Cultures & Conflits

93 | printemps 2014
Résistance, existence, autorité

La bienveillante neutralité des technologies d'espionnage des communications : le cas tunisien

The benevolent neutrality of communication surveillance technologies: the tunisian case

Marie Goupy

Édition électronique
URL : http://journals.openedition.org/conflits/18863
DOI : 10.4000/conflits.18863
ISSN : 1777-5345

Éditeur :
CCLS - Centre d'études sur les conflits lilberté et sécurité, L'Harmattan

Édition imprimée
Date de publication : 8 juillet 2014
Pagination : 109-124
ISBN : 978-2-343-04155-1
ISSN : 1157-996X

Référence électronique
Marie Goupy, « La bienveillante neutralité des technologies d'espionnage des communications : le cas tunisien », *Cultures & Conflits* [En ligne], 93 | printemps 2014, mis en ligne le 02 juillet 2015, consulté le 19 avril 2019. URL : http://journals.openedition.org/conflits/18863 ; DOI : 10.4000/conflits.18863

La bienveillante neutralité des technologies d'espionnage des communications : le cas tunisien [1]

Marie GOUPY

Marie Goupy est Docteure de l'ENS-Lyon. Elle est actuellement postdoctorante ETOS, Institut Mines-Télécom. Ses travaux de recherches portent sur les théories juridico-politiques de l'état d'exception.

Au moment même où l'affaire PRISM [2] relance les débats concernant l'usage des technologies de surveillance de masse dans les régimes démocratiques, il semble opportun de réfléchir aux alliances qui se sont nouées, depuis le début des années 1990, entre les ingénieurs, les entreprises et les services de police dans la mise en place de nouvelles formes de gestion des questions de sécurité. La collaboration des entreprises du net, des opérateurs téléphoniques ou des multinationales œuvrant dans le secteur des technologies de la sécurité avec les États, ou l'apparition de cette étrange catégorie des « policiers-ingénieurs » à l'intérieur même de leurs services de sécurité, pose effectivement de nouveaux problèmes dans le champ politique et juridique. Mais précisément, à la fois parce que le renseignement est par définition inaccessible au public et parce que les technologies de surveillance des communications reposent sur un ensemble d'outils et de dispositifs qui exigent des connaissances propres à décourager toute analyse approfondie, le fonctionnement de ces systèmes de surveillance technico-policier demeure extrêmement obscur et mal connu. Une obscurité qui permet le maintien du *statu quo* qui semble

1 . Cet article est issu d'une recherche engagée à l'origine avec J.-M. Salmon. Il doit beaucoup à l'aide de N. Beau, qui a contribué de manière déterminante aux enquêtes menées en Tunisie en me permettant d'accéder à de très nombreux contacts.

2 . Le « système » PRISM, dont le *Guardian* et le *Washington Post* ont révélé l'existence le 6 juin 2103 suite aux confidences d'E. Snowden, consiste en un programme de surveillance électronique mis en place en 2007 par l'administration américaine. Il s'agirait, d'après les informations qui demeurent partielles, d'un logiciel de collecte et de traitement de données qui permettrait aux services de renseignements américains, et plus spécifiquement à la NSA, d'analyser une masse énorme de données collectées, selon le *Guardian*, grâce à un accès direct de la NSA aux serveurs de très grandes entreprises du net (Google, Yahoo !, Apple, Skype, Microsoft, AOL, YouTube, Facebook) – ce que ces entreprises ont nié collectivement.

prévaloir sur la très délicate question des limites de l'usage légitime de ces technologies. Car, au cœur même des différents scandales diplomatiques produits par les révélations sur les programmes ECHELON ou PRISM, il semble que la limite tacitement admise entre l'usage légitime ou illégitime de ces technologies soit toujours plus ou moins la même : l'usage de ces technologies par *certains* États (les États démocratiques) pourrait être considéré comme légitime en vue de *certaines* finalités (la lutte contre le terrorisme). Autrement dit, seule la finalité – ou le bon usage – des technologies permettrait de fonder les justes limites de leur utilisation et de leur diffusion. Mais une telle limite repose sur un présupposé dont la nature idéologique a été relevée depuis longtemps déjà : les techniques seraient neutres, seules les finalités pour lesquelles leur utilisation a été envisagée permettant en fin de compte de les juger. Or, l'étude du cas tunisien [3] sur lequel nous nous sommes appuyés pour mener notre réflexion [4] permet non seulement de montrer que le développement et l'intégration des technologies de surveillance au cœur des dispositifs policiers dément avec force ce présupposé de la neutralité des technologies, mais montre surtout qu'il joue un rôle fondamental dans l'essor de ces technologies au sein même du système policier de Ben Ali, et, plus généralement, que la signification et la fonction mêmes d'un tel principe sont intrinsèquement liées à l'émergence de nouveaux modes de surveillance qui ne se laissent nullement appréhender à partir de la distinction entre État démocratique et État autoritaire. C'est donc le rôle et la signification de cette idée de neutralité des technologies dans l'essor de nouvelles formes de contrôle des populations que nous voudrions interroger en partant du cas tunisien, afin de montrer qu'elle cimente autant qu'elle dissimule des équilibres complexes entre les différents acteurs de ces systèmes de contrôle et de surveillance : les États, les entreprises, et les ingénieurs.

Les nouvelles technologies au service de la surveillance des populations

Peu après la chute de Ben Ali en janvier 2011, le directeur de l'Agence tunisienne de l'internet (ATI) nouvellement promu par le ministre des Communications, Moez Chakchouk, fait une déclaration fracassante à l'occa-

3 . Du fait de la situation de transition démocratique houleuse et chaotique qui prévaut en Tunisie, nous avons pu obtenir relativement facilement des informations sur le fonctionnement du système de surveillance technico-policier qui s'est développé sous Ben Ali et qui perdure en grande partie depuis le soulèvement. Cette étude de cas nous permettra d'ouvrir une réflexion plus large sur la fonction des technologies de surveillance dans l'évolution des modes de gestion des questions de sécurité dans le monde contemporain.

4 . Pour mener cette réflexion, nous nous sommes appuyés sur une quinzaine d'entretiens réalisés au mois de juin 2013 en Tunisie, à la fois avec des acteurs de ces systèmes de surveillance (ingénieurs et policiers, qui développent, pour la plupart, des stratégies de justification), des cyberdissidents et d'anciens opposants politiques à Ben Ali informés sur les méthodes de surveillance du net. Ces entretiens ont été étayés par des entretiens réalisés en France avec d'anciens employés d'entreprises de surveillance, ainsi que des membres d'ONG travaillant sur ces questions pour tenter de saisir l'implication et les pratiques de collaboration des entreprises occidentales avec des États autoritaires cherchant à développer leurs technologies de surveillance.

sion de la troisième Conférence annuelle des blogueurs arabes à Tunis [5], en affirmant que la Tunisie aurait servi sous Ben Ali de champ d'expérimentation à des entreprises occidentales pour tester leurs technologies de surveillance, non sans se rendre par la suite indirectement responsables de la répression, parfois même dans sa forme la plus extrême : la torture.

