

MARS 2022

Numérique au service de la sécurité : de l'exception à la banalisation ?

SYNTHÈSE DU DÉBAT DU 21 FÉVRIER 2022, ORGANISÉ PAR RENAISSANCE NUMÉRIQUE EN PARTENARIAT AVEC *L'EXPRESS*



Débat Numérique 2022



Alors que va s'ouvrir un quinquennat crucial pour un certain nombre d'enjeux sociétaux que la transformation numérique soulève, les questions liées au numérique sont quasiment absentes des débats à l'approche de l'élection présidentielle de 2022. Afin de les mettre en lumière, Renaissance Numérique a lancé, en partenariat avec *L'Express*, le cycle de rencontres «**Débat Numérique 2022.**» Au-delà de dresser le bilan des cinq dernières années et de dégager des points d'attention pour le prochain quinquennat, ce cycle vise à donner la parole aux acteurs qui font, vivent et pensent la transformation numérique de la société. La seconde édition, «**Numérique au service de la sécurité : de l'exception à la banalisation ?**», s'est tenue le lundi 21 février 2022.

Sur les dix dernières années, les initiatives législatives et actions publiques visant à favoriser le déploiement de technologies numériques toujours plus intrusives dans le champ de la sécurité se sont multipliées. Rien que sur les huit derniers mois, on peut citer la loi pour une sécurité globale préservant les libertés¹, la loi relative à la prévention d'actes de terrorisme et au renseignement² et la loi relative à la responsabilité pénale et à la sécurité intérieure³. En parallèle, les expérimentations et usages basés sur ces technologies (détection automatisée de comportements, scanners corporels, dispositifs de capture audiovisuelle embarqués, identification biométrique par reconnaissance faciale...) se développent et viennent percuter certains de nos droits les plus fondamentaux. Si ces développements visent en partie à faire respecter l'ordre public et à lutter contre la criminalité, le recours au numérique au nom de la sécurité et de la protection s'observe dans toutes les sphères de l'économie et de la société, y compris dans le domaine de la santé, à l'instar du passe sanitaire mis en place dans le cadre de la lutte contre le Covid-19.

Face à ces développements, se pose la question de l'équilibre entre le droit à la sécurité et nos autres droits et libertés fondamentaux. Les garde-fous juridiques et démocratiques existants suffisent-ils à maintenir cet équilibre à l'ère numérique ? Le besoin de ces technologies et leur apport incrémental sont-ils suffisamment interrogés ? Pour répondre à ces questions, Renaissance Numérique et *L'Express* ont réuni **Alexandre Archambault**, avocat au barreau de Paris, **Noémie Levain**, chargée d'analyse politique et juridique à La Quadrature du Net, et **Myriam Quéméner**, magistrate à la Cour d'appel de Paris. Cette synthèse retrace leurs échanges.

1 • Loi du 25 mai 2021 pour une sécurité globale préservant les libertés : <https://www.vie-publique.fr/loi/277157-loi-pour-une-securite-globale-preservant-les-libertes>

2 • Loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement : <https://www.vie-publique.fr/loi/279661-loi-30-juillet-2021-prevention-terrorisme-et-renseignement>

3 • Loi du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure : <https://www.vie-publique.fr/loi/280828-loi-24-janvier-2022-responsabilite-penale-et-securite-interieure>

