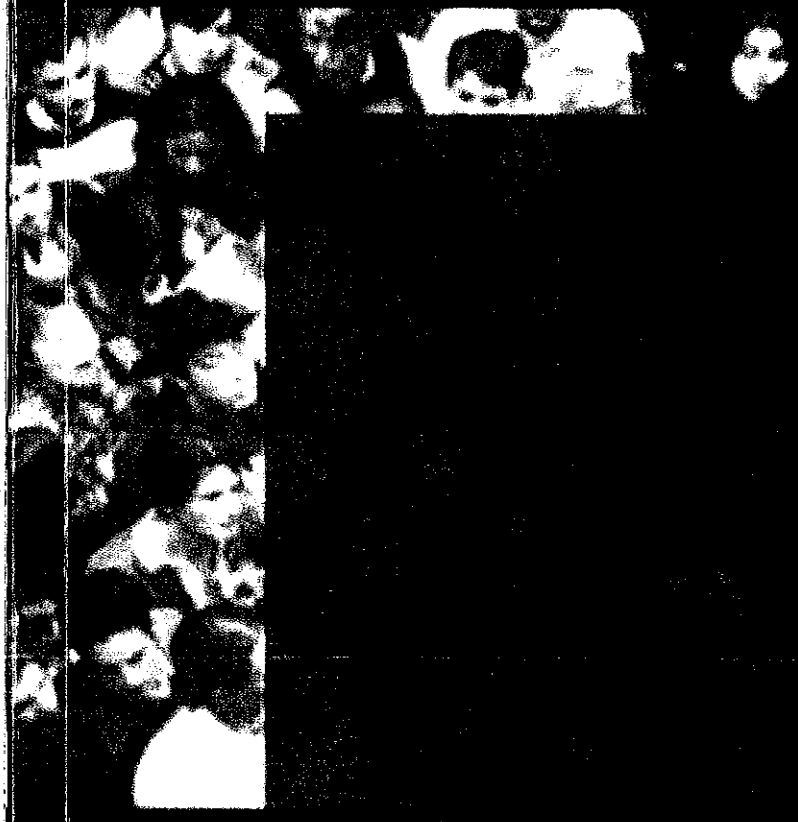
problèmes

Contrôles et surveillances dans le cyberespace



N° 988 • Septembre 2011

Frédéric Ocqueteau
Daniel Ventre

La **documentation** Française

Contrôles et surveillances dans le cyberespace

• Septembre 2011

Dossier réalisé par
Frédéric Ocqueteau

Sociologue et juriste, directeur de recherche au CNRS (CESDIP, Centre de recherches sociologiques sur le droit et les institutions pénales)

Daniel Ventre

Ingénieur CNRS, chercheur au CESDIP (Centre de recherches sociologiques sur le droit et les institutions pénales)

Avant-propos

À l'heure de la mondialisation des risques, des menaces et des vulnérabilités, si rien n'a véritablement changé pour les États démocratiques dont la vocation demeure de les combattre ou de les conjurer quitte à empiéter sur la liberté des peuples ou des citoyens (1), en revanche, tout invite à devoir repenser de fond en comble l'exercice de leurs missions régaliennes de surveillance et de contrôle. À mesure que se répandent les outils technologiques mobilisés par les puissances hégémoniques pour dominer leurs concurrents dans le domaine économique ou militaire, notamment par la meilleure maîtrise de l'information possible, cet enjeu devient en effet gros de conséquences quant à la manière de penser le destin collectif du monde régulé.

L'explosion et l'emprise des technologies de l'information et de la communication par le biais de l'internet, les possibilités de plus en plus sophistiquées de traçages électroniques (2) aussi bien des particuliers que des groupes sociaux spécifiques, l'essor fulgurant des systèmes biométriques qui prétendent définir « qui est qui » sans aucun risque d'erreurs..., tous ces phénomènes subvertissent progressivement les rapports de pouvoir et de domination traditionnels. À chaque fois qu'apparaissent sur le marché de nouvelles technologies de contrôle, de surveillance et de protection, et que se répandent le besoin et la demande afférents parmi les usagers potentiels – États, entreprises, groupes de la société civile ou particuliers isolés –, se nouent autant de nouvelles et complexes interdépendances de pouvoir potentiellement collusives ou conflictuelles.

