RENAISSANCE numerique

LIBERTÉS PUBLIQUES ET ÉTHIQUE
JUIN 2021

TECHNOLOGIES DE SÉCURITÉ :

Sans un contrôle effectif, pas de confiance des citoyens

Préambule

La note ci-après vise à contribuer aux travaux de la mission « Pour un usage responsable et acceptable par la société des technologies de sécurité », confiée par le Premier ministre au député Jean-Michel Mis.
Cette mission a vocation à étudier deux axes en particulier :

- *« Les opportunités offertes par les nouvelles technologies au service d'une meilleure offre de sécurité en analysant les besoins des forces de sécurité, entre autres dans la perspective des grands événements sportifs de 2023 et 2024.*
- *Les principes nécessaires à la préservation des libertés en définissant un cadre d'emploi global et cohérent des technologies de sécurité et en associant la société civile à cette définition pour renforcer la compréhension et l'acceptabilité des nouvelles technologies dans la société. »*[1]

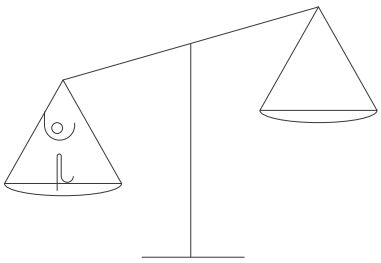
Cette note a également été partagée avec la sénatrice Agnès Canayer et le sénateur Marc-Philippe Daubresse, en tant que rapporteurs du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement.

La position partagée ici est issue d'une réflexion collective au sein de Renaissance Numérique[2].

1 Source : questionnaire de la mission.
2 La liste des contributeurs est mentionnée à la fin du document.

Les technologies numériques de sécurité sont en quête d'une gouvernance de confiance

Le champ de la sécurité connaît une multiplication des usages des technologies numériques. Usages publics, privés, voire publics-privés, les applications sont multiples et relancent avec une vive acuité le débat ancien de l'équilibre entre le droit à la sécurité et les libertés publiques.



La multiplication des textes législatifs visant à favoriser le déploiement de technologies toujours plus intrusives dans le champ de la sécurité est un marqueur des attaques successives à cet équilibre. Sur les trente-cinq premières années de l'application de la Loi Informatique et Libertés, douze textes principaux ont été consacrés à la création de fichiers de police ou de justice ou à la régulation de technologies de sécurité (vidéoprotection, empreintes ADN), contre vingt-neuf textes sur les dix dernières années pour introduire ou réguler *a posteriori* des technologies numériques de sécurité (géolocalisation, accès élargi aux données de trafic, nouvelles techniques de renseignement, *IMSI catchers*, drones, consultations élargies de fichiers centraux, nouveaux champs de l'identification génétique, reconnaissance faciale, etc.). Si cette tendance a accompagné l'essor même de l'innovation dans le champ de la sécurité, ce dernier ne suffit pas à justifier cet écart. Rien que sur cette dernière année, on dénombre trois textes liés aux enjeux de sécurité : la proposition de loi pour une sécurité globale préservant les libertés, le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, et enfin la proposition de loi d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle, portée par le député Didier Baichère.

Exécutifs et législateurs successifs semblent engagés dans une course en avant pour accroître le champ des usages des technologies numériques dans le domaine de la sécurité et les exceptions juridiques afférentes. Si cette tendance participe d'un affaiblissement progressif des libertés publiques, l'apport efficient pour la sécurité n'est, lui-même, pas toujours démontré. Il semblerait qu'il en soit de même de la mission parlementaire à laquelle répond cette position. Le besoin de ces technologies et leur apport incrémental au regard des moyens, des formations nécessaires et des capacités d'analyse ou de corrélation, est faiblement interrogé dans la lettre de mission. Qu'est-ce que l'on ne peut pas faire sans avoir recours à ces technologies ? A-t-on évalué leur performance au regard du besoin de sécurité dans un environnement où les formes de criminalité ou d'infractions se multiplient, en diversi-

té et en volume ?[3] Ces technologies ne sont d'ailleurs pas décrites, ni même mentionnées en exemples ou en « cas d'usage » précis. Quelles sont les technologies concernées par les termes de « technologies de sécurité » ? La mémoire est-elle une technologie de sécurité ? La multiplication des accès à des bases de données aussi ? Les nouveaux « capteurs » d'informations sont-ils en soi utiles sans interroger la capacité d'analyse ? Quelles données vont être traitées ? Qui va les utiliser ? Dans quel contexte ? Pour quel motif initial ? Pour quelle évolution des besoins ? Pendant combien de temps ? Cette analyse que l'on précipite en amont de plusieurs rendez-vous sportifs internationaux, mériterait une réflexion plus approfondie, qui dépasse la création d'un « produit » pour adresser un « besoin » particulier. Renaissance Numérique redoute que l'urgence de ces rendez-vous internationaux contribue à modifier durablement nos perceptions en la matière, sans que des justifications solides soient apportées à cette urgence.