Par cette déclaration très stratégique, Moez Chakchouk prend d'abord position à l'égard de son prédécesseur au poste délicat de directeur de l'ATI, Kamel Saadaoui, en se distanciant des activités menées jusqu'alors par l'agence en matière de surveillance et de censure du net, et en estompant du même geste sa propre proximité avec le Ministère de la Communication avant la Révolution tunisienne. Mais il cherche ensuite à redorer l'image très détériorée de l'agence elle-même et notamment à réhabiliter l'idée de la neutralité de ses activités techniques. Pourtant, on ne peut que constater l'intégration de l'ATI au sein des dispositifs de surveillances progressivement mis en place par un régime policier basé sur la recherche de renseignement et dirigé par un chef d'État porteur d'une véritable idéologie moderniste qui le rend prêt à investir beaucoup dans ces nouvelles technologies, dont il est particulièrement féru. Et de fait, l'essor parallèle d'internet et des technologies de surveillance sous Ben Ali est fulgurant : dès le début des années 1990, la Tunisie lance le premier projet africain de développement du net. Au départ, il s'agit seulement d'un simple réseau académique restreint, pris en charge par l'Institut régional des sciences de l'informatique et des télécoms (IRSIT). Mais à partir de 1996, l'équipe de l'IRSIT est appelée à participer à la mise en œuvre d'un grand projet de commercialisation, qui mettra une longue année à voir le jour. Et pour cause, la commercialisation devra attendre la mise en place d'un premier dispositif de surveillance, géré par une cyberpolice qu'il s'agit à la fois d'intégrer au système de sécurité et de former aux technologies [6]. La création de l'ATI l'année même du lancement de la commercialisation est déterminante dans l'organisation de ce dispositif : en effet, l'Agence tunisienne de l'internet, à laquelle tous les fournisseurs d'accès doivent acheter leur accès à l'international, concentre tous les flux des réseaux en un unique point de passage ; l'installation de technologies de surveillance y permet donc un contrôle généralisé de l'activité sur internet, sans avoir à négocier avec les opérateurs – ce qui n'est pas le cas pour les écoutes téléphoniques, nous y reviendrons. Les ingénieurs

5 . « Interview avec le directeur de l'Agence tunisienne de l'internet », entretien de Yasmine Ryan (Al Jazeera) avec Moez Chakchouk ; version française disponible sur le site de Fhimt : http://www.fhimt.com/2011/10/06/interview-avec-le-directeur-de-lagence-tunisienne-de-linternet/ (mis en ligne le 6 octobre 2011, consulté le 16 juillet 2013).

6 . Entretien avec K. Saadaoui réalisé le 24 juin 2013 à Tunis dans les locaux de l'Instance nationale des télécommunications, dont il est devenu le président en 2011. En dépit de son lourd passé d'ancien président de l'ATI sous Ben Ali, Saadaoui a su retrouver un poste important après la Révolution tunisienne. La stratégie argumentative qui a été sienne lors de notre entretien, particulièrement difficile à obtenir, permet sans doute d'expliquer son maintien : K. Saadaoui prend sur lui l'entière responsabilité de la collaboration technique de l'ATI avec les services de police, tout en demeurant globalement muet sur les acteurs qui ont été impliqués dans le système.

de l'IRSIT, mobilisés pour développer les moyens techniques de cette cybersurveillance, n'intègrent pas le nouveau projet sans résistance : comme le raconte Kamel Saadaoui [7], une partie de l'équipe démissionne et s'exile. L'autre, dont il fait partie, accepte cette collaboration technique au projet de surveillance. Une fois le système mis en place, Ben Ali décide de supprimer l'IRSIT, faisant de l'ATI, à laquelle le chef de l'État accorde suffisamment d'importance pour lui avoir cédé sa villa place Pasteur à Tunis, l'unique agence en charge du contrôle technique de l'internet. La naissance de l'ATI et son intégration immédiate aux dispositifs de surveillance de la population développés par le régime s'inscrivent donc dès l'origine en porte-à-faux avec la thèse tenace de la neutralité des techniques : non pas seulement parce que le développement des technologies numériques s'est produit dans ce contexte au service d'une finalité répressive – il suffirait alors d'opposer l'usage émancipateur de ces mêmes technologies durant la « révolution du Jasmin » [8] – mais plus profondément parce que leur développement, leur mode de fonctionnement, leur inscription dans un tissu social et leur localisation géographique mêmes sont le fruit d'une construction sociale déterminée qui ne permet pas de les isoler de ce contexte social sans perdre purement et simplement leur signification.

Et en effet, le système de surveillance du net se laisse certainement décrire d'abord comme un système ultra-centralisé, organisé à la fois autour d'un réseau internet lui-même centralisé et d'une unique agence de contrôle de l'accès à internet, l'ATI. Mais la surveillance effective du net ne peut être cependant analysée qu'au regard de son intégration au sein même du système policier de Ben Ali. Elle est en effet directement mise en œuvre – et de manière concurrente – à partir des différents centres de cyberpolice installés au sein du ministère de l'Intérieur, des locaux de l'ancien parti hégémonique, le Rassemblement constitutionnel démocratique (RCD), et dans le palais de Carthage, au sein desquels les cyberpoliciers, grâce à la formation délivrée par les ingénieurs de l'ATI, seraient progressivement devenus suffisamment qualifiés pour gérer leur système de surveillance de manière autonome. Le dispositif de surveillance et de contrôle, qui se structure autour de l'ATI, de l'Agence tunisienne de communication extérieure (ATCE) – véritable agence de propagande garant de la bonne image du régime à l'étranger et chargée des demandes officielles de censure du net – et des différents organes de la police politique partiellement en concurrence, est intégralement sous le contrôle de Ben Ali [9]. Lui-même issu des services de sécurité au sein desquels il a fait toute

7 . *Idem*.

8 . Voir par exemple Lecomte R., « Internet et la reconfiguration de l'espace public tunisien : le rôle de la diaspora », *TIC & société* [En ligne], 3, 1-2, 2009 (http://ticetsociete.revues.org/702, mis en ligne le 12 janvier 2010. Consulté le 11 octobre 2012).