Les sciences humaines soucieuses d'en rendre compte sont mises à rude épreuve et s'aperçoivent ne plus pouvoir embrasser la totalité du réel. Elles sont de surcroît de plus en plus souvent confrontées aux démentis de celui-ci, au fur et à mesure de la mondialisation des flux, du passage de l'informatique au numérique et, peut-être surtout, de l'accélération du temps (3). S'agissant du contrôle social à l'ère de la cybernavigation au sein de l'infosphère (4), personne ne croit plus vraiment à la consistance des métaphores du *Big brother* ou du *Panopticon*, excepté quand le besoin se fait impérieux de disposer de ces épouvantails pour décrire « ce qui aurait changé » en l'espace d'une seule génération.

Macro, meso, micro : un emboîtement des niveaux d'analyse

La modestie est donc de rigueur dans la description inépuisable de la réalité, mais une audace minimale doit néanmoins permettre d'établir

notes

1 Voir notamment « Polices et politiques de sécurité », *Problèmes politiques et sociaux* n° 972, 2010.

2 Voir notamment « Traçage électronique et libertés », *Problèmes politiques et sociaux* n° 925, 2006.

3 H. Rosa, *Accélération, une critique sociale du temps*, Paris, La Découverte, 2010.

4 Une sphère imaginaire enveloppant la planète parcourue d'incessants flux d'informations au sein de laquelle vivent et coexistent les humains et les organismes informationnels (*orins*), participant tout autant de la biosphère que de la logosphère. Cf. J.-G. Ganascia, *Voir et pouvoir : qui nous surveille ?*, Paris, Les Essais du Pommier, 2009, p. 149.

des liens entre les différents niveaux de la pensée de la surveillance et du contrôle. Un fil rouge semble réunir ces niveaux : la tension permanente entre tentations sécuritaires/autoritaires et tentations libertaires. Outre les domaines traditionnels du contrôle et de la surveillance du complexe pénal qui n'ont en rien disparu, se dessinent aussi, au sein du cybermonde, des lignes de fractures entre le ressenti d'une trop grande oppression par le haut qui secrète un travail de sape par le bas, et inversement, la perception de trop grandes avancées dans le domaine des libertés qui secrète des demandes de plus grande fermeté.

Les instances tierces qui arbitrent entre les citoyens et les États montent en puissance, telle la Commission nationale de l'informatique et des libertés (CNIL), et sont sommées de déterminer le point d'équilibre, révisable à tout moment, entre ces tendances contradictoires, notamment dans les démocraties dont certaines tendent à s'appuyer sur l'intérêt général pour imposer aux citoyens des projets sécuritaires potentiellement dangereux pour les libertés. Les discours justifiant les nouvelles modalités de surveillance et de contrôle des individus par la volonté de les rassurer ou de les protéger sont toujours susceptibles d'être remis en cause par des actions de contestation éclatées, de moins en moins bien unifiées. Par conséquent, à quelque niveau que l'on situe l'analyse, il faut concomitamment penser les germes du désordre et les soucis de remise en ordre. Et cela, dans des contextes de pouvoir asymétriques, de légitimation de pouvoirs instables, en puisant dans un nouveau répertoire de métaphores qui remplacent les plus anciennes. Il en est ainsi par exemple de l'horizontalité des réseaux de communication, d'influences, des regards *péri-optiques* (5), de la *sous-veillance* (6), qui viennent supplanter les rapports de pouvoir verticaux.

À l'heure des identités multiples, il faut revisiter de fond en comble les anciennes notions de la vie privée, renouveler les approches de sa protection contre les supposées intrusions illégitimes des technologies. Il faut réinterroger les rapports de l'individu exhibitionniste au citoyen de verre, les nouveaux rapports de l'homme à son corps, incarné et virtuel. Il faut analyser les nouvelles formes de contestation, de résistance ou d'adhésion, actives et passives, à tous les pouvoirs institués. Il faut questionner les pratiques d'auto-contrôle et de gestion de leurs identités multiples que mettent en œuvre les individus, et, en même temps, la demande parfois anxieuse de sécurité qu'ils émettent pour les autres ou pour se faciliter la vie dans tous les aspects du quotidien (vie domestique, scolaire, professionnelle, loisirs...).

