Technologies et sécurité : réguler pour reprendre le contrôle

Bertrand Warusfel

Technologies et sécurité : réguler pour reprendre le contrôle

Bertrand WARUSFEL

La numérisation du monde induit logiquement celle de la sécurité, mais cette « *technologisation de la sécurité*[1] » (dont l'une des premières grandes manifestations publique fut en 1995 l'introduction de la vidéosurveillance sur la voie publique) dissimule d'autres réalités sous-jacentes qui peuvent remettre en cause les fondements des pratiques et des compétences régaliennes dans un État de droit.

Car en même temps que la technologie offre de nouveaux outils utiles à la réalisation des missions de prévention ou de répression, on oublie souvent qu'elle produit elle-même sa propre insécurité et qu'elle transforme le cadre de mise en œuvre des missions de sécurité, au risque notamment de brouiller les distinctions essentielles que l'État de droit impose entre les pratiques préventives, y compris privées, et l'action publique garante de la sécurité collective des personnes et des biens.

La technologie produit sa propre insécurité

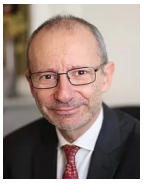
Il y a plus de trente ans Yves Lasfargues nous prévenait que nous étions « [passés de la] *civilisation de la peine* à la *civilisation* de la *panne*[2] ». À la même époque, Ulrich Beck publiait son ouvrage fameux sur la « société du risque[3] ». Dès avant le développement d'Internet et l'essor de tous les réseaux de communication numérique, nous étions donc prévenus de ce que la puissance technologique (et particulièrement la technologie numérique) porte en elle sa propre fragilité[4].

La fragilité intrinsèque des systèmes numériques

Les dernières décennies ont donné raison à ces avertissements que d'aucuns ont sous-estimés sur le moment, les estimant trop alarmistes. Plusieurs cas d'attaques informatiques spectaculaires (notamment contre l'Estonie en 2007, contre la chaîne francophone TV5 Monde en 2015 ou encore

(1) Formule que nous empruntons à Ayse Ceyhan, « Technologie et sécurité : une gouvernance libérale dans un contexte d'incertitudes », *Cultures & Conflits*, hiver 2006, n° 64.
(2) « Changements technologiques et changements du travail : de la peine à la panne », Le Monde, 22 août 1987, repris in Lasfargues (Y.), 1991, *Technojolies, Technofolies – Comment réussir les changements technologiques*, Éditions d'Organisation.
(3) Traduit en français : Beck (U.), 2001, *La société du risque. Sur la voie d'une autre modernité*, Paris, Aubier.
(4) Pour reprendre le titre d'un ouvrage d'Alain Gras, 2003, *Fragilité de la puissance : se libérer de l'emprise technologique*, Fayard.

Bertrand WARUSFEL



Bertrand Warusfel est professeur à l'Université Paris 8 et Vice-président de l'Association française de droit de la sécurité et de la défense (AFDSD). Il enseigne également le droit du numérique et des nouvelles technologies. Il est avocat au barreau de Paris.


© Colin Anderson - stock.adobe.com

la diffusion des virus WannaCry et NotPetya en 2017) ont, en effet, démontré la vulnérabilité de nos infrastructures numériques face à des actions cyber-malveillantes de grande ampleur. En novembre 2018, un rapport de l'Institut Montaigne a même pronostiqué que la France était potentiellement susceptible d'être frappée par un « cyber-ouragan », c'est-à-dire par une attaque massive touchant l'ensemble du tissu économique national et « détruisant une large partie des ressources numériques du pays[5] ». La découverte d'opérations d'espionnage numérique menées contre les organes les plus sensibles de l'État (comme ce fut le cas avec la pénétration des ordinateurs de l'Élysée à la veille de l'élection présidentielle de 2012, aujourd'hui attribuée aux services américains) ou à l'encontre de l'équipe de campagne du candidat Macron en 2017 (dont le GRU russe semblerait responsable, d'après une récente enquête de la justice américaine) confirme par ailleurs les révélations d'Edgar Snowden en 2013 sur les capacités extrêmement puissantes de certaines grandes centrales de renseignement technique (au premier rang desquelles la NSA[6]et son partenaire historique, le britannique GCHQ[7]).