VERS UNE BANALISATION DU RECOURS AU NUMÉRIQUE À DES FINS DE SÉCURITÉ

Malgré quelques divergences sur des points spécifiques, les intervenants ont tous trois souligné le fait que nous assistons depuis plusieurs années à un élargissement du champ du recours au numérique par les autorités publiques. À cet égard, **Noémie Levain** et **Alexandre Archambault** évoquent l'idée d'une banalisation de ces usages à des fins de sécurité, qu'ils attribuent à l'omniprésence du numérique dans toutes les sphères de la société. Alors que les *smartphones*, les objets connectés, les réseaux sociaux, la biométrie, l'identité numérique...font de plus en plus partie de notre quotidien, les technologies numériques sont de plus en plus mobilisées par les pouvoirs publics afin d'assurer la sécurité publique au sens large. Or, pour **Alexandre Archambault**, il faut absolument éviter de considérer le numérique comme une réponse à tous les problèmes, comme un « *formidable outil* » qui serait dépourvu d'aspects négatifs. Selon lui, si les technologies numériques peuvent comporter des avantages dans certains cas d'usage, elles constituent une sorte de « *prison dorée*. » Afin d'illustrer ce propos, il cite l'exemple du système PARAFE⁴ : « *en tant que consommateur, cela nous permet de gagner du temps, mais au prix d'une banalisation de l'exception. On abandonne collectivement l'un des fondements du libre-arbitre humain.* »

Noémie Levain regrette également cette « banalisation », qui aurait pris une nouvelle ampleur récemment : « *Du fait que tout le monde est aujourd'hui équipé de smartphones, on est passé à une échelle différente. On constate que, dans les moments de crise, les gouvernements jouent sur le sentiment de peur pour pérenniser des technologies et des lois d'exceptions. On banalise des techniques de contrôle, dont le gouvernement lui-même critiquait l'utilisation en Chine en 2020.* » Elle déplore tout particulièrement « *la rapidité à laquelle ces outils ont été banalisés* », et le fait que, dans le cadre de la lutte contre la pandémie de Covid-19, « *le premier réflexe a été la répression, la sécurité.* » Selon la représentante de La Quadrature du Net, le gouvernement a cédé à « *un solutionnisme technologique, où la technologie a été présentée comme la solution à la pandémie.* » En outre, la nécessité de recourir aux technologies dites « de sécurité » n'est selon elle pas prouvée. Afin d'étayer ce propos, la juriste évoque l'expérience de La Quadrature du Net qui, lorsqu'elle questionne des propositions de loi ayant trait au numérique devant le Conseil d'État ou la Cour de justice de l'Union européenne, se heurte régulièrement à l'incapacité des représentants du gouvernement à justifier le besoin de recourir à telle ou telle technologie.

4 • Le dispositif « Passage automatisé rapide des frontières extérieures » (PARAFE) repose sur le contrôle automatisé des passeports biométriques, soit par une analyse des empreintes digitales, soit par le recours à des technologies de reconnaissance faciale.

Un avis partagé par **Alexandre Archambault**, pour qui les arguments en faveur de l'utilisation de technologies numériques de sécurité ne sont que peu convaincants. Aussi appelle-t-il à un débat démocratique sur l'utilisation de ces outils : *« ces cinq dernières années, la plupart des lois sur le numérique ou sur le pénal sont passées en procédure d'urgence, avec des arguments d'autorité qui empêchent la tenue d'un débat raisonné. »* Selon l'expert, la technologie devrait se soumettre à un cadre juridique strict défini préalablement à son recours, après des débats de fonds auxquels les citoyens devraient pouvoir contribuer. Au lieu de cela, les lois votées se limitent selon lui à autoriser ou non le recours à une technologie, et à prévoir des garanties visant à encadrer les usages.

Pour **Noémie Levain**, cette banalisation répond par ailleurs à une logique d'économie de marché. Selon elle, ces outils sont commercialisés par des acteurs privés qui ont tout intérêt, d'un point de vue économique, à contribuer à la diffusion du sentiment d'insécurité, voire à sa fabrication. *« Cette croyance autour du sentiment d'insécurité est nourrie par des discours politiques et médiatiques, mais aussi par une industrie qui fabrique ces technologies de surveillance et qui impose son rythme »*, souligne-t-elle.

DES GARANTIES INSUFFISANTES POUR PROTÉGER LES DROITS FONDAMENTAUX ?