Mais il importe aussi de comprendre que le niveau micro est conditionné par le contrôle et la surveillance à l'œuvre au niveau macro, celui des États et des entreprises, où s'est toujours livrée une guerre de la communication entre les puissances, aujourd'hui déplacée dans le cyberespace. Cette dimension stratégique façonne les perceptions et les conditionnements des citoyens dans tous les moments de leur vie domestique, professionnelle et publique. Ces citoyens s'opposent, avec de plus faibles moyens – mais

notes

5 M. Lianos, *Le nouveau contrôle social : toile institutionnelle normative et lien social*, Paris, L'Harmattan, 2001.
6 J.-G. Ganascia, *op. cit.*

qui peuvent aussi être redoutables (pensons aux hackers) –, aux abus des positions dominantes. Tous, forts et faibles, peuvent s'approprier l'information et le renseignement afin d'obtenir une plus grande transparence sur les intentions des uns et des autres... Si les puissants poursuivent le rêve de tout savoir sur les masses pour mieux les contrôler et influer leurs croyances et leurs actes, les masses ne sont pas toujours apathiques. Les formes de résistance et de révolte sont nombreuses. D'aucunes prétendent parfois découvrir ce que les autorités leur cachent en dépit de ce qu'elles affirment vouloir leur apporter.

Le présent dossier s'efforce d'ordonner dialectiquement cette thématique foisonnante par le biais de trois entrées. La première (les individus) se demande avec quels outils et comment il faut repenser la défense de la (ou des) vie(s) privée(s) contre l'intrusion légitime – par exemple en matière de protection – ou illégitime des institutions. La deuxième (les États) cherche à analyser comment se remodèle la problématique du secret et la maîtrise de l'information à l'heure de la cyberguerre dans le cyberespace. La troisième (les groupes contestataires) apporte des clés de lecture sur les mécanismes de résistance aux options trop axées sur la sécurité des projets de contrôle et de surveillance des populations.

Repenser le contrôle des individus par les tactiques d'autocontrôle

L'individu contemporain est caractérisé par les philosophes comme un « citoyen de verre », plongé dans un monde de capteurs et de puces qui tracent et retracent le moindre des faits et gestes de sa vie sociale et privée. L'un des enjeux majeurs est de savoir si, dans ce nouveau monde, la vie privée naguère conçue comme un droit à ne pas être importuné a encore un sens. Certains se demandent si l'impudeur des internautes exposant leur intimité est le signe que l'abolition de la frontière entre vie publique et privée est pleinement assumée ou bien celui de nouvelles stratégies de surveillances interpersonnelles. Face à l'impressionnant succès des réseaux sociaux (7), parmi les *digital natives* notamment, la controverse s'accroît au sujet des paradoxes de la défense de l'identité. Les uns estiment que les comportements seraient plutôt guidés par la gestion personnelle du risque, voire une meilleure aptitude à intérioriser le processus de fouille permanente des données dans la construction de son propre espace personnel. Des économistes de la rationalité mobilisent différents paradigmes pour expliquer les prétendus illogismes des comportements, en avançant notamment l'incomplétude de l'information, la rationalité limitée ou les distorsions psychologiques (8). Les défenseurs d'une conception modernisée de la vie privée, préoccupés notamment par le potentiel liberticide des techniques de la vidéosurveillance (9), convoquent le juriste américain Daniel Solove pour faire un sort à la naïveté de la thèse selon laquelle « on ne saurait être suspecté quand on n'a rien à se reprocher ».

notes

7 Voir D. Cardon, « Internet et réseaux sociaux », *Problèmes politiques et sociaux* n° 984, mai 2011.
8 Voir sur cet aspect l'extrait de F. Rochandelet.
9 Sur la vidéosurveillance, voir la 3e partie de « Polices et politiques de sécurité », *Problèmes politiques et sociaux* n° 972, mai 2010. Cette question ne sera donc pas traitée ici.