Mais ces menaces en provenance du cyberespace ne sont pas seulement dues au développement (par ailleurs attesté) d'une nouvelle et très impénétrable forme de criminalité globalisée. Elles se traduisent aussi par un risque réel de perturbation, voire d'indisponibilité plus ou moins permanente des nouveaux outils technologiques dont l'État et ses services les plus régaliens (police, gendarmerie, justice, forces armées) usent pour remplir leurs missions de prévention et de répression.

Des risques et menaces qui n'épargnent pas les moyens technologiques de l'État

Qu'il s'agisse de parer des risques d'accident numérique majeur ou d'anticiper des actions offensives provenant de différents milieux hostiles (hackers, puissances étrangères, groupes criminels, groupes terroristes…), plus la puissance publique se repose sur des systèmes techniques complexes, plus elle doit intégrer la perspective d'être désarmée au moins temporairement par les effets des fragilités numériques.

La raison en est simple : même les États disposant d'un écosystème industriel et technologique national sont obligés de recourir pour l'essentiel de leurs infrastructures et de leurs outils numériques à des technologies du marché (qu'il s'agisse de postes de travail, de logiciels standards, de routeurs IP, de messageries électroniques, ou de communications mobiles – y compris la très prochaine

(5) *Cybermenace : avis de tempête* (Marwan Lahoud, dir.), Institut Montaigne, novembre 2018, p. 5.
(6) National Security Agency.
(7) Government Communications Headquarters.

5G). Or, tous les produits ou logiciels disponibles présentent des vulnérabilités que l'industrie mondiale n'arrive pas à colmater, car cette insécurité est en quelque sorte intrinsèque à tout système complexe[8].

Dans son introduction à un dossier consacré en 1995 aux technologies de sécurité (dans ces mêmes Cahiers de la sécurité), Gary Marx écrivait déjà : « Dans quelle société vivrions-nous alors si l'ordre et la sécurité dépendaient exclusivement de la technologie policière ? Que se passerait-il quand cette technologie tomberait en panne ? Car il faut bien penser qu'à terme, une technologie finit toujours par tomber en panne[9] ».

Un récent rapport parlementaire a mis notamment l'accent sur le fait que « les forces de sécurité intérieure s'appuient de plus en plus sur les réseaux civils pour certaines de leurs télécommunications », et que « si l'on avait pu envisager la construction d'un nouveau réseau propre aux forces de sécurité intérieure, basé par exemple sur des technologies de 4G, le ST-SI (service des technologies et des systèmes d'information de la sécurité intérieure du ministère de l'Intérieur) a fait valoir que l'État ne serait probablement pas en mesure de consentir les investissements nécessaires non seulement à la création mais aussi à l'entretien d'un tel réseau[10] ».

Dans le même domaine des communications mobiles, un bon exemple de la difficulté pour les services de l'État à trouver un équilibre entre la numérisation de leurs missions policières et le risque d'exposition aux vulnérabilités numériques globales a été le choix effectué par la gendarmerie et la police nationales de leurs nouveaux terminaux mobiles NEO (nouvel équipement opérationnel) pour remplacer progressivement leurs terminaux informatiques embarqués (TIE) à compter de 2017[11]. Le besoin de pouvoir bénéficier de la bonne couverture radio-mobile 4G sur le territoire pour relier sur le terrain les gendarmes et policiers en patrouille obligea à retenir des terminaux du marché (téléphones et tablettes) et l'OS de Google Androïd. Profitant certes du statut open source de ce système d'exploitation mobile mais ne pouvant envisager de le reprogrammer profondément, l'ANSSI a dû développer une version confidentielle adaptée d'une sur-couche logicielle libre préexistante dénommée SecDroïd.