Si cette banalisation interroge, **Alexandre Archambault** a tenu à rappeler que *« le juge ne remet pas en question le principe même de l'utilisation du numérique pour servir d'appui à la poursuite des auteurs d'infractions pénales, et pour la prévention de certaines atteintes à l'ordre public. »* Il conçoit en effet aisément que la collecte de données de toute nature par l'État puisse lui permettre de mieux orienter l'action publique et de la rendre plus efficace dans certains domaines, comme la criminalité grave. Mais à ses yeux, l'époque actuelle dénote un *« sacrifice de certains principes séculaires, voire millénaires »*, sur l'autel de l'efficacité. Selon l'avocat, *« le droit et l'action publique doivent être efficaces, mais pas au prix du renoncement de ce qui constitue l'essence même d'une démocratie : le respect de l'État de droit, des droits fondamentaux et de la procédure, du principe d'instruction à charge et à décharge. »*

Si **Myriam Quéméner** partage ce constat, elle estime néanmoins que les droits des citoyens sont toujours protégés par un certain nombre de garanties. Selon la magistrate, ces garde-fous se manifestent notamment par l'intervention du juge. Certes, souligne-t-elle, le législateur s'est adapté au glissement de la délinquance vers le numérique en mettant à jour l'arsenal législatif d'une part, et en autorisant certains

usages du numérique à des fins d'investigations d'autre part. Pour autant, elle estime que le pouvoir judiciaire a conscience que les textes peuvent être imparfaits et sait faire preuve de vigilance : « *les nouveaux moyens d'investigation, comme la captation de données, sont très encadrés* » en particulier par des « *garanties procédurales, rappelées notamment par le Conseil constitutionnel. La notion de proportionnalité doit être le fil rouge des évolutions procédurales. Tout est encadré, et tout peut être contesté devant un juge.* » Elle rappelle par exemple que des dispositifs tels que la captation de données ne peuvent être déployés que dans le cadre de procédures judiciaires relatives à des crimes et délits d'une particulière gravité (terrorisme, crime organisé).



« Le droit et l'action publique doivent être efficaces, mais pas au prix du renoncement de ce qui constitue l'essence même d'une démocratie : le respect de l'État de droit, des droits fondamentaux et de la procédure, du principe d'instruction à charge et à décharge. »

Alexandre Archambault

— Avocat au barreau de Paris

Une vision à laquelle n'adhère cependant pas **Noémie Levain**, qui considère que les garde-fous judiciaires ne constituent pas des garanties suffisantes pour protéger la vie privée des citoyens. Elle prend pour exemple la validation récente par le Conseil constitutionnel de la captation d'images par drones dans le cadre d'opérations de police administrative⁵, « *sans aucun débat sur le danger intrinsèque de ces technologies.* » Si, jusqu'à présent, le recours aux drones n'était autorisé que dans le cadre d'enquêtes judiciaires, cette décision pourrait, selon La Quadrature du Net, ouvrir la porte à une surveillance généralisée⁶. En outre, elle trouve dommageable que le Conseil d'État, dans sa décision du 21 avril 2021 relative à la conservation des données de connexion au regard de la sécurité nationale⁷, ait « *interprété de manière totalement contraire à son véritable sens* » une décision de la Cour européenne des droits de l'homme, en autorisant la conservation généralisée de ces données durant un an afin que la police puisse y accéder dans le cadre de ses enquêtes. Via cette décision, la juriste estime que « *le Conseil d'État, qui est censé être le garant des libertés, a manqué à son rôle de garde-fou.* » Ainsi, pour **Noémie Levain**, si des garde-fous existent en théorie afin de protéger nos droits fondamentaux, ils ne sont pas

5 • Conseil Constitutionnel, Décision n° 2021-834 DC du 20 janvier 2022, communiqué de presse, 20 janvier 2022 : <https://www.conseil-constitutionnel.fr/actualites/communiquedecision-n-2021-834-dc-du-20-janvier-2022-communiquedepresse>

