tic&société

Vol. 10, N° 1 | 2016
Contrôle social, surveillance et dispositifs numériques

Contrôle social et techniques numériques

Approche sociohistorique

Dominique Carré et Jacques Vétois

Éditeur
Association ARTIC

Édition électronique
URL : http://ticetsociete.revues.org/1973

Référence électronique
Dominique Carré et Jacques Vétois, « Contrôle social et techniques numériques », *tic&société* [En ligne], Vol. 10, N° 1 | 1er semestre 2016, mis en ligne le 24 octobre 2016, consulté le 06 novembre 2016. URL : http://ticetsociete.revues.org/1973

Contrôle social et techniques numériques

Approche sociohistorique

Dominique Carré et Jacques Vétois

Introduction

1 De tous temps, les sociétés ont mis en place sous des formes différenciées et suivant les époques des méthodes, des pratiques et des techniques pour observer, surveiller et ainsi contrôler des individus ou des groupes sociaux[1], pour éviter toute déviance à des normes sociales instituées (mœurs), pour prévoir toute révolte ou contestation des pouvoirs en place (délits d'opinion) ou encore pour prévenir de certaines actions (manifestations, grèves, attentats). Cela n'est guère nouveau. A. Mattelart et A. Vitalis (2015) étudiant le profilage des populations montrent que chaque travailleur se devait d'avoir, aux 18e-19e siècles, un livret ouvrier. Livret qui participait déjà au « profilage » de la population ouvrière.

2 Il ne s'agit pas ici de proposer à travers les siècles une rétrospective sociohistorique du développement du contrôle social, mais plus modestement de se limiter à une période plus contemporaine, c'est-à-dire celle qui permet la rencontre entre contrôle social et technique informatique, que l'on appellerait aujourd'hui plus volontiers le numérique, soit celle qui va des années 1970 jusqu'aux années 2010.

3 Certes, l'informatique[2] s'est développée en amont, dans les années 1950-1960, pour favoriser l'automatisation de calculs dans le domaine scientifique (météorologie, physique nucléaire) et dans ceux de l'armée (logistique, balistique) et de la recherche chimique et pétrolière. Cependant à partir des années 1960 l'informatique change de nature quand elle se diffuse tout en proposant de nouvelles applications logicielles qui vont permettre d'informatiser d'autres domaines d'activités : l'administration des populations par les États, les collectivités territoriales, la gestion des ressources humaines ou de clientèles par les grandes entreprises, entre autres. L'informatique va ainsi très

rapidement manier des informations nominatives concernant les personnes physiques, leur savoir, leur comportement, leur mode de fonctionnement, leur culture, comme en témoignent, dans les années 1970-1980, les publications de la collection « Informatisation et société » de La Documentation française[3].

4 La thématique « informatique et libertés » va émerger rapidement au milieu de thématiques plus classiques comme « informatique et politique industrielle », « informatique et emploi », « informatique et conditions de travail », « informatique et organisation du travail », « informatique et éducation » pour prendre de plus en plus d'importance et devenir dans les années suivantes une problématique à part entière. En France, le Centre de coordination pour la recherche et l'enseignement en informatique et société (CREIS) y contribue, notamment lors de la publication, en 1984, de l'ouvrage Société et informatique[4] – et non « Informatique et société ». L'accent est mis sur ce que fait la société de l'informatique et non l'inverse.

5 L'objet de cet article est de présenter, trop succinctement sans doute, l'évolution du contrôle social durant ces cinquante dernières années. Il est possible d'identifier la montée en puissance de ce qui est devenu la problématique « informatique et libertés individuelles et collectives » à travers quatre thématiques principales, permettant ainsi de mieux identifier les formes d'exercice de cette surveillance et de ce contrôle :

- Fichage, enfichage et tri (constitution de fichier volumineux pour administrer les populations).
- Surveillance planétaire (écoute et interception des échanges pour assurer la sécurité publique des populations).
- Affichage de soi et médiatisation du dévoilement (échange et marchandisation des données privées entre État et marché).
- Reconquête de l'anonymat et protection des données personnelles (cryptage des échanges).

6 Ainsi va-t-on assister en cinquante ans à une évolution des thématiques dominantes selon les périodes et les contextes. Certaines vont s'estomper, d'autres prendre de l'importance. La caractéristique est que l'apparition d'une nouvelle thématique ne se substitue en aucun cas à une plus ancienne.

Fichage, enfichage et tri

7 La technique informatique rendant possible l'établissement de fichiers concernant tout ou partie d'une population, le rapprochement entre ces fichiers, la confrontation de données multiples relatives à un individu à partir de critères prédéterminés, la prise de décision et la copie rapide et quasiment sans trace, des inquiétudes et interrogations dans un premier temps s'élèvent et sont suivies très vite de résistances, de contestations autour de la protection de la vie privée et des libertés individuelles et collectives. Ces questionnements ont été initiés dès les années 1960 aux États-Unis, puis dans les années 1970-1980 tant en France qu'en Europe et au-delà de ces territoires ensuite. La question « que faire pour que le développement de l'informatique n'attente pas aux libertés et à la démocratie ? », comme l'indiquent H. Delahaie et F. Paoletti (1987), a toujours perduré au fil du temps et est encore plus que jamais d'actualité. L'affaire Snowden (Wikileaks) ou plus récemment la controverse entre Apple et le FBI sont symptomatiques de cette constante.