QU'IL S'AGISSE DE PARER DES RISQUES D'ACCIDENT NUMÉRIQUE MAJEUR OU D'ANTICIPER DES ACTIONS OFFENSIVES PROVENANT DE DIFFÉRENTS MILIEUX HOSTILES (HACKERS, PUISSANCES ÉTRANGÈRES, GROUPES CRIMINELS, GROUPES TERRORISTES…), PLUS LA PUISSANCE PUBLIQUE SE REPOSE SUR DES SYSTÈMES TECHNIQUES COMPLEXES, PLUS ELLE DOIT INTÉGRER LA PERSPECTIVE D'ÊTRE DÉSARMÉE AU MOINS TEMPORAIREMENT PAR LES EFFETS DES FRAGILITÉS NUMÉRIQUES.

L'État est d'ailleurs bien conscient du paradoxe qu'il y a à numériser toujours plus ses pratiques de sécurité alors même que le socle technique des technologies de l'information recèle une insécurité irréductible. Ce n'est pas sans raison que le législateur a, en 2012, renforcé la répression pénale des actes de fraude informatique en alourdissant les peines prévues aux articles 323-1 à 323-3 du Code pénal lorsque les infractions correspondantes (pénétration illicite dans un système ou atteintes à l'intégrité du système ou des données) présentent la circonstance aggravante d'avoir été commises « à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État[12] ». D'une certaine façon on peut affirmer que plus les administrations publiques dématérialisent leurs procédures, plus l'État (et les autres personnes publiques, à un moindre niveau) doit craindre de devenir la cible directe d'actions malveillantes. La création beaucoup plus récente de l'Opérateur des systèmes d'information interministériels classifiés (OSIIC) manifeste d'ailleurs le souci des plus hautes autorités publiques de durcir le cœur de leurs systèmes d'information dédiés à ses missions de défense et de sécurité nationale[13].

(8) Voir notamment Dejean (P.), Sartre (P.), 2015, « La cyber-vulnérabilité », *Études*, 7, p. 21-31 (qui parlent notamment de la « *fragilité native du numérique* »).
(9) Marx (G.), 1995, « Technologies de sécurité et société », *Cahiers de la sécurité*, n° 21 p. 14.
(10) Avis sur la proposition de loi (n° 1722) visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, Assemblée nationale, document n° 1830, 2 avril 2019, p. 11.
(11) V. notamment, une présentation du programme par la gendarmerie : Marzin (Y.), Lagrange (T.), 2016, « Neogend au cœur d'une démarche participative », *Revue de la gendarmerie nationale*, n° 255, 1er semestre, p. 73-78.
(12) Par l'article 9 de la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.
(13) Décret n° 2020-455 du 21 avril 2020 portant création d'un service à compétence nationale dénommé « opérateur des systèmes d'information interministériels classifiés ».

La technologisation brouille le cadre des missions de sécurité

La technologisation de la sécurité intérieure ne fait pas qu'introduire potentiellement des risques d'insécurité numérique dans les process opérationnels mis en œuvre par les services publics compétents, elle favorise également des déplacements conceptuels et opérationnels qui peuvent, à terme, remettre en cause les fondements d'une sécurité publique démocratique.

L'influence indirecte d'une logique techniciste affectant les pratiques humaines

De nombreux auteurs nous ont alertés depuis longtemps sur l'irrésistible « *autonomie de la technique*[14] », c'est-à-dire sur l'emprise indirecte que les développements technologiques induisent sur les pratiques et les mentalités, au-delà des seuls effets mécaniques efficaces que peut avoir la mise en œuvre d'un outil technologique. Il en va bien évidemment de même dans le domaine des technologies de sécurité.