9 . Sur ce point, voir le rapport du Crisis Group en Tunisie, en date du 9 mai 2012 : « Tunisie : Lutter contre l'impunité, restaurer la sécurité. Rapport Moyen-Orient/Afrique du Nord n°123 » (http://www.crisisgroup.org/en/regions/middle-east-north-africa/north-africa/tunisia/123-tunisia-combatting-impunity-restoring-security.aspx?alt_lang=fr, consulté le 16 juil-

sa carrière avant d'accéder à la fonction présidentielle, il contrôle directement la Direction générale de la sûreté nationale (DGSN), qui rassemble l'essentiel de la police politique et la garde présidentielle, également intégrées au sein des forces de sécurité intérieures (FSI). Au sein de la DGSN, la direction des renseignements généraux (RG), la direction de la sûreté de l'État (DES) et la direction des services techniques (DST) ont également accès à l'ATI ; mais c'est la DST qui constitue à proprement parler le véritable centre de la cyberpolice politique, en assurant notamment le lien entre l'ATI et le ministère de l'Intérieur, en particulier par l'intermédiaire d'un personnage-clé de la cybersurveillance : le colonel et ingénieur N. Dhavi [10], qui incarne certainement le fonctionnement même d'un système réunissant ingénieurs et policiers, en relation directe avec le chef de l'État [11]. Enfin, selon toutes nos sources, la garde présidentielle a aussi disposé d'une cyberpolice directement reliée à l'ATI, ainsi que de systèmes d'écoute téléphonique – également sous contrôle de Ben Ali, secondé notamment par Ali Seriati, qui fut d'abord directeur de la DGSN durant dix ans avant d'accéder au poste de directeur de la garde présidentielle en 2001. Un système analogue se dessine pour les écoutes téléphoniques : ainsi, le RCD aurait disposé d'un système d'écoute ultrasophistiqué, placé sous l'autorité d'un ancien tortionnaire du nom de Ben Guebila [12]. Et de manière générale, le ministère de l'Intérieur, le palais de Carthage et le RCD ont chacun disposé de leur propre système d'écoute téléphonique [13]. Mais alors que la surveillance d'internet s'effectue par une connexion directe des différents organes policiers aux systèmes informatiques situés dans l'ATI – raison pour laquelle les ingénieurs de l'ATI affirmeront avoir pour l'essentiel ignoré la nature des interventions effectuées par la cyberpolice dont ils auraient pris connaissance suite aux plaintes déposées par les utilisateurs [14] –, les écoutes téléphoniques exigent pour leur part la collaboration des principaux opérateurs téléphoniques. Laquelle n'a guère été difficile à obtenir puisque ce sont pour l'essentiel les familles Ben Ali et Trebelsi, du nom de la

---

let 2013) ; voir également Séréni J.-P., « Après Ben Ali, quelle police en Tunisie ? », *Le Monde diplomatique* [en ligne], vendredi 1er avril 2011 (http://www.monde-diplomatique.fr/carnet/2011-04-01-Tunisie, consulté le 16 juillet 2013).

10. Le nom du « colonel-ingénieur » nous a été d'abord partiellement donné par K. Saadaoui, puis, complété et confirmé par un haut cadre de la police – ancien des renseignements généraux sous Ben Ali – dans un entretien réalisé le 25 juin 2013. Ce haut cadre n'a accepté de divulguer certaines informations qu'à la condition de voir son anonymat préservé.
11. Toujours selon le même cadre de la police mentionné plus haut (note 10), ses liens avec Ben Ali lui auraient valu d'être écarté de ses fonctions après le soulèvement, à l'instar d'un certain nombre de hauts cadres du ministère de l'Intérieur. Néanmoins, son nom n'apparaît pas dans la liste des 42 personnes écartées en 2011 et publiée sur le site de TunisiaWatch. *Cf.* TunisiaWatch, « Ministère de l'Intérieur Tunisie : liste des 42 personnes faisant objet de nomination ou de limogeage », 2 février 2011 (http://www.tunisiawatch.com/?p=4163, consulté le 16 juillet 2013).
12. Selon des propos rapportés par Mohamed Behnour, porte-parole du parti Ettakol, au journaliste Nicolas Beau. Entretien réalisé le 27 juin 2013.
13. Cette affirmation, qui nous a d'abord été donnée par le bloggeur et ancien journaliste de Nawaat, Ramzi Bettaieb, lors d'un entretien réalisé le 24 juin 2013, nous a été systématiquement confirmée dans tous nos entretiens, y compris par le haut cadre de la police.
14. Selon K. Saadaoui, entretien du 24 juin 2013.

seconde femme de Ben Ali, qui se sont emparées des principales entreprises de téléphonie, notamment à la faveur de la politique de libéralisation engagée en 2001 [15]. Reste que le développement et l'organisation de l'ATI – initialement conçue comme un simple réseau académique destiné à gérer la commercialisation d'internet avant de devenir l'unique agence de contrôle de son accès – ainsi que le rôle des principales entreprises de téléphonie dans les activités de censure et d'écoutes téléphoniques invitent très certainement à interroger l'intégration de nouveaux acteurs dans la gestion des affaires de sécurité : les grandes entreprises de haute technologie d'une part, déjà relevées par une partie de la littérature portant sur ces questions [16], et l'ingénieur – ou plus largement le technicien – d'autre part, dont la fonction demeure systématiquement occultée par celle des entreprises.

De nouveaux acteurs dans la gestion des questions de sécurité : les entreprises

Le rôle des entreprises de haute technologie se joue à de multiples niveaux : tout d'abord lorsque la surveillance étatique requiert une coopération des entreprises de téléphonie. Ainsi, même un État aussi centralisé que l'État tunisien ne peut guère, s'il veut s'insérer dans la mondialisation, se passer de la coopération des principaux opérateurs dans ses activités de surveillance. Pour ce faire, il a eu recours à la corruption massive des élites dirigeantes, en l'occurrence des familles Ben Ali-Trebelsi. Mais cette coopération aura exigé au minimum que les actionnaires minoritaires ferment les yeux sur les pratiques de leur entreprise. Il en fut ainsi pour ne prendre qu'un exemple qui a suscité bien des critiques, pour Orange (France Télécom), qui détient 49 % des parts du groupe Orange Tunisie, contre 51 % pour Marouane Mabrouk et sa femme Cyrine Ben Ali, la fille de Ben Ali [17].