Le dur constat que fait le think tank est que le débat a peu progressé depuis sa dernière position en 2015, relative à la loi Renseignement, qui a notamment créé la Commission nationale de contrôle des techniques de renseignement (CNCTR)[4]. Renaissance Numérique alertait alors sur l'accumulation des exceptions juridiques relatives aux usages numériques dans le champ de la sécurité, notamment en matière de surveillance. Le think tank appelait à ce que la CNCTR devienne un « *réel organe de contrôle, indépendant, autonome et compétent face aux risques de dérives liés à une surveillance accrue* ». Malgré une forte mobilisation des défenseurs des droits, cet appel n'a eu que peu d'effet et, six ans plus tard, la question est à nouveau posée par le législateur : comment mieux encadrer ce déploiement ?

Un prérequis : respecter la méthode instaurée par notre État de droit

Avant d'envisager toute évolution du cadre juridique, il conviendrait déjà d'établir un diagnostic fin du cadre existant et de l'effectivité de son application. Une réflexion récente du think tank relative aux technologies de reconnaissance faciale a par exemple démontré que le cadre juridique entourant ces technologies était relativement bien fourni (droits fondamentaux, textes européens — Règlement général sur la protection des données et Directive

3 À ce titre, les technologies de reconnaissance faciale sont un exemple particulièrement illustratif des limites de ces technologies, dont on ne peut en particulier garantir une fiabilité à 100 %. Voir le rapport de Renaissance Numérique sur ce sujet : « Reconnaissance faciale : Porter les valeurs de l'Europe », juin 2020, 104 p.
4 Renaissance Numérique, « Projet de loi Renseignement. Pas de garantie des droits sans un pouvoir de contrôle effectif », Position, Mai 2015.

Police-Justice —, et nationaux — Loi Informatique et Libertés, réglementation relative à la vidéoprotection —). Or, ce cadre pâtit de faiblesses dans son application qui le rendent peu efficient, puisque peu respecté[5]. Qu'en est-il concernant les autres technologies dites « de sécurité » ?

Donner les moyens aux forces de l'ordre d'assurer leur mission passe par un renforcement de la confiance des citoyens envers eux. Pour ce faire, le respect des procédures qui existent au sein notre État de droit est un prérequis. L'objectif de sécurité est nécessaire, mais il ne se suffit pas en soi — pas davantage que d'autres objectifs légitimes —, tant qu'on n'examine pas ses modalités de mise en œuvre. Cela paraît tellement évident qu'il est étonnant de se poser encore la question des modalités de mise en œuvre de technologies de sécurité. Les technologies de sécurité ne relèvent pas — pas davantage que les règles d'engagement des forces de l'ordre —, d'une liberté consistant à « essayer pour voir ».

L'innovation exploratoire est néanmoins possible pour déterminer quelle amélioration d'efficacité, quel coût de fonctionnement, quelle intégration opérationnelle et réglementaire, est applicable à ces technologies. Pour ce faire, toute technologie de sécurité se déploie dans un contexte opérationnel et réglementaire qui exige une justification préalable de la proportionnalité et de la pertinence de son usage. L'analyse d'impact est une méthode prescrite par les textes en vigueur. Elle ne consiste pas à être d'accord avec soi-même, mais à justifier préalablement auprès d'un organe indépendant ou légitime (le législateur, le Conseil constitutionnel, le Conseil d'État, la Commission nationale de l'informatique et des libertés (CNIL)) d'un certain nombre de critères objectifs : finalité légitime, modalités de collecte d'information, limitation à des données pertinentes et nécessaires, possibilité de filtres et de rejets des données collectées, destinataires limités et justifiés, durée proportionnée, analyse d'impact du recoupement avec d'autres sources, droit d'accès direct ou indirect, mécanisme de contrôle *a posteriori*, voie de recours à caractère juridictionnel, sanctions en cas de violation des règles établies.