Alors que l'être humain n'est pas assimilable à son corps biométrique, tout se passe pourtant comme si la force de la culture de l'identification biométrique était telle que le corps serait en somme devenu un *mot de passe*. Sur les lieux de travail, des juristes craignent que le recours à l'identification biométrique, et plus généralement à la surveillance, ne fasse l'objet d'un consentement forcé des salariés (10), tandis que des anthropologues estiment qu'à l'école, par exemple, la diversité de ses usages dans le cadre des cantines scolaires attesterait bel et bien de la réalité de la « société de contrôle » naguère prophétisée par Gilles Deleuze.

La légitimité des organismes similaires à la CNIL se renforce en Europe à mesure que cette autorité et ses homologues du G 29 apparaissent comme des tiers acteurs décisifs pour se préparer aux évolutions des technologies numériques intrusives, et statuer sur leur caractère positif ou néfaste. Autrement dit, pour arbitrer entre principes de finalité et de proportionnalité dès qu'apparaît sur le marché une technologie nouvelle. L'intensité du consentement exprimé et le degré d'intrusivité sont en effet deux dimensions de plus en plus problématiques à prendre en compte. Ainsi, concernant les technologies de géo-localisation, la CNIL distingue entre le consentement décalé et le consentement délégué pour les personnes vulnérables (11). Mais face à l'omniprésence des puces RFID (*Radio Frequency Identification*) annonçant un internet des objets ou un internet ubiquitaire – autrement dit la fin de la solitude et du secret –, un droit au silence des puces est désormais posé.

Repenser la maîtrise du secret et de l'information dans un contexte de « cyberguerre »

Au tournant des années 1990, la chute du mur de Berlin et l'effondrement de l'empire soviétique semblaient ouvrir de nouvelles perspectives à l'humanité. Les deux grands blocs autour desquels l'histoire du monde s'était organisée depuis la fin de la Seconde Guerre mondiale cédaient leur place à un environnement global, à la mondialisation de l'économie et des échanges. Cette mondialisation et les rêves de croissance qu'elle portait en elle s'appuyaient sur les nouvelles autoroutes de l'information, gages d'un monde ouvert, sans contraintes. Mais la mondialisation était aussi le lieu de la course à la domination, qu'il s'agisse de la conquérir ou de la préserver. Le cyberespace portait donc en lui les germes du conflit : car dominer grâce au cyberespace signifiait aussi chercher à écarter les adversaires de cette course à la domination.

Le cyberespace est alors devenu un nouvel espace d'affrontements. La première guerre du Golfe démontra toute la puissance conférée à un État capable de dominer l'espace informationnel. Depuis lors, les grandes puissances se sont lancées dans une course effrénée à l'informatisation des armées, des services de renseignement, des gouvernements, des sociétés. Maîtriser l'information, maîtriser l'espace informationnel, et bien entendu le cyberespace, est devenu l'un des enjeux majeurs des États modernes, source

notes

10 Par exemple, G. Deharo, « L'identification biométrique dans l'entreprise », et C. Strugala « Développement de la biométrie et droit au respect de la vie privée : un droit lacunaire ?, *in* A. Ceyhan et P. Piazza (dir.), *L'identification biométrique, champs, acteurs, enjeux et controverses*, Paris, MSH, 2011.

11 Voir l'extrait d'A. Türk.

de conflits entre acteurs de nature diverse : acteurs étatiques (autorités, militaires, renseignements), ou non étatiques (civils, hackers, hacktivistes, terroristes, etc.). Pour l'État, l'objectif est de maîtriser le cyberespace, que ce soit pour dominer le reste du monde, ses adversaires et ses concurrents, voire ses propres citoyens. En raison de la croissance considérable du cyberespace, au moins dans les pays industrialisés, c'est pratiquement toute la société qui se trouve liée au cyberespace : chacun se connecte à l'internet ; chacun ou presque utilise la téléphonie mobile ; les entreprises et les administrations multiplient les formes de leur présence sur la toile. De fait, la masse de données produites dans le monde est devenue une source de renseignements inépuisable que savent exploiter les États mais aussi les acteurs non étatiques. S'observer, s'espionner est la règle.