Si l'on s'intéresse aux investigations pénales par exemple, on ne peut qu'être impressionné par la manière dont l'analyse des prélèvements ADN est devenue la « reine des preuves », tant et si bien qu'une enquête de police judiciaire sans prélèvements exploitables est le plus souvent considérée comme vouée à l'échec. Or, « *l'ADN fait face à des limites scientifiques, éthiques et juridiques*[15] » et une thèse de criminologie soutenue il y a quelques années concluait que souvent, « *les juges n'examinent pas de façon critique la preuve par ADN* » et que *« les principes de rationalité dans l'appréciation de la preuve par ADN ainsi que d'égalité des armes face aux expertises ADN semblent, de ce fait, ne pas toujours être respectés comme ils le devraient*[16] ».

En 1995 dans ces mêmes *Cahiers de la sécurité*, Bernard Gravet, alors directeur central de la Police judiciaire, reconnaissait déjà que « *la pire des choses serait que l'ensemble des détenteurs du savoir et des responsabilités en matière de police technique et scientifique puissent fonctionner en une sorte de circuit fermé, et se marginaliser, tant de l'intérêt général et des objectifs sécuritaires que de l'usage qui est fait au quotidien des moyens les plus sophistiqués et des techniques*[17] ».

Le développement de la vidéoprotection sur la voie publique est une autre manifestation de cette survalorisation de la technologie sur d'autres moyens de prévention. Les caméras numériques mises en réseau et reliées à un centre de supervision sont devenues un instrument incontournable des politiques de « *prévention situationnelle* », conformément à la doctrine anglo-saxonne développée à partir des travaux de Ronald Clarke[18].

Pourtant l'efficacité de cette technologie pour la prévention de la délinquance reste assez controversée[19]. Mais là aussi la disponibilité de l'outil a induit de nouveaux comportements non plus s'agissant de sa supposée fonction préventive mais plutôt de son utilisation *a posteriori* pour établir le déroulement de faits délictueux et identifier éventuellement leurs auteurs. Or, rien ne démontre que les images de vidéosurveillance renforcent réellement le taux d'élucidation des crimes et des délits. Interrogée en 2019 par un parlementaire, la Chancellerie a dû avouer qu'elle « *ne dispose pas de statistiques sur la part d'affaires élucidées grâce à la vidéoprotection*[20] » tandis que la Cour des comptes a été encore plus claire dans son tout récent rapport sur les polices municipales : « *Au vu des constats locaux résultant de l'analyse de l'échantillon de la présente enquête, aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation*[21] ».

---

(14) Sur l'importance de cette notion chez Jacques Ellul notamment, Vitalis (A.), 1994, « Informatisation et autonomie de la technique », *in* Troude-Chastenet (P.) (dir.), *Sur Jacques Ellul*, Ed. L'esprit du temps, p. 151.

(15) Ménabé (C.), 2020, « L'ADN, la reine des preuves imparfaites », *Médecine & Droit*, n° 164, octobre, p. 129-133.

(16) Joëlle Vuille, *Ce que la justice fait dire à l'ADN (et que l'ADN ne dit pas vraiment) - Étude qualitative de l'évaluation de la preuve par ADN dans le système judiciaire pénal suisse*, thèse pour le doctorat en criminologie, Université de Lausanne, 2011, p. 437-438 (thèse qui se conclut ainsi : « *il serait nécessaire de procéder à quelques aménagements afin de garantir que la science puisse continuer à aider la justice, c'est-à-dire à la servir plutôt qu'à l'asservir* », p. 461).

(17) Gravet (B.), 1995, « Police technique et scientifique et pratiques professionnelles », *Cahiers de la sécurité*, *op. cit.*, p. 31.

(18) Sur la prévention situationnelle, v. notamment Maurice Cusson, « Comment prévenir ? Les techniques et la méthode de la prévention situationnelle », *in* Cusson (M.), Dupont (B.), Lemieux (F.) (dir.), 2007, *Traité de sécurité intérieure*, Montréal, Hurtubise HMH, p. 413-428.