À ce titre, nombre de questions de la mission parlementaire se rapportent au principe de proportionnalité. Or, il existe un cadre juridique très clair qui le régit : le devoir de proportionnalité consiste à opérer une mise en balance et réaliser un équilibre entre chacun des principes juridiques en cause — généralement un pouvoir reconnu à l'État (ordre public, force publique) — et des droits fondamentaux des personnes, ou entre plusieurs droits fondamentaux. Le respect du principe de proportionnalité impose qu'une mesure restreignant les droits et libertés respecte ce qu'on appelle le triple test, c'est-à-dire qu'elle soit à la fois : appropriée, en ce qu'elle doit permettre de réaliser l'objectif légitime poursuivi ; nécessaire, c'est-à-dire qu'elle ne doit pas excéder ce qu'exige la réalisation de cet objectif ; et proportionnée, en ce qu'elle ne

5 Renaissance Numérique, « Reconnaissance faciale : Porter les valeurs de l'Europe », juin 2020, 104 p.

doit pas, par les charges qu'elle crée, être hors de proportion avec le résultat recherché[6]. Le principe de proportionnalité doit permettre d'évaluer la nécessité ou les apports mesurables (en qualité, en pertinence, en efficacité) des technologies utilisées au regard des objectifs visés, afin de garantir les libertés publiques qui s'expriment dans la vérification que les finalités correspondent aux missions qui sont dévolues, qu'il n'y a pas notamment des données qui sont traitées plus longtemps ou à destination d'autres acteurs que ceux qui sont déclarés. Quels que soient les usages des technologies de sécurité, ils peuvent être traités au travers de la même méthode et répondre à la même question : ces usages passent-ils le triple test et permettent-il de garantir l'équilibre sécurité / libertés publiques ? Renaissance Numérique considère qu'il n'y a donc pas lieu de créer de nouvelles instances pour garantir ces équilibres. Le droit constitutionnel, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, la Charte des droits fondamentaux de l'Union européenne, la jurisprudence de la Cour de justice de l'Union européenne (CJUE), de la Cour européenne des droits de l'homme (CEDH) et du Conseil d'État[7], le Règlement général sur la protection des données (RGPD), l'ensemble de ce *corpus* juridique intègre le principe de proportionnalité, qui n'est pas un principe d'interdiction, mais une condition de validité.

Ainsi, des instances sont déjà en place pour garantir l'application de ce principe. À ce titre, même s'il ne faut pas limiter ce contrôle à la protection des données personnelles, de nombreux droits fondamentaux pouvant être mis en cause[8], il convient de noter que l'analyse de la conformité des technologies de sécurité aboutira toujours à cette question. Dans toutes les circonstances, il y aura un moment où il s'agira d'imputer un comportement (atypique ou criminogène) à une personne ou à un groupe de personnes, même si on part de données comportementales, anonymes, pseudonymes, ou de géolocalisation, qui ne sont pas rattachées à un individu *a priori* identifiable. On arrivera donc toujours à des questions de protection des données personnelles relevant du RGPD ou de la Directive Police-Justice. La CNIL joue ainsi un rôle essentiel dans la régulation de ces technologies par l'application du principe de proportionnalité, qui consiste d'abord à plaider sa cause dans une analyse d'impact pouvant faire l'objet d'un débat contradictoire, afin d'éclairer la décision publique. *A priori*, c'est la CNIL qui est consultée quand sont en cause des données susceptibles d'être qualifiées de personnelles ou de relever de la vie privée des personnes. Quand il s'agit des droits des personnes, c'est aussi cette commission qui est consultée, notamment

6 Renaissance Numérique, « Reconnaissance faciale : Porter les valeurs de l'Europe », juin 2020, 104 p.
7 Dans le cadre d'un rapport État-citoyen, ou administration-citoyen.
8 Voir sur ce sujet le rapport de l'Agence des droits fondamentaux de l'Union européenne sur les technologies de reconnaissance faciale : 2019, « Facial recognition technology: fundamental rights considerations in the context of law enforcement », 36 pp. : https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

dans la procédure de droit d'accès indirect[9].

Or, de manière récurrente, exécutifs et législateurs cherchent à remettre en cause ce cadre avec l'argument que ce dernier contraindrait les possibilités de sécurité. Un dernier exemple en date est la proposition de loi pour une sécurité globale préservant les libertés pour laquelle nombre d'acteurs, en dépit de son intitulé, ont soulevé les risques pour les libertés publiques. Dans sa décision du 20 mai 2021, le Conseil constitutionnel a invalidé plusieurs articles de la proposition de loi (7 articles sur 22), dont certains relatifs à l'emploi de technologies numériques par les forces de l'ordre[10]. Le juge constitutionnel a relevé ainsi plusieurs atteintes à l'équilibre entre « *les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions et le droit au respect de la vie privée* ».