8 Cette préoccupation va prendre de l'importance lors du développement de « fichiers pas comme les autres » dans les années 1970 ; ainsi, les projets de fichage de population comme Safari (Système automatisé pour les fichiers administratifs et le répertoire des individus) ou Gamin (Gestion automatisée de la médecine infantile) avaient pour objectif de dépister les enfants à risques à partir de critères médicaux et sociaux. Les investigations menées vont mettre à jour de nouvelles formes de contrôle social (CREIS, 1984) et enclencher une réflexion sur l'utilisation de cette technique auprès de travailleurs du secteur médico-social[5]. Mais c'est la publication, par le journaliste P. Boucher le 21 mars 1974, dans les pages « justice » du quotidien Le Monde, d'un article intitulé « Safari ou la chasse aux Français » qui va éveiller l'opinion publique sur le problème du fichage informatique et qui débouchera quelques années plus tard sur l'adoption de la loi Informatique et libertés.

9 La résistance se met alors en marche contre un État jugé trop tutélaire, portant atteinte aux libertés individuelles et collectives et remettant en compte certaines déontologies professionnelles. Elle favorisera en France la mise en place d'une réflexion (rapport Tricot, 1975) suivie, non sans mal, d'un premier projet de loi (1976) qui sera contrecarré, puis de la promulgation d'une loi (1978) régulant la constitution de fichiers de personnes physiques et des traitements nominatifs associés, l'une des premières au monde : Informatique, fichiers et libertés.

10 Le développement de l'État-providence ainsi que la gestion des prestations sociales favorisent d'une part la démultiplication des fichiers tenus par les administrations publiques qui comportent des données sensibles sur des personnes physiques. D'autre part, la création de fichiers de plus en plus élaborés et interconnectés grâce aux prouesses techniques, mais aussi résultant de l'adoption du RNIPP (Répertoire national d'identification des personnes physiques).

11 Les traitements informatiques vont ainsi rendre possibles la création et l'exploitation de fichiers volumineux concernant tout ou partie de la population, tâches qui étaient auparavant laborieuses et exigeaient des ressources humaines considérables. Grâce à des outils informatiques de plus en plus sophistiqués en relation avec des systèmes de gestion de bases de données, l'administration fiscale, par exemple, collecte et traite de plus en plus d'informations personnelles dans le but de simplifier la vie des contribuables certes, mais surtout pour débusquer les fraudeurs tout en cernant au mieux les administrés. Quant à la transmission automatique de renseignements émanant de différentes institutions (organismes de sécurité sociale, caisses d'allocations familiales, caisses de retraites, assureurs, etc.), elle ne va cesser de se déployer.

Surveillance planétaire globale

12 Le processus de mondialisation des échanges impulsé à la fin des années 1990 par certains acteurs économiques et financiers et soutenu, le plus souvent, par les pouvoirs politiques va mettre en exergue une thématique qui n'est certes pas nouvelle, à savoir l'internationalisation des fichiers, mais qui prend de l'ampleur avec les questions liées à la circulation des informations, au traitement et à la conservation de données en provenance d'un pays par d'autres États, par des entreprises étrangères ou encore celles qui sous-traitent l'exploitation de leurs fichiers informatiques sur un sol étranger. La

diffusion de l'Internet renforcera la délocalisation de ce type de pratique, le plus souvent dans des pays dont la législation est moins contraignante.

13 La thématique du fichage reste toujours présente, mais s'estompe et laisse de plus en plus place à la question de la surveillance planétaire via les techniques d'information et de communication. Cela ne veut pas dire qu'elle disparaît. À plusieurs reprises, elle refera surface, en France par exemple, lors de l'annonce de la mise en place de nouveaux fichiers, comme Edvige (Exploitation documentaire et valorisation de l'information générale) qui a pour objectif de centraliser et d'analyser les informations relatives aux personnes ayant exercé une activité politique, syndicale, économique ou religieuse, Base élèves, qui informatise la gestion nationale de la scolarité des élèves, ou encore Eloi dont le but était de lutter contre l'immigration clandestine etc.

14 L'affaiblissement de la thématique du fichage est la résultante de trois évolutions (Carré, 2004). La première est d'ordre juridique, par le biais de la promulgation d'une loi et la création de la Commission nationale de l'informatique et des libertés (CNIL), rassure et encadre le développement de ce type d'activité. La deuxième est d'ordre technique, alors que la diffusion de la micro-informatique permet aux usagers d'entrevoir un caractère ludique de l'informatique. La troisième et dernière, d'ordre politique, s'inscrit dans une orientation de libéralisation des marchés et de remise en cause ou de grignotage de l'État-providence. D. Forest estime même que :

« la société de surveillance s'inscrit dans un double mouvement de déréglementation encouragé par les politiques européennes au profit des lois du marché, d'une part, et de surréglementation policière, d'autre part » (Forest, 2009, p. 4).