6 • La Quadrature du Net, « Les drones policiers autorisés par le Conseil constitutionnel », 21 janvier 2020 : <https://www.laquadrature.net/2022/01/21/les-drones-policiers-autorises-par-le-conseil-constitutionnel/>

7 • Conseil d'État, Décision n°393099, 21 avril 2021 : <https://www.conseil-État.fr/fr/arianeweb/CE/decision/2021-04-21/393099>

nécessairement mis en pratique. Par ailleurs, trop souvent selon elle, les dispositions procédurales prévues par la loi ne sont pas mises en œuvre. Ainsi en serait-il de l'utilisation faite par les forces de l'ordre du fichier « Traitement d'antécédents judiciaires » (Taj)⁸. Selon l'experte, contrairement à ce qui est prévu par la loi, le recours par la police aux technologies de reconnaissance faciale pour la vérification des antécédents judiciaires des individus n'est, dans la pratique, pas soumis au contrôle préalable d'un magistrat.

CONSACRER UNE CULTURE DE L'ÉVALUATION ET DU DÉBAT

Pour certains des intervenants, si le recours au numérique dans le domaine de la sécurité a pu se banaliser jusqu'à empiéter sur l'équilibre entre les droits fondamentaux, c'est notamment du fait de l'absence d'une culture de l'évaluation des lois.

Alexandre Archambault dégage ainsi un schéma qui, selon lui, se répète à chaque fois qu'un événement d'une amplitude majeure survient (par exemple des attentats terroristes ou une crise sanitaire) : « *sous la pression de l'opinion publique, qui terrorise le politique, on nous sort des lois de circonstance sans faire le bilan des dispositifs existants.* » Et ce, d'après l'avocat, avec des résultats mitigés. Il note que, dans le cadre judiciaire par exemple, cet « *empilement de lois de circonstances complique la vie des enquêteurs qui n'ont ni les moyens, ni la formation* » pour s'y adapter. **Myriam Quéméner** le rejoint sur ce point, précisant que s'il avait évalué l'arsenal législatif en vigueur, le législateur aurait souvent constaté l'existence de mécanismes juridiques d'ores et déjà activables, et n'en aurait pas créé de nouveaux. Selon la magistrate, « *il faut introduire davantage cette culture de l'évaluation : il y a eu une frénésie de textes sur le happy slapping⁹, alors que ces comportements étaient déjà réprimés par les lois sur la violence psychologique. Pareil pour le phishing, qui est réprimé par l'escroquerie, et pour lequel un nouveau texte a été élaboré.* »

Alexandre Archambault déplore également que les textes visant à encadrer le recours à des technologies numériques à des fins de sécurité soient adoptés « *sans évaluation scientifique* », sans débats publics préalables, dans des contextes où l'opinion publique est « *en panique et a tendance à raisonner par l'émotion.* » Selon lui, cette façon de procéder n'est pas du tout à la hauteur des enjeux car, par essence, la loi se doit d'être objective : pour être efficace, elle se doit d'être prise hors du

8 • Pour en savoir plus sur le fichier Taj, voir : <https://www.service-public.fr/particuliers/vosdroits/F32727>

9 • Le « *happy slapping* » ou vidéolynchage ou vidéoagression est une pratique consistant à filmer l'agression physique d'une personne. Le terme s'applique à des gestes d'intensité variable, de la simple vexation aux violences les plus graves, y compris les violences sexuelles. Ce délit est puni par l'article 222-33-3 du Code pénal de 5 ans d'emprisonnement et de 75 000 € d'amende.

coup de l'émotion. À cet égard, il prend l'exemple de la « loi de 1881¹⁰ qui a vu arriver, après l'imprimerie, la radio, la télévision, le cinéma, l'audiovisuel, le minitel, Internet... » et a su traverser les siècles, dans la mesure où « tout était prévu dans ses principes. » Face aux évolutions technologiques, il nous enjoint collectivement à nous « garder de la tentation de l'ordre public numérique », qui ferait de ce sujet un droit à part, et à « nous donner les moyens [d'adapter] les lois existantes plutôt que de créer des lois spécifiques qui complexifient le droit. »