---

15. Ainsi, Orange Tunisie a notoirement remporté en 2009 l'appel d'offre pour la troisième licence téléphonique 2G/3G du pays en s'associant avec le groupe de Marouane Mabrouk et de sa femme Cyrine Ben Ali, la fille de Ben Ali (Divona Télécom). Une stratégie qui a permis au consortium de se voir attribuer le marché téléphonique. Devenu PDG d'Orange Tunisie, Mabrouk possède avec sa femme 51 % des parts, Orange (France Télécom) en possédant 49 %. Ironie de l'histoire, le marché est remporté contre le groupe turc Turkcell, qui s'est lui-même associé à Mohamed Sakhr El Materi, marié à Nesrine Ben Ali, la fille de Leïla Trabelsi. Si l'on prend également en compte le rôle joué par Mohamed Sakhr El Materi, le « gendre préféré » de Ben Ali, qui devient président du conseil d'administration de Tunisiana lors de l'entrée de son groupe au capital de Tunisiana en janvier 2011, on perçoit l'étendue de l'emprise de la famille Ben Ali-Trebelsi sur les opérateurs télécom. *Cf*. notamment Tesquet O., « Ben Ali : les compromissions d'Orange en Tunisie », *Owni*, 03 mars 2011 (http://owni.fr/2011/03/03/ben-ali-les-compromission-dorange-en-tunisie/, consulté le 16 juillet 2013).
16. Voir en particulier Bigo D., Walker R.B.J. et chercheurs Elise, « Liberté et Sécurité en Europe : enjeux contemporains », *Cultures & Conflits* [En ligne], 61, printemps 2006 (http://conflits.revues.org/2040, mis en ligne le 17 mai 2006, consulté le 4 mai 2013).
17. Notons que c'est également cette même corruption qui a très probablement conduit les États-Unis à lâcher Ben Ali en 2011.

C'est également le rôle des entreprises qui vendent ces technologies aux États demandeurs et assurent par la suite la formation des cyberpoliciers ainsi que les activités de maintenance qui doit être interrogé. En Tunisie, des technologies de filtrage, acquises notamment auprès des entreprises Blue Coat System, NetApp [18] et très probablement McAfee (Smartfilter) [19] ont permis, sous couvert de la loi de 1998 relative au code de la Poste [20] interdisant les « envois qui sont de nature à porter atteinte à l'ordre et à la sécurité publics », de censurer de très nombreux sites internet de partis politiques d'opposition, d'information ou de défense des droits de l'Homme. Ces mêmes technologies de filtrage ont également rendu possible une première forme de surveillance des communications, avant que le gouvernement tunisien ne commence à acquérir auprès d'entreprises occidentales, à partir de 2006, des technologies de surveillance en profondeur des réseaux basées sur la technologie Deep Packet Inspection (DPI) qui lui ont permis non seulement de surveiller systématiquement et massivement le contenu des communications des internautes, mais également de le modifier. De multiples entreprises sont pointées du doigt pour avoir vendu sous Ben Ali ces technologies de filtrage plus ou moins avancées : McAfee, Bluecoat Inc et NetApp Inc (États-Unis), mais aussi, avec moins de certitude, Ultimaco et Detica pour les technologies de filtrage, et les entreprises Nokia Siemens Networks, ETI A/S (Danemark), Blue Coat Systems, NetApp, Ultimaco (Grande-Bretagne) et Trovicor (Allemagne) pour l'installation de système de surveillance de l'activité des internautes [21] ; les Anonymous parlent également de Bull [22] (France). Néanmoins, ces dernières informations sont étrangement difficiles à vérifier : entre les clauses de confidentialité des contrats signés avec les entreprises [23], le désintérêt des hauts

18. L'implication de ces deux entreprises nous a été confirmée par l'actuel directeur de l'ATI, M. Chakchouk, lors de l'entretien réalisé dans les locaux de l'ATI le 25 juin 2013. Pour connaître les entreprises soupçonnées d'avoir vendu ces technologies en Tunisie, voir Wagner B., *Exporting Censorship and Surveillance Technology*, La Haye, Hivos, 2012, p. 7.
19. *Cf*. OpenNet Initiative, « Internet filtering in tunisia in 2005: A country study », novembre 2005 : https://opennet.net/studies/tunisia (mis en ligne le 10 juin 2008, consulté le 16 juillet 2013).
20. Loi n° 98-38 du 2 juin 1998 relative au Code de la Poste, art. 20 (http://www.intt.tn/upload/txts/fr/loi_192.pdf, consulté le 27 janvier 2014).
21. *Cf*. Wagner B., *Exporting Censorship and Surveillance Technology*, *op. cit.*, p. 8 ; Silver V., « Ammar 404 : les dessous de la société de la surveillance dans la Tunisie de Ben Ali », *Fhimt* : http://www.fhimt.com/2011/12/16/ammar-404-les-dessous-de-la-societe-de-la-surveillance-dans-la-tunisie-de-ben-ali/ (mis en ligne le 16 décembre 2011, consulté le 16 juillet 2013).
22. Si l'on en croit les Anonymous, l'entreprise qui aurait fourni les systèmes de surveillance de masse des communications est la société Bull. L'information est fondée sur une interprétation des images du Manuel Amesys-Eagle-Glint, dont les illustrations fournies portent traces d'une surveillance de la banque tunisienne BIAT. Elle nous a été démentie par K. Saadaoui et M. Chakchouk ; mais il pourrait s'agir des machines de test installées en Tunisie, dont parle M. Chakchouk qui affirme que, n'ayant fait l'objet d'aucun contrat avec l'ATI, elles ont été renvoyées à leur entreprise d'origine après les évènements de 2011. *Cf*. « Les Anonymous se liguent contre Bull #OpBull-s02e02 », *Fhimt* : http://www.fhimt.com/2012/05/27/les-anonymous-se-liguent-contre-bull-opbull-s02e02/ (mis en ligne le 27 mai 2012, consulté le 16 juillet 2013) ; voir également la publication du Manuel Eagle-Glint d'Amesys par Wikileaks : http://wikileaks.org/spyfiles/files/0/99_AMESYS-EAGLE-GLINT-Operator_Manual.pdf

cadres de l'administration étatique ou l'amnésie qui règne autour de cette interrogation, une large zone d'ombre recouvre l'activité de ces entreprises, qui exercent une forte pression pour maintenir cet anonymat [24]. Reste que ces éléments, et la difficulté même d'obtenir des informations, dessinent les grands traits d'une forme spécifique de coopération des entreprises et de l'État en matière de surveillance des communications : une coopération impulsée et dirigée par l'État, impliquant une multiplicité de sociétés de haute technologie dans un espace de forte mise en concurrence, et contribuant à intégrer ces acteurs privés dans la zone de pénombre propre aux questions de renseignement et de secret-défense.