15 La surveillance électronique mise en place par les États-Unis et leurs alliés, la Grande-Bretagne et le Canada, via notamment le système *Echelon*, permet une écoute des communications privées ou commerciales à l'échelle planétaire : espionnage économique, politique, militaire, puis lutte contre le terrorisme. Les révélations de Snowden sur le programme de surveillance massif de la NSA (agence de la sécurité américaine) en sont une parfaite illustration. Tous les systèmes installés reposent sur l'interception des signaux des satellites, des câbles subaquatiques, des radiocommunications et des communications circulant sur Internet sans être cryptées. L'espionnage n'est certes pas une activité nouvelle, mais c'est l'organisation de celle-ci, révélée par le rapport rédigé par D. Campbell pour le Parlement européen (2001), qui surprend. La surveillance devient globale et doit être considérée dorénavant comme une véritable activité industrielle de masse.

16 Suite aux attentats du 11 septembre 2001, le Congrès américain adopte le *USA Patriot Act* qui renforce considérablement les pouvoirs de différentes agences gouvernementales (FBI, CIA, NSA). S'en suivront d'autres textes, comme le *Homeland Security Act* (HSA), qui permet aux autorités de récolter auprès des fournisseurs d'accès à Internet (FAI) toute information nécessaire. Quant au passeport, il devient biométrique. L'accord *Privacy Shield* entre les États-Unis et l'Union européenne (UE) fournit aussi un cadre pour les transferts des données personnelles des citoyens européens aux États-Unis.

17 Le Canada, quant à lui, décide en 1999, via le Conseil de radiodiffusion et des télécommunications canadiennes (CRTC) de ne pas réglementer le réseau Internet aux motifs qu'il n'est pas un média de masse et que la réglementation pouvait s'appliquer moyennant quelques adaptations (George, 2007). Un revirement va s'opérer très vite suite aux attentats du 11 septembre 2001. Le gouvernement légifère rapidement afin de

prendre, comme l'indique É. George, des mesures susceptibles d'anticiper les actions terroristes qui déboucheront quelques années plus tard sur un projet de loi très controversé qui a vocation d'augmenter les capacités de surveillance électronique et de contraindre les fournisseurs d'accès à stocker les données disponibles dans le but de les remettre éventuellement aux personnes chargées d'appliquer les lois. Notons que la société Bell Canada, sans attendre une telle loi, a ajouté une clause dans ses contrats lui permettant la surveillance des usages des services dans le cadre des lois, des réglementations et de toute requête effectuée par le gouvernement (Geist, 2006)[6].

18 La France n'est pas en reste, avec le développement du projet PNIJ (Plate-forme nationale des interceptions judiciaires) même si, reconnaissons-le, ses moyens sont de moindre importance et que le dispositif ne maîtrise pas toutes les techniques numériques, dont la plupart ont vu le jour sur le sol américain. Depuis 1986, en France, ce ne sont pas moins d'une trentaine de lois qui vont être promulguées pour renforcer la sécurité publique et mettre en œuvre une idéologie sécuritaire[7]. Insécurité urbaine et terrorisme vont aussi favoriser grandement le recours à des techniques numériques[8] et audiovisuelles de surveillance (caméras de vidéosurveillance)[9].

19 Á cela s'ajoute la mise en commun de fichiers au niveau de l'espace Schengen, comme le SIS (personnes recherchées ou surveillées), l'Ecris (casiers judiciaires) ou le VIS (demande de visa pour entrer dans l'espace Schengen). Cette surveillance industrialisée et globalisée a aussi un autre objectif, celui de Surveiller et prévenir (Laval, 2012).

20 Pour lutter contre le terrorisme, la traque et l'analyse en continu des comportements de personnes dans l'espace public semblent devenir incontournables pour de nombreux gouvernements. Mais attention à certaines dérives sécuritaires. Le cas de la France est éclairant. Avec la loi sur le renseignement, l'état d'urgence et la réforme pénale, il n'y a pas que la sécurité publique qui est en jeu, même si cela en est un aspect important. On assiste clairement à la mise en œuvre d'une logique sécuritaire sociétale qui s'installe. Cet engrenage sécuritaire est d'autant plus insidieux qu'il se présente comme une protection contre un danger connu et reconnu : éviter les attentats et surveiller l'évolution de certaines personnes susceptibles de passer à l'acte. En pérennisant des mesures de surveillance exceptionnelles, ne va-t-on pas instituer une nouvelle gouvernance politique qui donne à l'administration des prérogatives appartenant dans les démocraties au pouvoir judiciaire ? On peut le craindre en France avec le vote du projet de loi dit de « lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale », qui intègre directement une partie des mesures de l'état d'urgence dans la loi.

21 Au niveau européen, la situation reste dans le clair-obscur avec le vote définitif par le Parlement européen sous forte pression médiatique et politique (en particulier française) de la mise en œuvre du *Passenger Name Record* (PNR). Longtemps refusé par le Parlement, cet accord institue la création de fichiers nationaux regroupant une quarantaine de données de toutes les personnes voyageant depuis ou vers l'Union européenne, y compris les vols internes. Mesure liberticide comprenant 40 renseignements (nom, numéro de passeport, itinéraire, type de repas choisi par chaque passager, etc.) – ces renseignements seront stockés pendant 5 ans. Mesure qui est contraire au traité européen.