Au-delà de l'évaluation du cadre juridique existant, les intervenants ont souligné l'importance d'évaluer les technologies en tant que telles, et de débattre collectivement de leurs usages. À cet égard, **Noémie Levain** préconise « d'arrêter la spéculation sur les outils sécuritaires et la surenchère dès qu'on parle de surveillance. » Elle nous invite ainsi à « repenser collectivement la question. » À ces yeux, la « répression numérique » n'a en effet pas permis d'atteindre l'objectif de sécurité poursuivi. Il conviendrait dès lors de recentrer le débat sur le choix d'un modèle de société fondé sur « l'entraide, l'associatif, les soins... d'autres possibilités que ces outils sécuritaires qui répondent à des logiques de marché. » Selon la juriste, la Commission nationale de l'informatique et des libertés (CNIL) pourrait par ailleurs prendre part à la mission de contrôle *a priori* de l'introduction de nouvelles technologies en matière de sécurité. « Historiquement, la CNIL a été créée pour contrôler l'État, pour empêcher les dérives de fichage généralisé. Aujourd'hui, ce n'est plus du tout son rôle : elle n'a plus de pouvoir contraignant. Il manque de la volonté politique : la CNIL pourrait être un vrai contre-pouvoir qui, à chaque technologie, impose un débat public. [Aujourd'hui], le débat public se fait après que ces technologies ont été créées, donc trop tard », a souligné la représentante de La Quadrature du Net.



« Historiquement, la CNIL a été créée pour contrôler l'État, pour empêcher les dérives de fichage généralisé. Aujourd'hui, ce n'est plus du tout son rôle : elle n'a plus de pouvoir contraignant. Il manque de la volonté politique : la CNIL pourrait être un vrai contre-pouvoir qui, à chaque technologie, impose un débat public. »

Noémie Levain

— Chargée d'analyse politique et juridique à La Quadrature du Net

10 • Loi du 29 juillet 1881 sur la liberté de la presse : <https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/>

Pour **Myriam Quéméner**, la question de la mise en œuvre d'une certaine « surveillance » numérique est loin de ne concerner que l'État, pourtant soumis, selon elle, à des cadres plus stricts que les acteurs privés en la matière. La magistrate compare ainsi ce qui est permis aux pouvoirs publics et aux géants du numérique en matière de géolocalisation, constatant par exemple que *« ces derniers peuvent vous géolocaliser quand vous souhaitez acheter un canapé, là où la géolocalisation dans le cadre pénal est un domaine extrêmement restreint et limité — ce qui est normal, d'ailleurs. »* Pour autant, le secteur privé a, d'après **Myriam Quéméner**, toute sa place dans le débat. Selon elle, *« il faut une réflexion interministérielle public-privé sur ces enjeux extrêmement forts, dans l'intérêt des citoyens. »*

Au-delà du cadre national, l'Union européenne pourrait également apporter des réponses. **Myriam Quéméner** constate que *« l'ordre public numérique est complètement international, et cette dimension internationale a modifié beaucoup de choses : cela implique des procédures adaptées, comme le mandat d'arrêt européen ou les décisions d'enquête européennes. »* Un point de vue partagé par **Alexandre Archambault**, pour qui *« la coopération internationale est plus que jamais nécessaire pour [...] se garder de la tentation des lois de circonstances. »*

RÉDACTION

Mehdi Rafenne

RELECTURE

Jessica Galissaire, Responsable des études, Renaissance
Numérique

Renaissance Numérique remercie chaleureusement les
intervenants et participants à ce débat qui s'est tenu dans le
cadre de la campagne présidentielle 2022, ainsi que *L'Express* et
l'équipe des Émotionneurs.

[\(Re\)Voir le débat](#)

Retrouvez nos publications sur: www.renaissancenumerique.org

MARS 2022 - CC BY-SA 3.0



Débat Numérique 2022