Un autre exemple est la difficulté du gouvernement à bâtir une doctrine sur la conservation des données de trafic, de connexion, de localisation ou de mise en ligne de contenus numériques, afin de se mettre en conformité avec les décisions de la CJUE et de la CEDH. Si, dans plusieurs arrêts, cette dernière a reconnu la surveillance de masse, elle exige des « *garanties de bout en bout* », dont une autorisation *a priori* et un contrôle *a posteriori* par des autorités indépendantes, et l'appréciation à chaque étape du processus de surveillance de « *la nécessité et* [de] *la proportionnalité des mesures prises* »[11]. Il n'y a pas de sécurité sans finalité de sécurité. Or, subsiste dans la loi française une faiblesse de ce contrôle, qui fait qu'une donnée peut être conservée alors que les raisons de sa collecte s'avèrent inexistantes. Il convient de savoir pourquoi les données doivent être captées, la façon dont elles le seront, qui y aura accès et dans quelles conditions, et connaître le tri *a posteriori* sur l'utilité à court ou long terme des données collectées.

Par ailleurs, au-delà des textes, c'est le respect même du cadre en pratique qui fait défaut. Le temps qui a été par exemple laissé à la CNIL afin qu'elle rende son avis sur la dernière loi Renseignement est assez significatif en la matière. Il est nécessaire de permettre aux autorités de contrôle indépendantes de jouer pleinement le rôle que la loi leur consacre afin de construire une stratégie prévisible, c'est-à-dire efficace.

---

9 La CNIL définit ce droit ainsi : « *Toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la Défense et la Sécurité publique.* » Source : https://www.cnil.fr/fr/definition/droit-dacces-indirect

10 Conseil constitutionnel, Décision n° 2021-817 DC du 20 mai 2021 : https://www.conseil-constitutionnel.fr/decision/2021/2021817DC.htm

11 Lire à ce sujet la synthèse de Nicolas Hervieu : https://twitter.com/N_Hervieu/status/1397128120654778370

Trois voies d'amélioration pour maintenir l'équilibre sécurité / libertés

Comment faire en sorte que le cadre juridique soit pleinement appliqué et le principe de proportionnalité respecté quand il s'agit de déployer des technologies de sécurité ? Pour ce faire, Renaissance Numérique entrevoit trois voies d'amélioration.

1. Partager une culture juridique et technique avec les décideurs publics et potentiels utilisateurs des technologies de sécurité

Au-delà des aspects purement politiques ou des intérêts privés au financement de telle ou telle technologie de sécurité, la mauvaise application du cadre juridique peut s'entendre également par un défaut de connaissance juridique et technique de la part des décideurs publics et des potentiels utilisateurs, qu'ils soient publics ou privés. Du point de vue de la conception de la loi, peu de législateurs appréhendent des notions comme le « triple test » ou les spécificités techniques de ces technologies, d'autant plus qu'elles sont multiples et évolutives. Il s'ensuit une méfiance, corollaire de la méconnaissance, des contraintes juridiques et des modalités techniques entourant les technologies de sécurité. Ces décisions devraient être éclairées par la réunion de différents types d'expertises et ce, de manière systématique, afin qu'il ne soit pas « trop tard » pour aboutir à un projet charpenté sur l'ensemble des enjeux en présence. Rien que sur le plan juridique, il conviendrait de réunir des experts du droit constitutionnel, de la protection des données personnelles, du droit international ou encore de la sécurité / du renseignement, chaque champ juridique ayant ses particularités. Alors que l'on réfléchit à l'évolution de la formation des agents de l'État et notamment de la haute fonction publique avec la transformation de l'École nationale d'administration en Institut du service public, cette nécessaire diversité et montée en compétences doivent être intégrées dans les nouveaux programmes.

2. Donner (enfin) un pouvoir de contrôle effectif à la CNCTR

Dans sa position de 2015 sur la création de la Commission nationale de contrôle des techniques de renseignement, Renaissance Numérique invitait à donner à cette instance un pouvoir de contrôle effectif et les moyens financiers, humains et techniques afférents. Or, telle qu'instituée par la loi de 2015, la CNCTR n'a la possibilité ni d'effectuer un contrôle d'opportunité,