22 Dans le même temps, le Parlement a adopté le règlement sur la protection des données personnelles, qui sera applicable d'ici deux ans. Celui-ci remplacera la directive de 1995, qui avait été diversement transposée par les États membres de l'UE. Il introduit également de nouvelles règles longtemps demandées par le G29 et les associations de

défense des droits et des libertés des citoyens sur Internet. Ainsi, l'accord explicite des internautes est requis pour l'utilisation des données personnelles. Le droit à l'oubli est intégré : l'internaute pourra demander l'effacement de ses données personnelles à tous les services en ligne, y compris aux moteurs de recherche. La portabilité des données est exigée et chaque service devra fournir des données formatées compatibles avec les logiciels concurrents.

Affichage de soi et médiatisation du dévoilement

23 Au fichage et à la surveillance planétaire globale s'ajoute une autre forme de contrôle qui va se développer : la médiatisation de l'affichage de soi. L'informatique, puis les technologies d'information et de communication (TIC) et aujourd'hui ce qui est appelé le plus souvent le numérique jouent un rôle essentiel dans le processus de mondialisation (Paoletti, 2003). D'une part, les industriels, par des stratégies d'alliance et de convergence, vont favoriser la constitution d'opérateurs mondialisés en position de quasi-monopole ou d'oligopole, dont le marché n'est plus national mais mondial. C'est le cas d'entreprises appartenant aux industries de la communication (électronique, informatique, télécommunications) qui proposent des services en ligne et gratuits : Google (moteur de recherche), Amazon (commerce électronique), YouTube (site d'hébergement et de diffusion de vidéos), Facebook (service de réseautage numérique), iTunes Store (achat de musique en ligne). D'autre part, en développant des infrastructures de réseaux planétaires, États et opérateurs contribuent fortement au développement du commerce électronique et à l'apparition d'une nouvelle forme d'entreprise qui a pour seule fonction l'infomédiation, c'est-à-dire la mise en rapport d'un agent économique, le demandeur, avec un autre agent, l'offreur de biens ou de services (Paoletti, 2003, p. 49).

24 Pour favoriser le commerce mondialisé sur Internet, il est alors nécessaire que le Net soit débarrassé de son orientation libertaire, expressive, afin de le rendre sûr. Pour ce faire, le Congrès et le Département de la justice américaine, qui sont les principaux acteurs de la gouvernance de l'Internet, vont invoquer la présence de pornographie et surtout de pédophilie, sources de vulnérabilité, pour dénoncer un cyberespace incontrôlable et favoriser la mise en place d'une gouvernance de l'Internet plus conforme aux marchés, comme l'a fait ressortir, dans sa thèse, G. Giudici (2010), quitte à éroder les libertés individuelles.

25 Les démarches marketing renforceront cette surveillance insidieuse via la mise en plage de programmes de reniflage (*datamining*), de captation des données, de collecte des adresses de connexions, de traçage des navigations au nom de la prise en compte des désirs des usagers-consommateurs. Ce qui permet aux commerçants du Net par homophilie de proposer, par exemple, à un consommateur des biens ou des services sélectionnés par d'autres ayant des goûts culturels semblables. C'est dans ce contexte que s'est mise en place une forme de contrôle social dont la force est d'être diffuse au point qu'elle en est invisible. L'objectif est de proposer d'une manière personnalisée des sollicitations le plus souvent à caractère commercial. Ce qui permet en retour aux industriels d'engranger de nouvelles traces ou données, afin d'autoalimenter le système. Les moteurs de recherche, les réseaux socionumériques sont bien entendu des pièces maîtresses du dispositif, car les données recueillies ont une valeur d'usage et une valeur marchande élevées (Carré, Panico, 2011). Les données sont ainsi au cœur des modèles

d'affaire du numérique. D. Cardon n'hésite pas quant à lui à noter que s'installe une économie de la visibilité (2012).

26 On assiste alors à une émancipation sans précédent, où la puissance d'agir des individus, l'affichage de soi et l'injonction de visibilité donnent corps en contrepartie à un contrôle social intrusif, discret, sans relâche et inédit, mais qui apparaît aussi librement consentie (Martin-Juchat et Pierre, 2011), ce contrôle qui est enchâssé dans des activités quotidiennes les plus ordinaires. Selon D. Carré et R. Panico (2012-a), ce contrôle joue sur un triple registre : ne pas apparaître a priori comme un contrôle discriminant ayant pour objet une population particulière ; ne pas apparaître comme un contrôle par la contrainte, dans la mesure où il s'applique à recueillir çà et là ce qui est laissé ou dit spontanément ; et faire de l'individu ordinaire, celui-là même sur lequel ce contrôle s'exerce, l'actionneur de ce contrôle (2012). Ce qui fait dire à ses auteurs que l'on est face à un :

« contrôle qui sait se nourrir au grand jour du simple recueil des traces qu'un peu partout les internautes abandonnent, parfois à leur insu, mais le plus souvent avec leur consentement passif, quand ce n'est pas à leur initiative, fournissant à tous ceux, policiers, marchands qui le désirent, un compte rendu minutieux de leurs comportements individuels là où jadis il fallait d'eux obtenir les aveux » (Carré et Panico, 2012-b, p. 197).

27 Ainsi, certains murs électroniques dédiés à l'affichage de soi ne seraient-ils pas en matière de renseignements et de contrôle social, du seul fait des pratiques de dévoilement qu'ils encouragent, rétribuent et normalisent, plus efficaces désormais que les fichiers de police les plus musclés ou les bases de clients hypersegmentées ? G. Deleuze ne l'avait-il pas entrevu d'une certaine manière lorsqu'il écrivait : « La formule abstraite du panoptisme n'est plus de "voir sans être vu", mais imposer une conduite quelconque à une multiplicité humaine quelconque » (1986, p. 41).

28 Observateur de ce processus à l'œuvre, J.-G. Ganascia (2009) qualifie notre société de société de « sousveillance », car le contrôle vient du bas de la multitude. Un nouveau modèle de surveillance serait en train d'émerger via le « Catopticon », à l'inverse du Panopticon inventé par J. Bentham et repris par M. Foucault (1975) pour décrire des systèmes institutionnels fondés sur des logiques de pouvoir centralisées et hiérarchisées. Le contrôle s'effectuant d'en haut, le dominant étant celui qui est capable de « voir sans être vu ». A contrario, le Catopticon désigne un type de système de surveillance fondé sur des logiques de pouvoir décentralisées. Celui qui aurait les moyens d'être vu serait dans la position du dominant. Toujours pour cet auteur, le développement des techniques numériques permettrait un repositionnement symbolique des pratiques de contrôle.

29 C'est également le point de vue de D. Kaplan (2010, p. 103) :

« il s'agirait alors de passer d'une approche défensive de l'identité et de la vie privée à une approche stratégique, donc à la fois défensive et offensive. De partager le pouvoir des technologies en outillant les individus au même niveau que les organisations qui veulent en savoir plus sur eux. D'aider les individus ou les communautés qu'ils composent à négocier mais aussi à jouer avec les organisations ».

30 La CNIL et les autorités de protection du G29 militent dans ce sens. Après que Facebook a annoncé la modification de sa politique de confidentialité, la CNIL a enquêté. Un groupe composé des cinq autorités de protection ayant décidé de mener des investigations (France, Belgique, Pays-Bas, Espagne et Land de Hambourg) a été créé en mars 2015 au sein du G29. Il est apparu que la pratique de Facebook n'est pas conforme à la loi

Informatique et libertés. Le réseau est accusé de pister les données de navigation de tous les internautes, même si ceux-ci ne disposent pas de compte Facebook, dès lors qu'ils visitent une page publique du site. La société dépose sur l'ordinateur des visiteurs un fichier informatique appelé cookie, qui identifie tous les sites sur lesquels ces internautes se rendent du moment qu'ils contiennent un bouton Facebook. La CNIL reproche aussi au réseau social numérique de croiser les données personnelles de ses membres sans leur consentement explicite, et ceci à des fins publicitaires. Le règlement sur la protection des données personnelles adopté par le Parlement européen en vue de remplacer la directive de 1995 s'inscrit également dans cette démarche.

Données personnelles : droit de propriété, anonymat ou chiffrement ?

31 Le rééquilibrage des relations entre les individus et les organisations peut-il se limiter à des aménagements techniques au niveau logiciel, comme le préconisent certains chercheurs et les autorités de protection ? « Si la régulation des algorithmes devient une question centrale, c'est en partie parce qu'ils entraînent parfois sans intention des discriminations », souligne D. Cardon (2016, pp. 86-87) dans un interview publié par La Recherche de mai 2016.

32 Faut-il adopter des mesures plus radicales ? Par exemple, celles qui rendraient les internautes propriétaires de leurs données personnelles à titre privé comme moyen de rééquilibrer les pouvoirs avec les entités collectrices ? La CNIL et le Conseil national du numérique (CNNum) ont pris position fermement contre cette proposition. À juste titre semble-t-il, car, bien que dans l'air du temps d'une société de plus en plus « individualiste », elle oublie le rapport de forces disproportionné entre l'individu et les entreprises. Le commerce des données personnelles qui en découlera n'enrichira que les grandes entreprises comme Google et Facebook ainsi que les prestataires de services auxquels une partie des internautes, faute de temps et de moyens, confiera la gestion de ses données. Les revenus que ceux-ci pourront en tirer seront minimes en général et ne profiteront qu'à quelques « débrouillards » qui pourraient développer des « paradis numériques », comme il existe des paradis fiscaux.

33 Le droit à l'anonymat historiquement est reconnu. Il reste en effet souvent l'unique moyen de publier des opinions face à des pouvoirs politiques ou économiques. De même, le secret de la correspondance est garanti dans toutes les constitutions de la planète, même si cela reste trop souvent encore théorique dans certains pays. La notion d'anonymat est en fait plus ambivalente : elle peut servir à dissimuler des actions contraires à la loi ou encore à nuire à d'autres personnes, que l'on pense aux nombreuses lettres anonymes envoyées lors de l'occupation de la France pendant la Seconde Guerre mondiale et après (Engelhard et Panico, 2010).