(19) V. Le Goff (T.), 2010, « Le faux et coûteux miracle de la vidéosurveillance », *Après-demain*, 4, p. 28-30 et plus récemment Mucchielli (L.), 2016, « À quoi sert la vidéosurveillance de l'espace public ? : le cas français d'une petite ville "exemplaire" », *Déviance & Société*, Médecine et Hygiène, 40 (1), p.25-50. Egalement son ouvrage : Mucchielli (L.), *Vous êtes filmés ! Enquête sur le bluff de la vidéosurveillance*, Paris, Armand Colin, 2018.

(20) Assemblée nationale, réponse ministérielle à la question n° 15585 d'Emmanuel Maquet, JO, 15 janvier 2019, page p. 409.

(21) Cour des comptes, *Les polices municipales* – Rapport thématique, octobre 2020, p. 70.

Mais aussi mal justifiée que soit cette course en avant de la vidéosurveillance, le « *paradigme du techno-solutionnisme*[22] » est toujours en marche, car désormais c'est du couplage des caméras vidéo installées dans l'espace public avec l'intelligence artificielle que l'industrie de la sécurité attend des résultats décisifs (et, rétroactivement, la démonstration tant attendue d'une réelle efficacité de ces dispositifs).

L'avenir seul dira si ce dopage de la surveillance vidéo par les algorithmes se fera sans altération grave de la vie privée des citoyens ni sans les risques de fausse identification dont la plupart des systèmes actuels sont encore largement affectés. Mais ce domaine de la vidéosurveillance publique nous montre déjà comment le recours à la technologie entraîne presque inévitablement la recherche d'une justification *a posteriori* qui interdit tout retour en arrière (même lorsque le législateur avait prudemment prévu une phase d'expérimentation).

Mais ce techno-solutionnisme sécuritaire a une autre dimension. Il renforce également l'incitation à la privatisation croissante des missions et des prestations de sécurité.

La technologie favorise la privatisation de la sécurité

Le lien entre technologie et implication de la sécurité privée est largement établi. Écrivant sur « privatisation et technologie » Jean-Paul Brodeur considérait déjà en 2003 que la « *prédominance de la technologie* » était le « *phénomène dont la signification nous apparaît la plus profonde* » et que « *le changement crucial résidait non pas dans la croissance du personnel de la sécurité privée, mais dans la somme des revenus générés par la vente d'équipements de technologie de sécurité*[23] ».

Les raisons de ce phénomène sont assez simples à identifier. Tout d'abord, la puissance publique, forte en hommes et en droit, est presque entièrement démunie en matière technologique. La plupart de ses moyens industriels et techniques propres ont été soit privatisés (ce fut le cas des « arsenaux » de la direction générale de l'Armement (DGA) dans les années 1980-90 ou de l'opérateur de télécommunications France Telecom devenu la société Orange) soit réduits à la portion congrue (s'agissant des services techniques et des centres d'expertise d'État). Conformément à la « *gouvernance libérale*[24] » du domaine de la sécurité, ce sont donc les entreprises privées de technologie qui sont seules à même de fournir aux services de l'État les systèmes dont ils ont besoin.

Mais comme les technologies sont largement duales et transnationales, on est dans ce domaine de moins en moins dans une politique de la demande (publique) mais plutôt de l'offre (privée). Ce n'est plus nécessairement le cahier des charges de l'administration qui entraîne un développement spécifique réalisé par un prestataire extérieur, mais plutôt la disponibilité au catalogue d'une entreprise, française ou étrangère, qui induit le choix de retenir la technologie présente sur le marché. L'un des exemples, assez choquant dans son principe, fut le choix par la Direction générale de la sécurité intérieure (DGSI) du logiciel Palantir pour gérer les données du renseignement intérieur, malgré les liens avérés du fournisseur américain avec les services de renseignement de Washington.