Mais si un État tire profit de ces ressources nouvelles, il est aussi l'objet d'attaques de la part d'autres États et acteurs non étatiques, adversaires et alliés. Les cyberattaques, à l'image de celles qui ont touché le ministère des Finances français au début de l'année 2011, sont symptomatiques de ce nouveau contexte qui voit se multiplier les intrusions à des fins d'espionnage dans les systèmes d'information des États, des entreprises et même des citoyens. L'État est contraint à prendre des mesures strictes de sécurisation de ses propres systèmes d'information. Mais l'approche est nécessairement plus large : il lui faut veiller à la défense des intérêts économiques, du patrimoine scientifique, des échanges diplomatiques, de la culture même. L'ANSSI (Agence nationale de la sécurité des systèmes d'information) a été créée en 2009, dans le prolongement des recommandations du Livre Blanc de 2008 (12). L'une de ses missions essentielles est de protéger la France contre les cyberattaques qui pourraient mettre en péril les intérêts de la nation. La défense de la souveraineté a conduit des États à mettre en place des systèmes de collecte et traitement des données (concernant par exemple les flux migratoires) ; d'autres encore n'hésitent pas à faire appel de manière plus ou moins officieuse à des pirates informatiques en soutien aux activités policières et de renseignement.

Dans le contexte concurrentiel international, en situation de paix, de crise ou de conflits ouverts, les États sont désormais appelés à utiliser le cyberespace comme nouvelle dimension de leurs actions. La lutte pour la domination sur la scène internationale passe désormais par le cyberespace, qui est un espace public contesté. Maîtriser le cyberespace impose de lutter pour assurer sa protection, sa stabilité, sa défense. Les États, les armées, les agresseurs et les défenseurs, rêvent depuis le début des années 1990 de transparence (tout voir, tout savoir du monde), d'invisibilité (pouvoir observer, analyser, agir en étant indétectable, échapper à la surveillance adverse), d'immédiateté (disparition de la notion de temps), d'effacement des distances (être capable de voir et frapper au-delà de l'horizon). Ces utopies sont inscrites dans les doctrines de guerre de l'information formulées depuis les années 1990 et s'affirment pour certaines dans les premières formes de cyberguerre (recours aux capacités cybernétiques pour mener des opérations agressives dans le cyberespace), en ce début de XXIe siècle. La

note

12 *Défense et sécurité nationale. Livre blanc*, préface de Nicolas Sarkozy, vol. 1 et 2, Paris, Odile Jacob/La Documentation française, 2008.

multiplication des capteurs dans toutes les dimensions accroît les capacités de renseignement. Mais la technologie demeure encore incapable de traiter la masse inépuisable d'informations produites. La présence des États, des armées, des entreprises et des citoyens dans le cyberespace est indispensable à l'acquisition de la puissance. Elle est de fait aussi l'une des sources majeures de l'insécurité qui peut peser sur tous ces acteurs.

Repenser les stratégies de résistance à un contrôle oppressif des populations

Il est clair que les modalités de surveillance et de contrôle déployées par certains États sur des catégories spécifiques de populations ou des individus réputés « à risque » ne peuvent continuer à être pensées comme de purs effets d'oppression justifiés par les nécessités de la protection collective. Nos schémas de pensée traditionnels demandent à être fondamentalement remis en cause à cet égard.

À partir d'analyses mieux assises sur les faits, ce dossier montre comment le réalisme exige de rester plus en phase avec la complexité de questions ouvertes qui ne peuvent préjuger des orientations futures d'une histoire en train de s'écrire : les modalités actuelles du contrôle ne peuvent plus être pensées dans des finalités uniques et totales. Il convient notamment d'en finir avec la figure du Panoptique qui a trop longtemps servi de métaphore facile pour rendre compte de la nature intime d'un prétendu contrôle social à visée disciplinaire qui nous gouvernerait tous. Cette métaphore est devenue obsolète. On commence plutôt à accepter l'idée que, malgré leurs tentatives incessantes pour contrôler l'ensemble des dérives de l'internet, les États n'y parviendront jamais complètement eu égard à l'architecture même du réseau. En dépit des intentions stratégiques affichées par les nations les plus puissantes d'utiliser le cyberespace à des fins de domination, les faits montrent que les capacités réelles sont rarement au rendez-vous. Preuve en a été donnée par la Chine lors de la crise de Xinjiang en 2009. Les spécialistes, et même les plus hostiles aux thèses libertaires, sont bien obligés de reconnaître les fragilités de la volonté de puissance et de contrôle, à partir notamment du coup de tonnerre qu'a constitué *l'affaire WikiLeaks* (13). On peut en inférer que la curiosité de la blogosphère l'emportera toujours sur la volonté des États de cacher ce que la diplomatie aurait intérêt à vouloir tenir secret. Si le personnage de Julian Assange reste éminemment controversé, la presse internationale n'a pas eu trop d'états d'âme à révéler au monde entier ce qu'elle a pu décrypter des données brutes qui ont été rendues publiques sur le site WikiLeaks.

