TECHNOLOGIE, CRIME, CRIMINALITÉ ET CRIMINOLOGIE

Stéphane Leman-Langlois

1) *LA TECHNOLOGIE COMME OUTIL CRIMINEL*

L'ère de l'information apporte avec elle un nombre de changements profonds dans la structure des sociétés modernes. Entre autres, 1) la production de richesse est de plus en plus centrée sur l'information comme bien commercialisable ; 2) la vie du citoyen est dépendante de la production, de la consommation de cette information ; 3) l'existence individuelle est liée à cette information de plusieurs façons, telles que la communication, le travail, les relations sociales, le divertissement, etc., au point qu'on parle aujourd'hui de « netoyenneté » (*netizenship*) en référence à l'existence virtuelle parallèle de beaucoup de gens actifs sur Internet.

Dans ce contexte, les prédations, exploitations, dommages divers qui peuvent survenir via les technologies de l'information prennent une signification particulière. Ce ne sont pas de simples manifestations alternatives de conduites dommageables conventionnelles — officiellement criminalisées ou non. On a, jusqu'ici, peu étudié ces aspects fondamentaux, se contentant plutôt de passer en revue les nouveautés technocriminelles une à une, en faisant des parallèles, ou en les amalgamant tout simplement avec des conduites déjà criminalisées qui semblent équivalentes.

Fonctionnellement parlant, on peut faire un certain nombre de catégories utiles des conduites dommageables, potentiellement criminelles ou déjà criminalisées qui sont réalisées à l'aide de technologies de l'information (TI).

Premièrement, il s'agit de conduites criminalisées dont les principaux aspects ne sont pas reliés à la technologie — ici, la technologie a un apport minimal. Par exemple, la GRC a arrêté plusieurs individus qualifiés de « cybertrafiquants » de marijuana le 28 février 2006. En fait, les trafiquants vendaient des graines de plants de marijuana via un site Internet. Autre exemple, les « cyberterroristes » qui n'ont de « cyber » que leur mode de communication ; à l'époque où les terroristes se contentaient du téléphone personne ne les appelait « téléterroristes ». Cela dit, ce genre de transformation, bien que mineure, peut en entraîner de plus significatives. Par exemple, la structure organisationnelle de groupes criminalisés peut être transformée par l'utilisation de certaines formes de communication.

Deuxièmement, il existe des actes criminels dont la commission est facilitée par la technologie à un point tel qu'ils sont transformés dans leur nature même. La pornographie juvénile est un exemple frappant. Bien que n'ayant pas attendu les TI pour exister, cette pornographie est massivement transformée par l'amélioration spectaculaire des technologies de production (photo et vidéo numériques, surtout), de stockage (disques durs de grande capacité à bon marché, DVD inscriptibles, etc.) et de diffusion. Un autre exemple est celui de l'échange de fichiers musicaux en ligne. Qualifié de « vol » ou de « piraterie » par l'industrie de la musique, l'échange de chansons numérisées est tellement plus facile que la bonne vieille copie sur cassette qu'un effort sans précédent de pression sur les gouvernements occidentaux pour le criminaliser est déployé depuis les cinq dernières années. Enfin, le vol d'identité, crime déjà relativement répandu dans l'ère pré-Internet, est désormais décuplé à un point tel que des millions de renseignements personnels peuvent être dérobés à la fois.

Il faut éviter de limiter notre compréhension de la technologie aux technologies de l'information et aux ordinateurs. Les technologies hydroponique et aéroponique, par exemple, ont également un impact non négligeable sur les possibilités de culture clandestine de plantes interdites.

Troisièmement, il est des conduites qui sont non seulement impossibles, mais impossibles à imaginer dans un monde non « branché ». C'est le cas de l'utilisation malveillante d'images produites par des téléphones portables, des caméras cachées ou des caméras de surveillance, à des fins de chantage, d'attaque personnelle ou tout simplement d'amusement public. Les guerres informatiques se manifestant dans la destruction d'espaces virtuels où des communautés de nettoyens évoluent ou dans la paralysie de sites commerciaux entravant la bonne marche d'entreprises sont également nouvelles.

Cela dit, il faut également noter que la nouveauté du contexte technocriminel est telle que l'horizon est entièrement ouvert à toutes les sortes de créations d'objets. Le cyberespace, surtout, est un lieu de conflits entre des intérêts dissemblables et le « crime » est souvent considéré comme un moyen de gouvernance particulièrement efficace (même si, en pratique, patrouiller l'Internet est loin d'être facile).

2) *LA TECHNOLOGIE COMME OUTIL DE CONTRÔLE SOCIAL*

Il est faux, contrairement à l'affirmation souvent entendue, que les moyens de contrôle sont « en retard » sur les moyens de commettre des crimes — à moins de comprendre le contrôle seulement à travers la lunette ultra-étroite des appareils policiers conventionnels. Au Canada, la plupart des escouades anti-« cybercrime » sont des ajouts considérés peu importants en eux-mêmes, créés pour apporter un support et une expertise technique aux enquêtes conventionnelles (lorsqu'on a besoin de fouiller le contenu d'un disque dur saisi, par exemple).

Cependant, la catégorie « contrôle social » doit être pensée de façon beaucoup plus large. Si on considère les efforts de surveillance de l'ensemble des organismes privés et publics, en ajoutant la surveillance que chaque individu peut faire de tous les autres, l'utilisation de technologies variées à des fins de surveillance et de contrôle (au sens large) est multipliée de façon spectaculaire.

Voyons quelques catégories de surveillance où la technologie a un effet important.

- *Contrôle d'accès* : il s'agit de dispositifs permettant l'accès sélectif à des lieux physiques ou virtuels. Ici, il faudrait inclure la bonne vieille serrure, qui est une technologie de contrôle d'accès ayant fait ses preuves. Aujourd'hui, cette serrure est secondée de dispositifs permettant une flexibilité décuplée. Les premiers sont biométriques (lecture de l'iris, de la rétine, des empreintes digitales, des proportions de la main, de la forme du visage, de la démarche, etc.) et permettent l'accès différentiel selon les jours et les heures de la journée à différentes personnes ; ils permettent également de savoir, avec une précision variable selon les systèmes, *qui* se trouve *où*, *à quel moment*. Des banques de données contenant les demandes d'accès et les déplacements de chaque personne peuvent être conservées indéfiniment. Les mots de passe, qui servent à donner accès à certains lieux virtuels et à certains services, permettent de garder la trace des activités des usagers dans le cyberespace.
- *Vérification de l'identité* : les technologies décrites ci-haut peuvent servir au simple contrôle d'identité, sans qu'un accès soit demandé. Par exemple, avec la reconnaissance du visage on peut identifier automatiquement des citoyens se déplaçant sur la voie publique. Les employés d'une entreprise peuvent être reconnus et retracés dans leurs déplacements durant leur quart de travail.
- *Commerce* : les entreprises commerciales ont un intérêt économique dans le contrôle de leur clientèle. Plusieurs moyens de « fidéliser » le consommateur, de modifier son comportement en lui promettant des bénéfices ou en contrôlant les informations contenues dans l'espace virtuel où il évolue, ont connu des développements importants avec l'utilisation de technologies avancées. La « personnalisation » du cyberespace permet de filtrer le contenu offert au visiteur selon les informations qu'on détient à son sujet au plan de ses préférences, ses habitudes de consommation et les lieux qu'il a visité auparavant.
- *Surveillance du comportement* : plusieurs technologies sont dédiées à la surveillance du comportement et à l'identification des personnes. Les caméras sont un palier dans ce système de surveillance, auquel s'ajoute des logiciels d'analyse de l'image variés. Ces logiciels peuvent analyser le mouvement des objets et des personnes et différencier les comportements « acceptables » (se diriger vers son véhicule et y monter) des comportements « louches » (se promener d'un véhicule à l'autre). Mentionnons également que d'autres dispositifs permettent de voir bien mieux que les caméras ordinaires. Plusieurs nouveaux produits sont équipés de senseurs infra-rouge et d'amplificateurs de lumière, mais d'autres, s'éloignant encore plus du spectre visible, peuvent aussi détecter des personnes ou marchandises à travers les murs de véhicules, de conteneurs ou d'édifices. À ceci on peut ajouter les dispositifs qui reniflent les émanations chimiques ou biologiques et ceux qui détectent les radiations, incluant la chaleur du corps (avec lesquels on a récemment tenté dans les aéroports canadiens de détecter les passagers porteurs de SRAS — maladie causant une fièvre).

  D'autres technologies ne sont pas principalement utilisées pour la surveillance, mais peuvent y servir. Par exemple, on peut retracer les déplacements de la plupart des usagers de téléphones portables. On peut utiliser les tours de communication téléphoniques pour suivre, tel qu'au radar, les déplacements de véhicules (bateaux, avions, camions, voitures). Enfin, certaines technologies,

en particulier l'« exploration de données » (*datamining*), permettent d'exploiter des informations existantes (potentiellement, *toutes* les transactions gérées par ordinateur) pour analyser le comportement de millions de personnes à la fois.

3) *LA TECHNOLOGIE COMME OUTIL SCIENTIFIQUE*

Les criminologues peuvent utiliser les nouvelles technologies dans trois principaux types d'activités. Premièrement, la diffusion des savoirs est, comme pour toutes les disciplines scientifiques, de grande importance. La collaboration entre chercheurs qui ne se rencontrent jamais est désormais possible, à travers des outils variés de traitement de texte, par courriel bien sûr et par conversations directes à travers des services comme Skype, MSN Messenger, Yahoo Messenger, etc. Ensuite, les travaux achevés ou à différentes étapes de développement peuvent être diffusés publiquement ou à un lectorat plus ou moins restreint sur Internet. La peur du « vol » et du « plagiat » subsiste toujours évidemment, mais risque de disparaître éventuellement sous la pression de la cyberculture. L'ensemble des disciplines bénéficieront énormément de cette disparition, peut-être autant qu'elle bénéficièrent de l'avènement de la presse à caractères mobiles. Plusieurs recherches ont déjà démontré à quel point la notion périmée (et incompatible avec le cyberespace) de propriété intellectuelle freine le développement des connaissances humaines.

Deuxièmement, les TI sont des moyens pédagogiques puissants. Bien qu'en retard extrême à ce chapitre, les institutions d'enseignement peuvent mettre à grand profit les nouvelles TI, à condition d'en comprendre les conséquences (entre autres, celles qui sont identifiées ci-dessus). Contrairement à la bulle audio-visuelle des années '70, la bulle TI ne s'évaporera pas sous le soleil de la réalité. Les institutions qui ne prennent pas le virage seront dépassées par les autres. Pour l'instant, la lenteur administrative et le point de vue suranné qui dédaigne tout ce qui se trouve sur Internet sans support traditionnel (publications sans équivalent papier, cours sans équivalent en classe, etc.) ont retenu ces développements un peu partout dans le monde. Ceci risque peu de rester le cas encore longtemps.

Enfin, les institutions doivent mousser leur présence, leur formation, leur production scientifique et leur placement étudiant sur Internet puisque de plus en plus de leurs clients magasinent à l'aide de leur fureteur. Les institutions qui font meilleure figure sur leur site sauront attirer d'avantage d'étudiants, de chercheurs collaborateurs et de bailleurs de fonds. Le site du CICC, qui reste encore un modèle de ce qu'il ne faut pas faire, est sur le point d'être rénové en profondeur pour se débarrasser de son aspect d'amateurisme primaire et de vide intellectuel.