Cette coopération s'est effectivement exercée à deux niveaux : non seulement les entreprises de téléphonie ont dû fournir un accès à leurs réseaux en ce qui concerne les écoutes téléphoniques, mais la collaboration des entreprises et des États s'est avérée étroite au niveau de la création et du développement même des technologies de surveillance – non sans résister à la thèse d'une simple application abusive de technologies préexistantes et commercialisées dans d'autres buts par les entreprises. Ainsi, K. Saadaoui raconte-t-il qu'il a négocié pour l'ATI à partir de 2006 avec des entreprises dont il refuse de dévoiler le nom, pour acquérir des technologies susceptibles de répondre aux besoins de la cyberpolice. Autrement dit, les entreprises ont développé des machines adaptées aux objectifs de la cyberpolice, selon un cahier des charges précis [25]. De même, si l'affirmation de M. Chakchouk selon laquelle les entreprises auraient utilisé la Tunisie comme « cobaye » pour tester leurs nouvelles technologies, installées dans les locaux de l'ATI sans aucun contrat de vente, vise à l'évidence à déresponsabiliser l'agence, elle n'en indique pas moins l'existence d'un processus de développement des technologies « sur le terrain ». Un processus confirmé par ailleurs dans le cadre de la vente de technologies similaires à la Libye de Kadhafi par un ancien employé de Qosmos [26], qui raconte comment les logiciels de captation et de traitement des données transitant par les réseaux ont été produits d'abord au cas par cas [27], en fonc-

23. En effet, l'ancien directeur de l'ATI, K. Saadaoui, qui a été en charge de négocier et signer certains de ces contrats, notamment à partir de 2006, et son nouveau directeur, M. Chakchouk, refusent de transmettre le nom de ces entreprises, au motif d'une clause de confidentialité. Entretiens avec K. Saadaoui le 24 juin 2013 et avec M. Chakchouk le 25 juin 2013.
24. M. Chakchouk laisse même entendre que les entreprises auraient fait pression contre la suppression de l'ATI, notamment par crainte qu'elle donne lieu à une ouverture des archives. Entretien du 25 juin 2013.
25. Entretien du 24 juin 2013.
26. Entretien du 3 octobre 2013 à Paris avec James Dunne, ancien responsable de la documentation technique au sein de Qosmos. James Dunne est actuellement en procès avec son ancien employeur, Qomos, après avoir été licencié pour faute grave en 2012.
27. Le projet Eagle, du nom de la technologie de traitement de l'information développée par la société française Amesys, qui commande elle-même à Qosmos un certain nombre d'outils pour le développement d'un système global de surveillance mis au service de l'intelligence libyenne, est lancé au sein de Qosmos en avril 2007 – le contrat entre Amesys et les autorités libyennes est signé la même année selon le « Communiqué de la direction de la communication d'Amesys du 1er septembre 2011 ». Soit plus ou moins à la même époque où K. Saadaoui

tion d'un cahier des charges remis par les autorités libyennes d'abord, puis en fonction de nouvelles demandes résultant de leur application sur le terrain et faisant progressivement évoluer les machines.

Il ne semble guère probable que la vente de technologies de surveillance par des entreprises d'État, ou des entreprises soumises à un certain contrôle étatique, à des États étrangers, qui plus est à des États autoritaires, ait pu se réaliser sans l'aval politique des gouvernements en place. Le cas tunisien demeure sur ce point très obscur, à la fois en raison du grand nombre d'entreprises et, par suite, du nombre d'États concernés, et de l'incertitude qui entoure les contrats passés. Néanmoins, le cas de la vente de technologies similaires par Amesys aux autorités libyennes confirme ce point, puisque ce sont des accords passés entre les gouvernements français et libyen en matière de lutte contre le terrorisme qui ont permis la vente très contrôlée de ces technologies [28]. Un lien très étroit que confirme par ailleurs l'effort du gouvernement français visant à placer l'activité des entreprises concernées sous le sceau du secret-défense, ainsi que l'autorise la loi de programmation militaire 2009-2014, présentée par le ministre de la Défense, Hervé Morin, qui a permis à l'entreprise Qosmos d'obtenir le statut d'entreprise protégée par le secret-défense en 2009 [29].

Néanmoins, si d'un côté une telle collaboration ne fait aucun doute, de l'autre, les entreprises comme les États maintiennent des stratégies de communication insistant sur l'autonomie des entreprises et des intérêts commerciaux poursuivis. Ainsi, suite au scandale mondial provoqué par la révélation de la vente de ces technologies de surveillance à des États autoritaires ou non démocratiques, divers efforts politiques et juridiques ont été fournis en vue d'encadrer leur exportation. Sans qu'il nous soit possible de développer ce point dans le cadre de cet article, notons seulement que deux types de stratégies ont été suivies sur cette question : une stratégie juridico-politique, qui tend à instituer progressivement un régime de contrôle juridique de ces biens, comme le vote du *Global Online Freedom Act* de 2006 aux États-Unis [30] ou encore

négocie auprès d'entreprises occidentales de nouvelles technologies plus perfectionnées pour la surveillance du net tunisien. De ce point de vue, la première décennie du XXIe siècle semble avoir été un moment essentiel dans le développement « sur le terrain » de ces technologies de surveillance.

28. Un point nettement souligné par le « Communiqué de la direction de la communication d'Amesys du 1er septembre 2011 », versé au dossier de l'instruction de l'affaire Amesys, née de la plainte de la Fédération internationale des droits de l'homme et de la Ligue des Droits de l'Homme le 19 octobre 2011. Ce point, par ailleurs démontré par l'enquête du journaliste Paul Moreira dans un reportage diffusé sur Canal + le 14 mars 2012, nous a été confirmé par James Dunne, dans l'entretien du 3 octobre susmentionné.
29. Selon James Dunne, à partir du printemps 2009, Qosmos reçoit une enveloppe de 250 000 euros pour payer les frais de sécurisation de l'entreprise (blindage des fenêtres et des portes, protection renforcée des salles, caméras de surveillance, etc.) Entretien réalisé le 3 octobre 2013.
30. Le *Global Online Freedom Act* de 2006 prévoit notamment l'interdiction d'exportation de ces technologies vers des pays comme la Syrie et l'Iran.

l'Arrangement de Wassenaar de 1996, qui consiste en un régime multilatéral de contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage, signé à l'origine, en 1996, par 33 États [31] ; et une stratégie politico-économique, sur le modèle de la *Global Network Initiative* (GNI) [32], qui cherche à inciter les entreprises à une forme d'autorégulation. Dans ce second cas, il est intéressant de noter que c'est alors pour l'essentiel contre les pressions des gouvernements exigeant des entreprises qu'elles contribuent aux politiques de surveillance des activités dites criminelles ou terroristes sur internet que les organisations non gouvernementales comme le GNI prétendent résister [33]. En revanche, les efforts de règlementation qui se développent au niveau international semblent bien d'avantage mettre en jeu (et en doute) la capacité des États à imposer des normes contraignantes aux entreprises exportant des technologies de surveillance à des États susceptibles d'en faire un usage militaire ou répressif. Un renversement de point de vue qui reflète deux pans de la réalité actuelle, mais qui témoigne, en dernière instance, d'une relative accointance entre les intérêts économiques et les objectifs sécuritaires des États et les intérêts strictement économiques des entreprises mêmes. Et sous cet angle, comme « il n'y a pas de divergence significative entre les intérêts des États et ceux des acteurs non étatiques, la technologie DPI continuera à se diffuser dans les réseaux mondiaux d'Internet [34] ». Une diffusion qui ne peut, en outre, que s'accentuer du fait du statut très ambivalent de ces technologies : technologies de gestion de réseaux, de ciblage commercial, de surveillance. Il est clair que la pluralité des applications possibles de ces outils, qualifiés juridiquement de « technologies à double usage », multiplie les acteurs susceptibles de faire pression en faveur de leur diffusion. Mais on peut enfin y voir le trait central d'un nouveau système de gestion des ques-