De la vente d'équipement à la fourniture de services, puis à la sous-traitance et à la délégation indirecte d'une partie des activités de sécurité il n'y a qu'un pas, dont a témoigné d'une certaine manière l'exemple du marché confiant jusqu'en 2024 la gestion de la plateforme nationale des interceptions judiciaires (PNIJ) à la société Thalès, qui avait soulevé certaines interrogations. En effet, on comprend que les obstacles juridiques et statutaires qui interdisent de déléguer les missions régaliennes de défense et de sécurité publique[25] sont facilement contournables par un recours à une prestation technologique ou simplement matérielle confiée à un prestataire privé.

Cette privatisation de la sécurité soutenue, voire accélérée par le recours à des technologies de sécurité largement issues de la révolution numérique ne se limite ni à la fourniture de caméras aux collectivités territoriales ni même à numériser les chaînes de traitement des services de police ou de la justice pénale. Elle touche également le domaine du renseignement de sécurité nationale qui, notamment sous l'effet du dopage budgétaire lié à la

(22) Pour reprendre une formule d'Evgeny Morozov issue de son livre (E. Morozov, *To Save Everything, Click Here : The Folly of Technological Solutionism*, Public Affairs, 2013), déjà appliquée à la vidéosurveillance par Hubert Guillaud (v. notamment sa tribune « Vidéosurveillance : paradigme du technosolutionnisme », blog Internet Actu, 2 juin 2018).

(23) Brodeur (J.-P.), 2003, *Les Visages de la police : Pratiques et perceptions*, Nouvelle édition [en ligne], Montréal, Presses de l'Université de Montréal, p. 219 et p. 222.

(24) V. Ayse Ceyhan, *op. cit.*

(25) Bien que ceux-ci aient été rappelés par le Conseil constitutionnel en 2011 lorsqu'il censura un article de la LOPPSI 2 qui permettait de déléguer à une société de vidéosurveillance le visionnage de la voie publique (Cons. Constit., *10 mars 2011, n° 2011-625 DC*).

réévaluation de menace terroriste, devient un grand utilisateur de moyens numériques de surveillance. Comme c'est déjà bien le cas aux États-Unis, se constitue progressivement ce que l'on peut appeler un « *complexe industriel du renseignement*[26] », fait de relations étroites et secrètes[27] entre les services de l'État et un écosystème d'entreprises intervenant comme fournisseurs mais aussi parfois comme sous-traitants potentiels de certaines prestations.

Dans ce secteur très sensible du renseignement également, la logique technicienne s'impose par-delà une appréciation rationnelle de l'efficacité réelle des outils techniques mobilisés[28]. Un exemple récent concerne la technique de renseignement généralement dénommée « algorithme » (et qui avait été autorisée à titre expérimental pour lutter contre le terrorisme par l'article L.851-3 du Code de la sécurité intérieure jusqu'à fin 2020). La délégation parlementaire pour le renseignement évoque bien dans son rapport des « *résultats encore décevants* » et que « *ce dispositif technique n'a pas encore donné tous les résultats escomptés*[29] ». Pour autant, il est question non seulement de proroger une nouvelle fois pour quelques mois ce dispositif (ce qui peut se comprendre, compte tenu du regain des actes de terrorisme), mais également d'envisager une future extension possible de son emploi (en élargissant le type de données qui seraient analysables[30]). En d'autres termes, une fois mis en place un outil, il est peu envisageable de s'en défaire et si ses résultats s'avèrent insuffisants, il convient plutôt de rechercher une manière de le renforcer et de lui trouver une nouvelle justification.