34 Le développement des techniques numériques a largement facilité le travail des « lanceurs d'alerte » et des opposants aux pouvoirs autoritaires en tout genre. Le recours aux techniques de chiffrement, soit pour le contenu du disque dur des ordinateurs, soit des communications a limité les actions des forces de répression dans certaines circonstances et peut être considéré comme un soutien à la démocratie. En ce sens, il doit être défendu et encouragé. Mais sous prétexte de lutte contre les organisations terroristes et contre le crime organisé, des gouvernements démocratiques et des grandes entreprises

mènent campagne contre l'utilisation des logiciels, en général des logiciels libres, qui permettent à tout utilisateur un tant soit peu « informé et bidouilleur » de crypter aussi bien ses propres données que ses échanges par Internet. Les gouvernements acceptaient que les entreprises de communication et les fournisseurs d'accès cryptent par sécurité les données de leurs clients car, comme l'a montré l'affaire Snowden, il était toujours possible de faire pression sur leurs responsables pour obtenir les clefs de déchiffrement en cas de nécessité. Mais le problème devient plus ardu quand chaque internaute met en œuvre directement ces techniques. D'où cette multiplication d'articles, d'interviews de consultants en sécurité, d'hommes politiques arguant les difficultés rencontrées par les services de police dans la lutte contre le terrorisme à cause de ces techniques.

35 Mais en fait, ce qui gêne aussi bien la NSA que la DGSE, c'est la difficulté, si la cryptographie se généralise, de faire de l'espionnage de masse (comme le prévoit l'utilisation des IMSI-catchers[10], par exemple dans la loi sur le renseignement) dans un quartier sans savoir exactement ce qui est recherché et ciblé. La surveillance sous contrôle judiciaire dispose d'autres moyens pour obtenir des informations précises sur un suspect. Depuis les révélations de l'affaire Snowden et par peur des réactions de leurs clients, les grandes entreprises du Net ont tendance à se désengager de cette collaboration avec les agences de renseignement et à fournir des logiciels permettant aux utilisateurs de mettre en œuvre leur propre chiffrement (Apple contre le FBI[11]).

36 Le chiffrement n'est pas pour autant la panacée. Il peut être difficile à mettre en œuvre pour certaines applications. Crypter toutes les données sur sa machine entraînerait forcément un surcoût non négligeable en temps de calcul. Et un moteur de recherche aura quelques difficultés à accéder à des données chiffrées. Mais surtout, la garantie offerte par les techniques actuelles de chiffrement ne durera qu'un temps limité qui dépendra de la longueur des clefs choisies : de quelques mois à quelques années, en fonction des progrès de la recherche en cryptologie et en mathématiques et de l'accroissement de la puissance de calcul des ordinateurs. Les services de renseignement et les grandes entreprises auront toujours les machines les plus rapides à leur disposition. Sans parler de la menace d'un hypothétique ordinateur quantique susceptible de casser théoriquement tous les codes actuels.

Conclusion

37 Tout d'abord, indiquons que les thématiques ont été traitées pour des raisons de commodité et de compréhension, selon leur ordre d'apparition chronologique dans la société. Bien entendu, les situations, selon les périodes, sont plus complexes et des interrelations, des entrelacs, existent entre ces différentes thématiques qui auraient nécessité des développements trop importants pour les expliciter ici. Ce qui n'était pas l'objet de cette contribution. Ensuite, précisons que l'émergence d'une thématique est la résultante d'une triple influence, d'orientations culturelles et idéologiques, d'un dispositif technico-organisationnel dominant et de l'intervention d'acteurs sociaux dans l'espace public. Enfin, mentionnons que la caractéristique principale est qu'en matière de contrôle social, l'apparition d'une nouvelle thématique ne se substitue pas ou ne fait pas disparaître une plus ancienne. Une thématique qui était principale à une période, supplantée ensuite par la montée en puissance d'une autre, peut revenir en force quelque temps plus tard. C'est le cas, par exemple, comme nous l'avons vu, de la thématique du fichage (1970-1980) qui, avec la prolifération de nouveaux projets de création de fichiers

au début du 21e siècle (Edvige, Base élèves ou Eloi), refera surface et prendra de nouveau de l'importance.

BLACK E., 2001, *IBM et l'Holocauste : L'Alliance stratégique entre l'Allemagne nazie et la plus puissante multinationale américaine*, Paris, Robert Laffont.

CAMPBELL D., 2001, *Surveillance électronique planétaire*, Paris, Éditions Allia.

CARDON D., 2016, « Faut-il réguler les algorithmes ? », entretien avec GLAVIEUX, V., *La Recherche*, n° 511, pp. 86-87.

CARDON D., 2012, « Montrer/regarder – L'Économie de la visibilité sur les réseaux sociaux d'Internet », in *Lien social et Internet dans l'espace privé*, sous la direction de C. JANSSEN et J. MARQUET, Louvain-La-Neuve, Harmattan-Academia, pp. 21-50.

CARRÉ D. et PANICO R., 2012-a, « Du fichage subi à l'affichage de soi : Éléments pour une approche communicationnelle du contrôle social », in *Connexions : Communication numérique et lien social*, sous la direction de S. PROULX et A. KLEIN, Presses universitaires de Namur, pp. 269-283.

CARRÉ D. et PANICO, R., 2012-b, « Dévoilement, mise en scène et médiatisation. Nouvelles normes de sociabilité sur le Websocial ? », Colloque international « Communiquer dans un monde de normes », coorganisé par l'Association internationale de communication, GERiiCO et la SFSIC, Roubaix, 7-9 mars 2012, https://halshs.archives-ouvertes.fr/hal-00826060.

CARRÉ D. et PANICO R., 2011, « Le Contrôle social à l'heure des technologies de mobilité et de connectivité : Du fichage ciblé des individus au traçage continu des agissements », *Terminal*, https://terminal.revues.org/1292, dernière consultation le 14 septembre 2016.

CARRÉ D., 2004, « Des dégâts du progrès... au marketing de l'usage. Revirement de perspectives en matière de critique sociale dans le champ "Informatique et société" », in *Société de l'information, société du contrôle ? Évolution de la critique de l'informatisation*, actes du 13e colloque international du Centre de coordination pour la recherche et l'enseignement en informatique et société (CREIS), Paris, du 30 juin au 2 juillet 2004, http://www.lecreis.org/?p=188.

CREIS, 1984, *Société et informatique*, Paris, Delagrave.

DELAHAIE H. et PAOLETTI F., 1987, *Informatique et libertés*, Paris, Éditions La Découverte.

DELEUZE G., 1986, *Foucault*, Paris, Les Éditions de Minuit.

ENGUEHARD C. et PANICO R., 2010, « Technologies et usages de l'anonymat sur Internet » (dossier), *Terminal*, n° 105, Paris, L'Harmattan.

FOREST D., 2009, *Abécédaire de la société de surveillance*, Paris, Éditions Syllepse.

FOUCAULT M., 1975, *Surveiller et punir*, Paris, Gallimard.

GALLOUEDEC-GENUYS F. et LEMOINE P., 1980, *Les Enjeux culturels de l'informatisation*, Paris, La Documentation Française, coll. « Informatisation et société ».

GANASCIA J.-G., 2009, *Voir et pouvoir : qui nous surveille ?*, Paris, Le Pommier.

GEIST M., 2006, « Bell Controversy Puts Spotlight on Net Surveillance », Toronto Star, www.michaelgeist.ca/content/view/1314/159, dernière consultation le 14 septembre 2016.

GEORGE É, 2007, « Après le 11 septembre 2001 : sécurité ou surveillance ? Analyse de la politique canadienne en matière de contrôle du contenu informatique », in *De l'insécurité numérique à la vulnérabilité de la société*, actes du 14e colloque international « Informatique et société » du Centre pour la recherche et l'enseignement en informatique et société (CREIS), pp. 189-199,

www.lecreis.org/colloques%20creis/2007/EGeorge.pdf, dernière consultation le 14 septembre 2016.

GIUDICI G., 2010, *Les Mutations de l'Internet entre régulation juridique et pratiques de file sharing*, Université Paris 13-Universita La Sapienza di Roma.

KAPLAN D., 2010, *Informatique, libertés, identités*, Limoges, Éditions Fyp, coll. « La fabrique des possibles ».

LANG H., MARTIN, D., MOUSSAOUI-SUARD B. et RODRIGUEZ N., 1985, *Informatique oui, mais... : L'Outil informatique dans le secteur médico-social*, Annales du Centre de recherche sociale, n° 19, Genève, Les Éditions I.E.S.

LAVAL C., 2012, « Surveiller et prévenir. La nouvelle société panoptique », in « Sortir de (la) prison : Entre don, abandon et pardon », *Revue du M.A.U.S.S.*, n° 40, pp. 47-72.

MATTELART A. et VITALIS A., 2014, *Le Profilage des populations : Du livret ouvrier au cybercontrôle*, Paris, Éditions La Découverte.

MARTIN-JUCHAT F. et PIERRE J., 2011, « Facebook et les sites de socialisation : une surveillance librement consentie », in *L'Homme trace : Perspectives anthropologiques des traces contemporaines*, sous la direction de B. GALINON-MÉLÉNEC, Paris, CNRS Éditions, pp. 105-125.

PAOLETTI F, 2003, *L'homme et l'ordinateur : Les Enjeux de l'informatisation de la société*, Paris, L'Harmattan.

NOTES

1. Le panoptique de Jeremy Bentham en est une bonne illustration ; il permet à un individu d'observer d'autres personnes sans que ces dernières ne sachent qu'elles étaient observées.
2. Même si auparavant d'autres machines ont permis le traitement automatisé de l'information, comme la machine mécanographique de Herman Hollerith à la fin des années 1800 et dont Edwin Black montre, dans son ouvrage *IBM et l'Holocauste : L'Alliance stratégique entre l'Allemagne nazie et la plus puissante multinationale américaine* (2001), qu'elles ont permis l'identification et le traitement automatisé des Juifs avec une redoutable efficacité pendant la Seconde Guerre mondiale.
3. En particulier la publication parue en 1980, *Les Enjeux culturels de l'informatisation*, ouvrage collectif sous la direction de F. Gallouedec-Genuys et P. Lemoine, préface de B. Tricot.
4. Dans cette publication, si majoritairement la plupart des chapitres sont consacrés à la question du travail, quatre se rapportent à celle du contrôle social : le contrôle social (chap. 5), les libertés (chap. 6), la démocratie (chap. 7), l'information automatisée (chap. 8).
5. Cf. Lang H., Martin D., Moussaoui-Suard B., Rodriguez N., 1985, *Informatique oui, mais... : L'Outil informatique dans le secteur médico-social*, Annales du Centre de recherche sociale, n° 19, Genève, Les Éditions I.E.S.
6. Rapporté par É. George (2007) dans son texte *Après le 11 septembre 2001 : sécurité ou surveillance ? Analyse de la politique canadienne en matière de contrôle du contenu informatique.*
7. Après les premiers attentats de Paris, la loi du 9 septembre 1986 relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État a été promulguée. Elle sera suivie de beaucoup d'autres, comme la loi d'orientation et de programmation pour la sécurité du 21 janvier 1995 qui

