s'infligent à elles-mêmes au nom de la « sécurité ».
Il est du devoir d'un régime démocratique de protéger les populations, même après sa disparition et dans l'attente de sa résurrection. Cette préoccupation fondamentale doit conduire à réactiver et renforcer le droit fondamental à la sûreté, que certains

19 Il s'agit de l'affaire dite « Élodie Kulik ».
20 Celle-ci sera autorisée a posteriori par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, en son article 80, voir : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231 .
21 Pour de plus amples développements sur ce sujet, voir : Ousmane GUEYE et François PELLEGRINI, « Vers une remise en cause de la légalité du FNAEG ? », in Actes des Convergences du droit et du numérique, septembre 2017, https://hal.inria.fr/hal-01630870 .
22 C'est le cas, au niveau de l'Union européenne, au sein des fichiers VIS (« Visa Information System ») et Eurodac.
23 Alexandre MUSE, « How the NSA identified Satoshi Nakamoto », Medium.com / CryptoMuse, 26 août 2017, https://medium.com/cryptomuse/how-the-nsa-caught-satoshi-nakamoto-868affcef595 .
24 Voir par exemple : François PELLEGRINI, « La portabilité des données et des services », *op. cit.*
25 Laurent MUCCHIELLI, *Vous êtes filmés - Enquête sur le bluff de la vidéosurveillance*, Paris, Armand Colin, ISBN 978-2-200-62123-0, 2018.
26 François PELLEGRINI et André VITALIS, « La création du fichier biométrique TES : la convergence de logiques au service du contrôle », Sociologie, Presses Universitaires de France, 2017, 8(4), pp. 447-452, https://journals.openedition.org/sociologie/3394 .
27 Yuval Noah HARARI, « La stratégie de la mouche : pourquoi le terrorisme est-il efficace ? », Bibliobs, 18 août 2017, https://bibliobs.nouvelobs.com/idees/20160331.OBS7480/la-strategie-de-la-mouche-pourquoi-le-terrorisme-est-il-efficace.html .

tentent d’évincer au profit d’un inepte et illusoire « droit à la sécurité ». Ce principe doit guider les pouvoirs publics dans la définition et la mise en œuvre d’un « cahier des charges démocratique » devant s’imposer à tous les traitements de données publics.
Parmi les dispositions attendues d’un tel document, doivent figurer le refus de la conservation par l’État, au sein de ses fichiers administratifs, des données biométriques des citoyens, ainsi que la limitation de la taille des fichiers de police, seuls à même de conserver de telles informations. Tous les fichiers potentiellement utilisables à l’encontre des populations (le RNIPP de l’INSEE, mais également les fichiers tels que TES) doivent disposer de dispositifs d’auto-destruction opérationnels et fiables, encadrés par des procédures prédéfinies, permettant à la puissance publique de supprimer ces fichiers en cas d’atteinte majeure au fonctionnement démocratique de l’État.
Il est également indispensable de disposer d’un système administratif d’identification contournable permettant, en cas de crise majeure, aux personnes menacées de disposer de « vrais-faux » papiers afin d’échapper à l’arbitraire. Nombre de personnes n’existent actuellement que parce que leurs grands-parents ont pu bénéficier de tels documents, avec l’aide de fonctionnaires courageux. Il est pour cela essentiel de se prémunir contre les mécanismes facilitant la détection d’identités multiples, appelée « déduplication ». C’est à ce titre que les empreintes digitales et les photographies ne doivent pas être conservées dans les bases administratives centralisées, mais seulement au sein des documents délivrés aux personnes. L'absence de ces données vise également à empêcher la mise en œuvre à grande échelle de « rafles assistées par ordinateur ».
La puissance des outils numériques modifie profondément l’équilibre des pouvoirs au profit des acteurs capables de collecter et traiter de grandes masses d’informations. La puissance publique n’est pas un acteur comme les autres, car elle dispose d’un droit de contrainte sur les personnes que ne possèdent pas les acteurs privés. Cette responsabilité considérable doit la conduire à une prudence extrême dans l’usage de la puissance numérique, afin d’en amoindrir autant que possible les risques de mésusage sur le temps long.