En conclusion, on rappellera ce que relevait Gary Marx dans le numéro des *Cahiers de la sécurité* de 1995 déjà cité : « *le recours à la technologie est trop souvent légitimé par une représentation réductrice et unilatérale de ses effets et objectifs. On tend ainsi à perdre de vue – à dessein ? – le fait que les conséquences de l'application concernent tout autant les destinataires que les utilisateurs*[31] ». Ce faisant, il introduisait dans le débat les grands absents de tout ce mouvement de technologisation de la sécurité qui sont les citoyens, destinataires mais aussi objets des pratiques techno-sécuritaires (puisque la technologie est par nature invasive pour pouvoir traiter préventivement la masse plutôt que pour surveiller seulement *ex post* le délinquant identifié). Le propre d'un développement endogène des outils techniques mis en œuvre par les forces de sécurité est qu'il ignore largement la délibération démocratique, et ce pour une double raison : d'un côté, parce que toutes les questions de sécurité sont aisément recouvertes du voile du secret, mais aussi d'un autre côté parce que la technicité des solutions proposées semble empêcher un débat citoyen.

Tout au plus est-il possible, dans notre tradition administrative française, de compter sur quelques autorités administratives indépendantes pour maintenir un certain niveau d'expertise autonome et de recul critique. On a vu ainsi le Défenseur des droits (héritier de la commission de déontologie de la sécurité) soulever des objections à l'usage de certains équipements de maintien de l'ordre par les forces de maintien de l'ordre[32]. C'est également le mandat de la plus récente Commission nationale de contrôle des techniques de renseignement (CNCTR) de veiller à ce que les services de renseignement n'outrepassent pas le périmètre d'usage des techniques numériques intrusives que le Code de la sécurité intérieure leur autorise[33]. Mais c'est aussi l'un des rôles de la très sollicitée Commission nationale de l'informatique et des libertés (CNIL) qui n'hésite pas régulièrement à formuler des réserves ou des critiques à l'encontre de nouveaux projets numériques susceptibles de mettre en cause la protection des données à caractère personnel, y compris dans le champ des activités régaliennes touchant la sécurité publique[34]. À l'évidence, ces différentes autorités manquent encore de moyens humains et techniques pour suivre la course vaine vers la « *société de sécurité maximale* » que décrivait déjà G.

(26) Le Voguer (G.), 2014, « Le "complexe industriel" du renseignement américain et la préservation des libertés », *Politique américaine*, 2, n° 24, p. 29.
(27) Rappelons que la directive 2009/81 du 13 juillet 2009 relative aux marchés publics de défense et de sécurité exclut de son champ d'application b) les « marchés destinés aux activités de renseignement » (art. 13(b)).
(28) On se rappellera de la formule inquiète (inquiétante) de Patrick Calvar, alors directeur général de la Sécurité intérieure, intervenant le 22 mars 2017 dans un colloque organisé par la Commission nationale de contrôle des techniques de renseignement (CNCTR) et estimant qu'en matière de contrôle des services « *seule la machine pourra arrêter la machine* » (cité in B. Warusfel, « Acquis et limites de l'encadrement du renseignement : premier bilan d'étape de la réforme », publié sur le site hestia.hypotheses.org).
(29) Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020, 11 juin 2020, document AN n° 3097/ Sénat n° 506, p. 70-71.
(30) Rapport de la mission d'information commune sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement, Assemblée nationale, doc n° 3069, 10 juin 2020, p. 191.
(31) Gary Marx, 1995 précité.
(32) V. notamment : Défense des droits, Rapport sur le maintien de l'ordre au regard des règles de déontologie, décembre 2017, p. 25-29, p.12.
(33) V. son dernier rapport annuel : CNCTR, 4e rapport 2019, La documentation Française, 2020.
(34) V. par exemple, sa délibération n° 2018-342 du 18 octobre 2018 portant avis sur le système d'authentification électronique ALICEM (et émettant des réserves sur certains aspects de ce projet gouvernemental utilisant la reconnaissance faciale).