ni de proportionnalité, ni d'injonction, ni de correction, sur les mesures de renseignement. Pour maintenir les équilibres fondamentaux, notamment entre la sécurité et la vie privée, il est nécessaire que ce contrôle porte sur un examen au préalable de tout dispositif de surveillance avant que ceux-ci ne puissent être employés par les services de renseignement, et le refus que pourrait émettre la CNCTR doit s'imposer aux administrations. Concernant son pouvoir de contrôle *a posteriori*, ce dernier doit s'exercer sans devoir passer par une saisie hypothétique du Conseil d'État manquant de contexte et de matière pour constituer une voie effective à un recours juridictionnel. Aujourd'hui, la CNCTR est enfermée dans un principe de recommandation. Pour être en conformité avec le droit de l'Union européenne, il conviendrait que cette instance soit dotée d'un véritable pouvoir de contrôle. Dans une décision récente, le Conseil d'État a, à ce titre, ordonné au gouvernement « *de réévaluer régulièrement la menace qui pèse sur le territoire pour justifier la conservation généralisée des données et de subordonner l'exploitation de ces données par les services de renseignement à l'autorisation d'une autorité indépendante.* »[12] Il s'inscrit non seulement dans la lignée des exigences de la CJUE[13], mais aussi de celles de la CEDH sur les « garanties de bout en bout ».

En 2015, le think tank invitait également à l'existence d'une voie de recours accessible à tout citoyen. Cette dernière doit être simplifiée, digitalisée et la notoriété de la CNCTR renforcée. Le mécanisme d'interpellation en vigueur, qui s'exerce par courrier postal, ne peut aboutir qu'à un débat stérile entre une réclamation et l'absence de réponse utile, la CNCTR n'ayant, en pratique, aucune réponse substantielle à fournir à un justiciable, ni pour estimer infondée sa demande, ni pour l'instruire d'une manière susceptible d'être corrective.

Par ailleurs, il est nécessaire de donner à ces autorités de contrôle (CNCTR, CNIL) les moyens nécessaires à leur mission. Leurs capacités demeurent encore trop limitées et surtout en décalage par rapport à l'élargissement de leur champ de contrôle.

Renaissance Numérique invite les parlementaires à se saisir du projet de loi Renseignement en discussion au Parlement pour donner toute son effectivité à un pouvoir de contrôle de la CNCTR, organisant une compatibilité entre les objectifs de respect du secret de la défense et de la sécurité nationale, et

12 Conseil d'État, « Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité », 21 avril 2021 : https://www.conseil-etat.fr/actualites/actualites/donnees-de-connexion-le-conseil-d-etat-concilie-le-respect-du-droit-de-l-union-europeenne-et-l-efficacite-de-la-lutte-contre-le-terrorisme-et-la

13 Cour de Justice de l'Union européenne, « La Cour de justice confirme que le droit de l'Union s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation », Communiqué de presse n° 123/20, 6 octobre 2020 : https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123fr.pdf

le questionnement légitime de dérives ou d'imprécisions inconciliables avec le devoir de proportionnalité.

3. Renforcer la voie d'accès du citoyen et instaurer une réponse publique

Le droit d'accès indirect qui constitue une autre voie de recours à la disposition des citoyens doit également être renforcé. Il s'agirait de faire évoluer le rôle du commissaire de la CNIL chargé de garantir l'effectivité de ce droit par l'interrogation des organismes publics détenant des informations sur un requérant. En l'état, il faut notamment lui donner les moyens juridiques et techniques nécessaires à ce contrôle, pour que la simple consultation de documents triés par l'administration puisse être assortie d'une capacité à tester — dans le respect des secrets en cause — l'effectivité des mécanismes de purge, lorsqu'il est établi que des informations auraient été stockées sans aucune pertinence.

Depuis 1978, ce droit s'exerce par le truchement d'un commissaire de la CNIL, qui a une fonction juridictionnelle par ailleurs. Il exerce auprès des administrations concernées des droits d'accès des personnes. Cette procédure est sous le contrôle du Conseil d'État et peut faire l'objet d'un contrôle de la Commission d'accès aux documents administratifs (CADA). Un tel mécanisme de contrôle indépendant n'a jamais mis en cause les missions dévolues aux services de police et de justice, ni l'efficacité du renseignement policier. Il n'y a dès lors pas lieu de craindre qu'une voie d'interrogation effective ouverte aux justiciables remette en cause l'équilibre sécurité / libertés, sauf à s'exposer à des cycles de construction législative et de destruction jurisprudentielle, qui nuisent profondément à l'efficacité des politiques publiques en matière de sécurité et fragilisent les équilibres démocratiques en suscitant la défiance de l'ensemble de nos concitoyens, qu'ils soient réputés « libertaires » ou « sécuritaires ».

—

Rédaction

Jennyfer Chrétien, Déléguée générale, Renaissance Numérique

Étienne Drouard, Associé, Hogan Lovells

—

Contribution

Henri Isaac, Président, Renaissance Numérique

Samuel Le Goff, Consultant, CommStrat

Marine Pouyat, Présidente, W Talents

Nicolas Vanbremeersch, Président, Spintank