a pour objectif, suite aux émeutes urbaines, de développer la vidéosurveillance afin d'accroître la protection des lieux publics... À partir des années 2010, la promulgation de lois se renforce. On en compte alors une à deux par an.

8. À titre d'exemples : loi pour la sécurité intérieure, fichier national automatisé des empreintes génétiques (FNAEG, 2003) ; loi relative à la lutte contre le terrorisme (2006), dont l'article 6 impose aux opérateurs télécoms, aux fournisseurs d'accès à Internet (FAI) mais aussi à tout établissement public proposant un accès au Net, comme les cybercafés, de conserver les données de connexion (logs) pendant un an. La loi prévoit que l'accès à ces logs par les autorités policières n'est plus soumis à autorisation d'un magistrat et donc effectué sous contrôle judiciaire ; loi sur la surveillance dans un but préventif des données de connexions (Internet, géolocalisation, factures détaillées de téléphone (2005), une disposition temporaire qui sera ensuite prolongée ; loi d'orientation et de programmation pour la performance de la sécurité intérieure, qui permet la captation des données informatiques (2011).

9. Notons que depuis quelque temps l'appellation « vidéosurveillance » a été remplacée par « vidéoprotection ». On l'aura compris, le renversement sémantique est symptomatique du positionnement adopté par les pouvoirs publics pour soi-disant « protéger » et non « surveiller ».

10. Fausses antennes-relais qui peuvent capter toutes les données téléphoniques sur un rayon de quelques centaines de mètres jusqu'à deux kilomètres.

11. Le FBI n'a pu contourner le chiffrement des mots de passe des iPhones, car Apple n'en possédait pas la clef. Plus récemment, Microsoft s'est appuyé sur les lois européennes pour refuser de transmettre des données (courriers électroniques) stockés en Irlande à la justice nord-américaine.

RÉSUMÉS

L'objet de cet article est de présenter à grands traits l'évolution du contrôle social par la technique informatique, que l'on appellerait plus volontiers aujourd'hui le numérique. Il est possible d'identifier au cours de ces cinquante dernières années la montée en puissance de ce qui est devenu la problématique « informatique et libertés », qui va s'affirmer à travers quatre thématiques : fichage, enfichage et tri ; surveillance planétaire globale ; affichage de soi, médiatisation du dévoilement ; reconquête de l'anonymat et protection des données personnelles. La caractéristique principale est que l'apparition d'une nouvelle thématique ne se substitue pas à une plus ancienne.

The purpose of this article is to present the evolution of social control by computer technology, more often called digital technology, today. There has been an increasing concern for data protection over the past fifty years. Four areas of concern are: uses of personal information such as date of birth, account passwords, etc.; comprehensive global surveillance; self-presentation and the mediatisation of private information; and reclaiming anonymity and the protection of personal data. The main theme of this article is that the emergence of a new theme which does not replace older ones.

El objetivo de este artículo es el de presentar sucintamente la evolución del control social mediante técnicas informáticas, a las que, de manera general, denominamos *lo digital*. Durante los últimos cincuenta años, es posible identificar, el crecimiento de lo que constituye la problemática

“informática y libertades”, que se articula en torno a cuatro temáticas: registro, archivo y clasificación; vigilancia planetaria global; muestra de sí mismo, mediatización del desvelamiento; reconquista del anonimato y protección de datos personales. La característica principal que se deduce es que la aparición de una nueva temática no sustituye a una más antigua.

INDEX

Mots-clés : informatique et libertés, fichage, tri, surveillance planétaire, données personnelles, protection
Keywords : digital technology and freedom, profiling, sorting, global surveillance, personal data
Palabras claves : Informática y libertades , fichaje, clasificación, vigilancia planetaria, datos personales, protección

AUTEURS

DOMINIQUE CARRÉ

Dominique est professeur en sciences de l’information et de la communication et dirige l’Unité de formation et de recherche (UFR) des Sciences de la communication (université Paris 13). Il anime la thématique 3 du Laboratoire des Sciences de l’information et de la communication (LabSic) « Innovations communicationnelles : dispositifs, normes et usages ». Ses recherches portent sur les sujets suivants : mobilisation par la communication ; puissance d’agir et espace public ; approche communicationnelle du contrôle social ; mise en réseau, rationalisation, industrialisation de l’information et de la communication ; numérique et environnement. Il coordonne avec Geneviève Vidal, chez ISTE Éditions, la série « Informatique et société connectées ».

JACQUES VÉTOIS

Jacques Vétois est membre du comité de rédaction de la revue *Terminal*. redaction@revue-terminal.org