Marx il y a trente ans[35]. De même leur composition assez technocratique aurait intérêt à mieux s'ouvrir à l'expertise académique indépendante et aux relais de la société civile. Mais surtout, on peut imaginer que plutôt qu'agir chacune de manière isolée, il y aurait un intérêt public majeur à ce que le droit mais aussi la pratique favorisent une mise en réseau de ces instances de contrôle autour d'un objectif commun, celui de la régulation démocratique des technologies.

L'heure nous y pousse, car les perspectives immenses qu'ouvrent tant l'intelligence artificielle que l'Internet des objets (IoT) risquent de nous de faire tomber – surtout et y compris dans le secteur sécuritaire – dans une « *gouvernementalité algorithmique*[36] » avec tout ce que cela pourrait avoir comme conséquence en termes de restrictions des libertés fondamentales et de basculement vers une société du soupçon cherchant à détecter la supposée « dangerosité » par la surveillance de masse[37].

Cette régulation de la technologie ne devrait pas s'interdire de prescrire chaque fois que cela est nécessaire de réglementer – voire de prohiber – la mise en œuvre de certains moyens techniques reconnus comme intrinsèquement attentatoires aux libertés. De même que nous connaissons sur le plan national la prohibition des armes létales (et des matériels de guerre) mais aussi de certains moyens d'espionnage numérique[38], l'Union européenne s'apprête à étendre les restrictions à l'exportation aux technologies de surveillance numérique pouvant mettre en cause la sécurité humaine[39]. De son côté, la Cour de justice vient de remettre en cause la possibilité pour les États-membres d'imposer une rétention généralisée et indifférenciées des données de connexion par les opérateurs de communication[40]. C'est donc aussi, et surtout, au niveau de l'Union européenne (et sous le contrôle indirect de la Cour européenne des droits de l'homme), qu'il importe de construire les bases d'une nouvelle gouvernance démocratique des technologies numériques en y distinguant clairement certaines technologies de souveraineté dont la mise en œuvre serait réservée aux autorités publiques et particulièrement contrôlée par des contre-pouvoirs efficaces. Par ailleurs il conviendrait d'établir un cadre d'usage par les entreprises et les citoyens des moyens privés de sécurité qui leur garantisse un niveau de robustesse technique et d'intégrité, comme le règlement eIDAS de 2014 a commencé à le faire s'agissant de la fourniture des services numériques « de confiance » en y introduisant un certain contrôle des prestataires par les autorités nationales de sécurité des systèmes d'information[41].

C'est à ce prix que l'on pourra peut-être stopper la dérive actuelle dans laquelle l'offre technologique privée entretient la quête magique (et dangereuse) d'une sécurisation automatisée d'un monde débarrassé de tout risque et de toute menace. Seule une régulation politiquement justifiée et juridiquement organisée peut nous permettre de reprendre le contrôle sur des technologies qui – livrées à elles-mêmes et entre les mains des seuls opérationnels – seront plus ressenties comme des instruments d'intrusion et de violence que comme des outils de confiance ■

(35) Marx (G.), 1988, « La société de sécurité maximale », *Déviance et société*, Vol. 12, n°2, p. 147-166.
(36) Pour reprendre le terme et le concept développé par A. Rouvroy (v. notamment Rouvroy (A.), Berns (T.), 2013, « Gouvernementalité algorithmique et perspectives d'émancipation : Le disparate comme condition d'individuation par la relation ? », *Réseaux*, 1, n° 177, p. 163-196).
(37) Le nouveau mécanisme de « scoring social » chinois fait figure d'épouvantail en la matière mais aussi d'une forme de préfiguration.
(38) V. notamment les articles 226-3 et 323-3-1 du Code pénal.
(39) La Commission a notamment annoncé, en novembre 2020, un accord avec le Parlement européen sur une prochaine révision en ce sens du règlement 428/2009 sur le contrôle du commerce et des transferts des biens à double usage.
(40) CJUE, 6 octobre 2020, aff. jointes C-511/18, C-512/18, C-520/18 et aff. C-623/17.
(41) Règlement 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques.