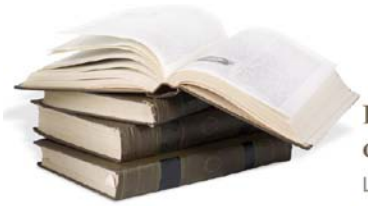

Le Dictionnaire encyclopédique
de l'administration publique
La référence pour comprendre l'action publique

CYBERSURVEILLANCE

Monica Tremblay, Agente de recherche
École nationale d'administration publique
monica.tremblay@enap.ca

La cybersurveillance est un mécanisme de surveillance de personnes, d'objets ou de processus qui repose sur les nouvelles technologies et qui s'exerce à partir et sur des réseaux d'information, tel Internet. Elle vise à faciliter la surveillance, compte tenu de la quantité, de la rapidité ou de la complexité de l'information à traiter. Tout comme la surveillance, elle renvoie à des activités de collecte et d'analyse d'informations poursuivant diverses finalités, notamment prévenir certains risques, orienter les conduites humaines et trouver des responsables en cas de problème (Commission de l'éthique de la science et de la technologie, 2008; Cahen, s.d.; Boudreau, 2006).

Le terme *cybersurveillance* fait partie d'une catégorie de mots récents qui se sont insérés dans le vocabulaire depuis l'avènement de la cybernétique en 1948, et de façon plus marquée depuis l'essor important dans les années 1970 des réseaux numériques de communication. Plusieurs mots ont vu le jour surtout à la faveur de l'accessibilité d'Internet au milieu des années 1990. Le préfixe *cyber-* est ainsi juxtaposé à des activités qui ne sont pas nouvelles, mais qui se réalisent dans l'espace virtuel à l'aide de l'informatique et des télécommunications.

La cybersurveillance s'est installée dans notre quotidien au gré de l'évolution, du raffinement et de l'ubiquité des technologies de l'information afin de mieux gérer d'innombrables risques et d'assurer la sécurité des personnes, des lieux, des informations, des infrastructures et des processus dans divers milieux (Commission nationale de l'informatique et des libertés, 2004; Leman-Langlois et Ouimet, 2006; Bajc, 2007). La cybersurveillance s'est intensifiée depuis les attentats terroristes internationaux, tels que les attaques perpétrées aux États-Unis le 11 septembre 2001 ou dans le métro de Londres en juillet 2005. Le besoin de mettre en place des mesures visant à minimiser les risques qui menacent la sécurité d'un État et de sa population et les craintes qu'ils suscitent s'est alors imposé. Sous un autre angle, la cybersurveillance est aussi de plus en plus instaurée par des gouvernements en tant que mécanisme qui aide à réaliser certaines tâches administratives relatives à la gestion de la santé, du bien-être, de l'éducation et de la sécurité de la population (Commission de l'éthique de la science et de la technologie, 2008). Les entreprises soucieuses de protéger certaines informations, de surveiller le comportement de leurs employés ou de leur clientèle y ont également recours. Des organisations de la société civile et des citoyens peuvent aussi se servir des nouvelles technologies de l'information afin de surveiller les faits et gestes des autorités ou des entreprises pour ensuite dénoncer des conduites jugées inacceptables (Häyhtiö et Rinne, 2009; Leman-Langlois et Ouimet, 2006; Boudreau, 2006). Enfin, dans la poursuite de leurs objectifs, les délinquants et les groupes criminels sont aussi susceptibles de recourir à la cybersurveillance.

La cybersurveillance s'exécute par la collecte d'informations au moyen d'outils technologiques et de logiciels de surveillance. Ces informations, souvent nombreuses (événements, messages, déplacements, accès, etc.), sont enregistrées et passent par un processus d'analyse informatisé dont le résultat consiste en une information bonifiée. C'est ce produit filtré qui facilite le travail du surveillant et qui peut être utilisé dans les décisions visant à orienter les conduites. Suivre le comportement d'individus en temps réel sur une période précise et à travers le monde est désormais possible (Bajc, 2007). L'interception et l'analyse des messages électroniques est un exemple courant de cybersurveillance (Cahen, s.d.; Commission nationale de l'informatique et des libertés, 2004). D'envergure internationale, ECHELON, un projet d'espionnage électronique lancé par plusieurs pays, conçu et coordonné par la National Security Agency des États-Unis et révélé au grand jour en 1988, permet aux gouvernements participants d'intercepter les télécommunications, numériques ou non, transmises sur les différents réseaux mondiaux. De puissants ordinateurs analysent une quantité phénoménale d'informations captées par différents systèmes afin d'extraire les messages pouvant révéler des renseignements stratégiques, représentant notamment un risque pour la sécurité nationale. Les exemples de cybersurveillance faite par les États sont nombreux, notamment en ce qui concerne la lutte contre le vol d'identité, le piratage, le terrorisme, les fraudes économiques ou la pédophilie. La cybersurveillance contribue à la surveillance de masse.

Selon l'objectif poursuivi, la complexité de la cybersurveillance diffère. La surveillance de masse fait généralement partie des exemples plus évolués. Ainsi, plus la quantité d'informations à collecter et à traiter est abondante et plus les variables à analyser sont stratégiques, plus le système devra être sophistiqué.

La cybersurveillance peut être utilisée à différentes fins : prévention, détection des risques de crimes ou de délits divers, enquête à la suite d'un événement. « La cybersurveillance peut être utile, tant pour des raisons de sécurité et de bonne gestion d'un système informatique que pour des raisons de vérification de la bonne transmission de correspondances » (Cahen, s.d.). En France, le vocable *cybersurveillance* est plus fréquemment associé à la surveillance de l'utilisation des technologies au travail à des fins privées.

Bien que les avancées technologiques permettent des types de surveillance jadis insoupçonnés, la cybersurveillance soulève des interrogations et des craintes. De plus en plus omniprésente et invisible, et souvent réalisée à distance à l'insu des individus, la cybersurveillance suscite la crainte d'un contrôle social serré par les autorités qui en viendraient à réprimer toute forme de liberté individuelle. Au chapitre des inquiétudes se trouve le risque de glissement de finalités pour lesquelles les informations ont été recueillies au départ, ce qui pourrait porter atteinte à la vie privée des personnes et à leur intégrité (Boudreau, 2010). À ce sujet, les risques de profilage et de discrimination raciale nourrissent de vives appréhensions (Biseul, 2004). Apparaissent également des questions relatives à l'équilibre entre la quête de sécurité et les droits des individus. Jusqu'où sera-t-il permis de recueillir des renseignements et de les recouper avec d'autres informations personnelles sous l'impératif de la sécurité d'un État sans porter atteinte à la vie privée? La technologie permet désormais la surveillance de masse, de telle sorte que ce ne sont pas uniquement les suspects qui sont dans la mire des surveillants; toutes les personnes qui se trouvent dans un processus de surveillance deviennent suspectes (Commission nationale de l'informatique et des libertés, 2004; Commission de l'éthique de la science et de la technologie, 2008). La surveillance des passagers aériens en est un exemple. Dans le contexte de la mondialisation, une attention particulière devra être portée aux aspects juridique et éthique du partage et de l'utilisation des renseignements recueillis sous un système législatif donné.

Bibliographie

Bajc, V. (2007). « Debating Surveillance in the Age of Security », *American Behavioral Scientist*, vol. 50, n° 12, p. 1567-1591.

Biseul, X. (2004). *Cybersurveillance : les nouvelles technologies ravivent les vieilles peurs*, www.01net.com/article/248848.html (page consultée en avril 2010).

Boudreau, C. (2010). *Cybercriminalité et cybersurveillance*, Notes de cours, ENAP.

Boudreau, C. (2006). « Multipolarité de la surveillance et gestion des médicaments au Québec », *Recherches sociographiques*, vol. 47, nº 2, p. 299-320.

Cahen, M. (s. d.). *Le rôle de l'administrateur réseau dans la cybersurveillance*, www.netalya.com/fr/Article2.asp?CLE=162# (page consultée en avril 2010).

Commission de l'éthique de la science et de la technologie (2008). *Viser un juste équilibre : un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*, Avis adopté à la 34e réunion de la Commission de l'éthique de la science et de la technologie le 12 février.

Commission nationale de l'informatique et des libertés (2004). *La cybersurveillance sur les lieux de travail*, www.ladocumentationfrancaise.fr/rapports-publics/044000175/index.shtml (page consultée en avril 2010).

Häyhtiö, T. et J. Rinne (2009). « Little Brothers and Sisters Are Watching », *Information, Communication and Society*, vol. 12, n° 6, p. 840-859.

Leman-Langlois, S. et M. Ouimet (2006). « Introduction », *Criminologie*, vol. 39, nº 1, p. 3-6.

Pour citer Tremblay, M. (2012). « Cybersurveillance », dans L. Côté et J.-F. Savard (dir.), *Le Dictionnaire encyclopédique de l'administration publique*, [en ligne], www.dictionnaire.enap.ca

Information Pour information veuillez consulter www.dictionnaire.enap.ca

Dépôt légal Bibliothèque et Archives Canada, 2012 | ISBN 978-2-923008-70-7 (En ligne)