31. Signé en 1996, l'Arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage constitue l'un des principaux outils juridiques visant à réguler l'exportation des technologies à double usage au niveau international. Il n'est pas contraignant sur le plan juridique et repose donc sur la bonne volonté des États signataires (http://www.wassenaar.org). Voir également Matelly S., « Un code de conduite européen pour sécuriser les exportations ? Le cas des exportations d'armes en Europe », *Cahiers Irice* [en ligne], 6, Actes de la journée d'études du 4 décembre 2009, Université Paris I Panthéon-Sorbonne (http://irice.univ-paris1.fr/spip.php?article599#, consulté le 16 juillet 2013).
32. La création, en 2008, de l'organisation non gouvernementale Global Network Initiative, cofinancée pour l'essentiel par de grandes multinationales (Microsoft, Yahoo ! Google, etc.), d'autres ONG (Human Rights Watch, etc.) et des universités, et visant à lutter contre la censure sur internet et la protection de la vie privée, s'inscrit clairement dans le cadre de la seconde stratégie.
33. Ainsi, sur le site du GNI est annoncé : « GNI exists to provide guidance to the ICT industry and its stakeholders on how to protect and advance the human rights of freedom of expression and privacy when faced with pressures from governments to take actions that infringe upon these rights. » (voir le site de Global Network Initiative, *Core commitements* : http://www.globalnetworkinitiative.org/faq/index.php, consulté le 27 janvier 2014).
34. « As there is no significant divergence of interests between state and non-state actors, DPI technology will continue to spread throughout global Internet networks ». Wagner B., "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'", *Global Voices Advocacy Defending Free Speech Online*, 2009 (http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf, consulté le 27 janvier 2014).

tions de sécurité associant plus intimement l'État et les grandes entreprises de haute technologie, et qui repose sur le présupposé de la neutralité des technologies et le caractère apolitique des activités techniques que leur développement et leur application supposent, qui se traduit ensuite dans des discours concordants des autorités politiques et des entreprises concernant l'autonomie des entreprises et de leurs stratégies commerciales – qu'il s'agisse de préserver cette autonomie contre l'État ou que l'on en dénonce au contraire les objectifs purement économiques et l'indifférence éthique.

La double fonction de l'ingénieur et du technicien dans l'essor des nouveaux dispositifs technologiques de surveillance

Dans ce cadre, l'ingénieur – ou plus largement le technicien qui participe à la fois au développement des technologies de surveillance et à leur mise en application – constitue un nouvel acteur dont on ne saurait trop souligner l'importance dans le développement de ces nouveaux dispositifs de surveillance. En Tunisie, ce rôle est évidemment signalé par le développement et la fonction stratégique de l'ATI au sein des dispositifs de contrôle. Mais il est plus largement en jeu dans l'essor même de l'internet en Tunisie, qui s'est appuyé sur la solide formation d'ingénieurs et de chercheurs tunisiens en informatique dans les années 1990, dispensée pour l'essentiel à l'étranger, notamment dans les universités et les écoles françaises [35]. Or ce rôle, systématiquement occulté par la mise en cause des entreprises du net ou de technologies de surveillance, se joue selon nous à un double niveau : les ingénieurs interviennent d'abord dans la création et le fonctionnement des machines. Ils permettent ensuite de « neutraliser » l'ensemble du dispositif, ou plus exactement, de faire du dispositif liant l'État, les écoles d'ingénieurs ou les centres de recherche [36], les professionnels de la sécurité, les entreprises du net et les entreprises de technologies de surveillances, un dispositif neutre, dont les excès ou les abus ne résultent que d'un usage dévoyé, et par suite, un dispositif peu questionnable en tant que tel. Autrement dit, les techniciens, les ingénieurs et l'ensemble des experts techniques participent à la production d'un système supposément neutre d'outils technologiques dont ils fixent la signification en faisant des logiciels de traitement de l'information de simples outils de gestion des réseaux liés au fonctionnement même d'internet, politiquement neutres (comme doit en témoigner leur très large commercialisation) et dont on ne saurait au mieux juger que le mauvais usage et non les formes d'économie de pouvoir dont ils sont les supports. Ainsi, K. Saadaoui souligne-t-il constamment l'absence totale de responsabilité des ingénieurs de l'ATI sous Ben Ali, en distinguant nettement mission technique et mission policière, ce

35. Renaud P., « Internet au Maghreb et au Machrek. De la "Recherche et Développement" à l'appropriation sociale », in Mezouaghi M. (ed.), *Le Maghreb dans l'économie numérique*, Paris, Maisonneuve & Larose, 2007, p. 47.
36. C'est ce qu'illustre selon nous l'origine d'une entreprise comme Qosmos, née de la volonté de deux doctorants et de leur professeur de commercialiser le produit de leurs recherches. Entretien avec James Dunne réalisé le 3 octobre 2013.

qui lui permet d'endosser seul la responsabilité d'une collaboration avec le ministère de l'Intérieur en vertu de sa position hiérarchique [37]. Et M. Chakchouk, qui présente avec succès aux médias l'image d'une ATI soucieuse de résister aux pressions exercées en faveur de la censure par certains acteurs, justifie cette position au nom de la « neutralité de l'ATI » : « nous ne faisons pas de politique [38] ». Sans doute peut-on être tenté d'établir un parallèle entre le rôle joué par les entreprises fournissant des technologies de surveillance aux États qui en font usage à des fins répressives et celui des entreprises de l'armement. Mais c'est précisément manquer la spécificité de ce processus de neutralisation des technologies de contrôle et des tâches effectuées par les ingénieurs et les entreprises, qui permet la mise en place d'un système de surveillance non pas seulement généralisé, mais impliquant surtout une multiplicité d'acteurs – policier, experts techniciens et entreprises participant de la très large diffusion de ces technologies – dont les liens et les divers dispositifs qui les intègrent sont systématiquement occultés.