Nous ne devons pas nous montrer naïfs pour autant : si une guerre de l'information reste une réalité tangible, il vaut mieux se poser les bonnes questions à son sujet. Quelles que soient les solutions technologiques qui s'imposent pour améliorer les systèmes de sécurité de l'information, économistes et industriels nous apprennent que les

note

13 Voir les extraits de F.-B. Huyghe et de A. Rusbridger.

rapports de concurrence économique dans la promotion des technologies de contrôles et d'identification continuent à dominer macro structurellement la marche du monde. Par exemple, les solutions de contrôle biométriques qui s'imposent partout (cartes d'identité biométriques) montrent que les industriels des États-Unis d'Amérique auraient pour l'instant gagné une manche sur ceux de l'Europe.

Ce dossier explore également les foyers de résistance aux États désireux de contrôler de manière absolue et en temps réel l'identité des territoires, des hommes et les flux. Car cette ambition étatique provoque immanquablement une opposition de la part de la « société civile », qui développe des logiques de subversion tout aussi pérennes que le sont les stratégies de lutte contre les dérives engendrées par la (trop grande ?) liberté des internautes. Ce sont alors des figures d'horizontalisation des rapports d'interdépendance et de conflit autour du contrôle et de la surveillance qui se dessinent, plutôt que des figures d'États dominants et de populations dominées.

Si la maîtrise du cyberespace, depuis son apparition, a toujours été un enjeu de lutte entre internautes et États, c'est bien parce que reste enracinée la certitude que personne ne devrait pouvoir s'approprier définitivement le cyberespace. Des ONG y veillent de leur côté, et font un point permanent sur les « bonnes pratiques » des États pour garantir la liberté laissée aux réseaux sociaux du Web 2.0. Cette tension n'est au demeurant conceptuellement intelligible que parce que nous disposons désormais de plusieurs paradigmes capables de rendre compte de l'enjeu, à commencer par l'une des métaphores alternatives les plus prometteuses, celle de l'utopie réalisée du *Catopticon* : celui-ci désignerait le regard venu d'en bas et la sous-veillance, qui vient du dessous, par opposition au regard de l'autorité, autrement dit à la surveillance, qui vient du dessus.

La défense relookée de la vie privée (14) reste un enjeu ultime pour les défenseurs des intérêts des internautes. Certains s'attachent à détailler et à faire connaître les moyens de déjouer la traçabilité de la navigation sur internet. D'autres analysent comment des mobilisations collectives sont parvenues à faire reculer des projets gouvernementaux jugés dangereux pour les libertés. D'autres encore montrent que des stratégies de résistance par l'anonymisation collective dans le cyberespace peuvent avoir raison de régimes autoritaires, comme récemment en Tunisie. On peut penser qu'un certain activisme médiatique contre le secret remportera des succès tant que les sphères du journalisme professionnel et celles des mobilisations informationnelles s'enrichiront mutuellement plutôt que d'agir en concurrence. Le besoin de disposer de relais d'opinion ou de lobbys efficaces reste en effet essentiel pour préserver l'équilibre des pouvoirs de demain, et nous permettre de continuer à vivre en démocratie.

note

14 Cf. les conseils de J.-M. Manach en direction des jeunes, *La vie privée, un problème de vieux cons ?*, Paris, Fyp éditions., 2010.

Frédéric Ocqueteau
Daniel Ventre