Les technologies de surveillance au cœur d'un nouveau mode de gestion des questions de sécurité

Le système de surveillance des communications qui s'est progressivement mis en place sous Ben Ali doit donc être analysé à un double niveau : d'un côté, il s'inscrit dans le cadre de la politique de contrôle de la population caractéristique de l'État policier qui s'est notamment traduite en Tunisie par une omniprésence policière, par la domination du ministère de l'Intérieur sur toutes les autres administrations, un contrôle global de l'information et un quadrillage de la société par des cellules du parti, des comités de quartiers ou des indicateurs de police [39]. Et de ce point de vue, les systèmes de surveillance des communications constituent un outil supplémentaire au service d'un régime fondé sur le contrôle policier de la population et la corruption de son élite économico-politique dirigeante, relais essentiel dans le bon fonctionnement des dispositifs de contrôle eux-mêmes. Mais d'un autre côté, ce système témoigne d'une évolution beaucoup plus générale des formes de gestion des questions de sécurité à l'échelle mondiale, qui se traduit très différemment au sein d'États de droit démocratiques ou d'États autoritaires, mais qui lie dans les deux cas des acteurs, des outils et des dispositifs similaires voire identiques.

Depuis quelques années déjà, d'importants travaux sur la Tunisie ont montré que le caractère policier du régime de Ben Ali ne pouvait être dissocié de l'effort mené par ce dernier en vue d'inscrire la Tunisie dans la mondialisation [40], afin de permettre à une élite corrompue de profiter d'une politique

37. Entretien réalisé le 24 juin 2013.
38. Entretien réalisé le 25 juin 2013.
39. Sur ce point, voir en particulier Hibou B., *La force de l'obéissance*, Paris, La Découverte, 2006, p. 95 et ss. ; Camau M., Geisser V., *Le syndrome autoritaire. Politique en Tunisie de Bourguiba à Ben Ali*, Paris, Presses de Sciences Po, 2003, chapitre 5.

économique susceptible d'attirer des capitaux. Et sous cet angle, l'acquisition des technologies de surveillances par le régime de Ben Ali ne traduit pas seulement le caractère systématique de l'État policier, mais également un double effort visant à moderniser l'économie et à promouvoir l'image publique du régime auprès de l'opinion internationale [41], dans le cadre d'une politique économique de prédation. Et ce, car l'usage des technologies de surveillance de masse procède d'une stratégie d'économie en termes de répression pure et simple, ainsi qu'en termes de visibilité du contrôle, qui ne peut être isolée de l'évolution générale de la gestion des questions de sécurité dans un monde globalisé. Ainsi, contrairement aux forces de police qui sont pléthoriques en Tunisie [42], c'est une équipe assez restreinte, bien loin des chiffres fantasmés qui circulent (on parle souvent de six cents personnes), qui se charge de la surveillance du net : cyberpoliciers et techniciens n'auraient, au plus haut des activités d'espionnage, jamais dépassé cent vingt personnes – avec à peu près soixante-dix personnes au sein de l'ATI même [43]. Une équipe qu'il faut resituer dans l'importante masse policière engagée par ailleurs par l'État tunisien pour saisir la nature du régime, mais qui procède, nous semble-t-il, du développement parallèle d'une autre stratégie de surveillance : une surveillance moins visible, moins coûteuse en hommes et qui tend progressivement à s'automatiser ; une surveillance technologique qui s'articule intrinsèquement avec le double effort de modernisation technique et économique déjà évoqué, et qui doit donc relativiser l'idée d'après laquelle ces technologies sont de simples techniques coercitives [44]. Cette stratégie d'économie de moyens se traduit en termes d'image ou de vitrine publique : sans doute le caractère répressif du pouvoir tunisien n'est guère ignoré que par ceux qui le veulent bien sous Ben Ali ; sans doute aussi, les multiples violations des libertés individuelles et de la vie privée sont-elles également régulièrement dénoncées. Néanmoins, la Tunisie va pouvoir faire perdurer son image d'État modèle en matière de réformisme [45], notamment par son effort de modernisation économique et technologique qui la conduit à faire appel à des bailleurs de fonds et à des entreprises étrangères, et par sa stabilité politique [46]. Deux éléments dans lesquels le développement des technologies de surveillance joue un rôle central, puisqu'il incarne la modernisation du pays tout en assurant une forme de

40. *Cf*. Camau M., Geisser V., *Le syndrome autoritaire. Politique en Tunisie de Bourguiba à Ben Ali*, *op. cit.* ; Camau M., « Tunisie : vingt ans après. De quoi Ben Ali est-il le nom ? », *L'Année du Maghreb*, IV, 2008, p. 4. (http://anneemaghreb.revues.org/480, mis en ligne le 1er octobre 2011, consulté le 16 juillet 2013).
41. Wagner B., *Exporting Censorship and Surveillance Technology*, *op. cit.*, p. 12.
42. Ainsi, Béatrice Hibou note que la présence policière est estimée entre 80 000 selon les observateurs étrangers et 133 000 selon l'opposition tunisienne – ces derniers chiffres étant certainement exagérés – pour dix millions d'habitants. Hibou B., *La force de l'obéissance*, *op. cit.*, pp. 95-96.
43. Entretien avec K. Saadaoui réalisé le 24 juin 2013.
44. Ce qui constitue la thèse générale de l'ouvrage de Hibou B., *La force de l'obéissance*, *op. cit.*
45. Sur le sens et l'histoire du réformisme tunisien, *cf*. Hibou B., « Le réformisme, grand récit politique de la Tunisie contemporaine », *Revue d'histoire moderne et contemporaine*, 56-4 bis, mai 2009, pp. 14-39.
46. *Ibid*., p. 37.

contrôle plus acceptable aux yeux de l'opinion internationale – la lutte contre le terrorisme islamiste se chargeant de justifier les formes de répression trop ouvertement violentes. Et sous cet angle, l'analyse du système de surveillance qui s'est progressivement développé dans le pays doit être effectuée dans le cadre plus large d'une économie générale du pouvoir à laquelle on pourrait attribuer, à la suite de Michel Camau, le nom même de Ben Ali qui s'avère « en définitive le nom d'un mode antidémocratique d'intégration au capitalisme mondialisé [47] ».

Mais plus largement encore, l'étude des technologies de surveillance développées sous Ben Ali, des dispositifs dans lesquels elles s'inscrivent et des différents acteurs qui y sont engagés dessine la mise en place de nouvelles politiques de sécurité associant une multiplicité d'acteurs dans un espace mondialisé et qui se fondent sur la diffusion relativement banalisée des technologies de surveillance. Ces politiques de sécurité ont été assez largement appréhendées, dans la littérature anglo-saxonne, au moyen de la notion de sociétés de surveillance ou de sociétés de contrôle [48], en vue notamment d'insister sur la substitution de la répression pure et simple par l'expansion de la surveillance dans les sociétés contemporaines, et pour souligner le caractère généralisé et décentralisé d'un tel contrôle qui n'est plus, s'il l'a jamais été, le monopole de l'État. Sans prendre position dans ces débats qui exigeraient une longue analyse, notre étude devrait contribuer à souligner deux points importants : d'une part, ces nouveaux systèmes de surveillance se fondent sur un principe de neutralité technologique, qui ne permet pas seulement de légitimer leur expansion à des fins policières [49], mais plus profondément de masquer complètement la pluralité d'acteurs engagés dans cette expansion, ainsi que la forte intégration de leurs fonctions qui demeurent pourtant appréhendées comme des activités et des intérêts autonomes. Et de ce point de vue, il est certainement important d'interroger la pertinence du critère généralement retenu, tant comme critère politique que comme critère éthique, entre bon et mauvais usage des technologies de surveillance : celui de la finalité légitime – soit, concernant spécifiquement la surveillance policière, la lutte contre le terrorisme. Depuis longtemps déjà, la dangereuse flexibilité d'un critère tel que la « lutte contre le terrorisme » fait l'objet de critiques [50]. Mais concernant l'implication des technologies de surveillance dans cette lutte, c'est l'articulation des fins et des moyens qu'un tel critère sous-tend qui pose question, en tendant à faire des

47. Camau M., « Tunisie : vingt ans après. De quoi Ben Ali est-il le nom ? », *op. cit.*
48. Sur ce point, voir en particulier Lyon D. (ed.), *Surveillance Studies. An overview*, Cambridge, Polity, 2007 ; *Theorizing surveillance. The panopticon and beyond*, Portland, Willan publishing, 2006. Voir aussi Deleuze G., « Post-scriptum sur les sociétés de contrôle », in *Pourparlers 1972-1990*, Paris, Les Éditions de Minuit, 1990, pp. 240-247.
49. De même Gary T. Marx souligne-t-il, dans le cadre de son travail sur les prisons, que la « scientifisation du travail de la police offre en même temps des méthodes nouvelles et les moyens de légitimer le pouvoir de la police ». Marx G. T., « La société de sécurité maximale », *Déviance et Société*, 12-2, 1988, p. 149.
50. Voir par exemple Bonelli L., « L'exception ordinaire. Services de renseignement et anti-terrorisme dans les démocraties libérales », *Erytheis*, 2, novembre 2007, p. 140.

technologies de surveillance un moyen neutre, au service de fins pouvant être elles-mêmes bonnes ou mauvaises. D'autre part, il convient de relativiser l'idée d'une disparition ou d'un effacement de l'État dans l'essor de ces nouvelles formes de surveillance – une idée que traduisent les notions deleuziennes de société et de technologie de contrôle [51]. Car non seulement l'État tunisien est le principal acteur de la mise en place de ces nouvelles technologies et dispositifs de surveillance, ce qui pourrait d'ailleurs être attribué au caractère autoritaire du régime, mais en outre, les États demeurent très largement impliqués dans les contrats commerciaux signés par les entreprises qui exportent ces technologies, de même que le développement de liens toujours plus étroits entre les écoles d'ingénieurs et les entreprises ne sauraient être compris que dans le cadre de politiques publiques. Autrement dit, et contrairement à la thèse d'après laquelle nous assisterions à l'émergence de sociétés de contrôle généralisées qui ne s'ordonnent pas à une finalité unique et imposée par l'État [52], il nous semble que l'État demeure à la fois le référent et le point de liaison central de ces nouvelles stratégies de sécurité.

Le principe de neutralité technologique et l'expansion des technologies de surveillance

Il convient, pour conclure, de revenir sur le principe de neutralité technologique, qui fonde et organise selon nous les nouvelles formes de gestion des questions de sécurité à l'heure de la mondialisation. Ce principe a effectivement, de longue date, été critiqué par un courant important de la littérature portant sur les techniques. Ainsi, des auteurs comme Martin Heidegger ou Jacques Ellul ont-ils déjà largement déconstruit les théories déterministes de la technique, qui font de cette dernière un moyen neutre (et apolitique) au service de finalités naturelles et relativement immuables, et dont le développement se produit de manière autonome, dans le sens du progrès de l'histoire. Au contraire, pour Heidegger ou pour Ellul, la technique est considérée comme un phénomène dont le développement est autonome, mais surtout essentiellement orienté vers la domination [53]. Sans doute cette lecture a-t-elle eu le mérite de refuser l'idée de neutralité de la technique ; mais par son affirmation d'une essence relativement immuable de la technique, elle ne permet pas de saisir les liens qui la soudent à l'organisation sociale au sein de laquelle elle émerge. De ce point de vue, l'approche constructiviste de la technique défendue par Andrew Feenberg, qui met en lumière la grande variété des groupes sociaux et des alliances sociales qui interviennent dans le développement de la technique dans le cadre d'un questionnement politique large [54], nous semble beaucoup plus pertinente pour tenter de saisir à la fois la signifi-

51. Deleuze G., « Post-scriptum sur les sociétés de contrôle », *op. cit.*
52. Voir par exemple Lyon D., *Surveillance Studies. An overview*, *op. cit.*, p. 12.
53. Cf. Heidegger M., « La question de la technique », in *Essais et conférences*, Paris, Gallimard, 1958, pp. 9-48 ; Ellul J., *Le Système technicien*, Paris, Calmann-Lévy, 1977.
54. Feenberg A., *(Re)penser la technique. Vers une technologie démocratique*, Paris, La Découverte/Mauss, 2004, p. 34.

cation politique de ces nouveaux outils et dispositifs de surveillance et le rôle joué par l'idée de neutralité technologique qui perdure. Dans ce cadre théorique, il convient alors non seulement de souligner le rôle joué par les États et les services de police, les écoles et les ingénieurs, les grandes entreprises de haute technologie numérique et les entreprises du net, dans le développement de ces outils et dispositifs de surveillance, mais surtout d'analyser la forme prise par leur « collaboration », qui se caractérise à la fois par leur forte intégration au sein de dispositifs de coopération organisés et par un jeu de renvoi dans lequel chacun semble totalement autonome vis-à-vis de l'autre. Or, cette collaboration exige un réinvestissement de l'idée de neutralité technologique, qui ne permet pas tant de légitimer des décisions politiques en masquant leur caractère politique, conformément aux analyses habermassiennes portant sur la science et la technique comme idéologie [55], que de masquer le fait même de la coopération de ces acteurs, et la diffusion très large qu'implique le développement de ces nouvelles technologies de contrôle dans l'ensemble des sociétés s'insérant dans la mondialisation. Et de ce point de vue, il nous semble que certains acteurs – les ingénieurs ou les experts techniciens – jouent une fonction spécifique dans la construction même de la signification de l'idée de neutralité technologique et dans le processus de neutralisation de l'ensemble du dispositif.

55. Habermas J., *La technique et la science comme « idéologie »*, Paris, Gallimard, 1973.