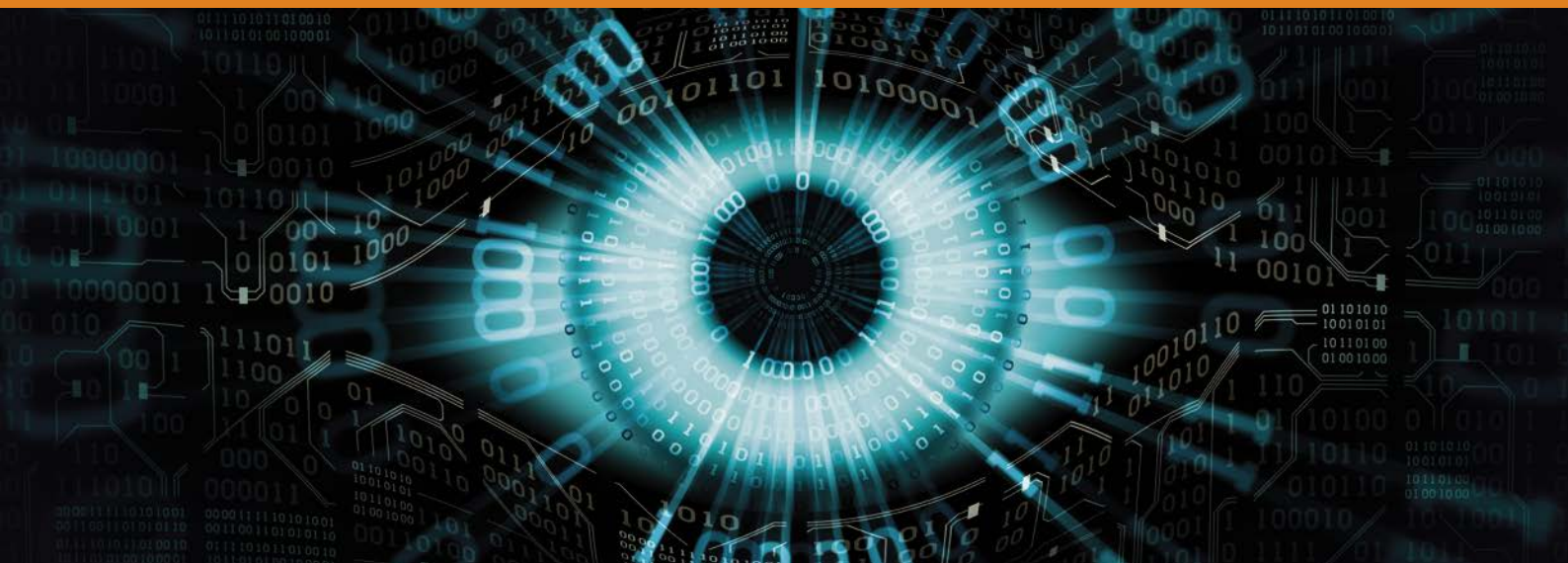
PSC INFO

2 | 2021

LE MAGAZINE DE LA PRÉVENTION SUISSE DE LA CRIMINALITÉ

Dossier
Surveillance



Chère lectrice, cher lecteur,


PSC

Pour beaucoup d'entre nous, le mot «surveillance» évoque probablement tout d'abord «Big Brother», l'ennemi de la sphère privée, ou l'instrument potentiel qu'utilisent les puissants pour régner sans partage. Ou encore l'émission de téléréalité du même nom dont les participants abandonnent volontairement leur sphère privée pour amuser le spectateur. Ces deux aspects importants sont traités dans le présent numéro de PSC INFO : Erik Schönenberger (directeur de *Société numérique)* met en garde dans l'interview qu'il nous a accordée contre l'utilisation des techniques de surveillance par les pouvoirs publics, dès lors que les bases légales la légitimant dans un Etat de droit font défaut ; et l'écrivain engagé en politique Jürg Halter parle dans une autre interview de l'étrange décalage qui existe dans le comportement d'une foule d'individus qui, d'une part, livrent sans cesse et volontairement leurs données personnelles, par ex. dans les médias sociaux, et qui, d'autre part, lors de la crise du COVID-19, refusent de coopérer et de faciliter le traçage parce qu'ils craignent que leurs données ne soient utilisées à mauvais escient. Quant à la question de savoir qui peut filmer qui, l'avocat Martin Steiger montre pourquoi il serait utile de renforcer et d'affiner le dispositif légal – à une époque où on a le sentiment que chacun filme constamment l'autre.

La surveillance sous forme d'opérations de cyberpatrouille est une pratique de plus en plus courante pour lutter contre la criminalité, comme le montre l'article de l'analyste NEDIK Tamara Schmid. Comment la surveillance électronique (ou sa forme commune, le bracelet électronique) sera mise un jour en place contre la violence domestique et le stalking, c'est ce qu'expliquent Alain Hofer (secrétaire général suppléant CCDJP) et Janine Repetti-Dittes (association Electronic Monitoring). Dans cette édition aussi, on découvrira l'éclairage de Nadja Capus (professeure à l'Université de Neuchâtel) sur les difficultés techniques et juridiques auxquelles sont confrontés les médiateurs linguistiques lors de la surveillance en temps réel des communications entre des criminels ; la professeure explore avec son équipe ce sujet peu étudié et pourtant primordial dans le but d'établir des normes pour la pratique. Enfin, nous jetons un regard juridique sur ce qu'il en est des drones et du regard qu'ils ont le droit ou pas de jeter au-dessous d'eux ; découvrez ce qu'en disent les auteures, Sandra Bodmer et Amanda Boekholt.

Il est évident que la surveillance a tant de visages que nous avons dû opérer un choix dans ce numéro de PSC INFO. Et puis, rappelons en conclusion que la surveillance permet d'empêcher que ne surviennent des infractions, ou encore des accidents de la route et des catastrophes écologiques ; elle est primordiale dans l'espace aérien et surtout en médecine, car elle permet de sauver des vies tous les jours. Cela dit, et c'est essentiel, elle doit reposer sur un fondement juridique solide, être validée démocratiquement et il faut pouvoir s'assurer que l'usage des données collectées soit effectivement contrôlé.

Je vous souhaite une agréable lecture !

Fabian Ilg
Directeur de la Prévention Suisse de la Criminalité

IMPRESSUM

Editeur et commande
Prévention Suisse de la Criminalité
Maison des cantons
Speichergasse 6
3001 Berne

Courriel : info@skppsc.ch
tél. 031 511 00 09

PSC Info 2 | 2021 est téléchargeable en format PDF, à l'adresse : www.skppsc.ch/skpinfo.
PSC Info 2 | 2021 paraît aussi en allemand et en italien.

Responsable		Chantal Billaud, directrice suppléante PSC
Rédaction, interviews		Volker Wienecke, Berne
Traduction	**fr**	ADC, Vevey
	it	Annie Schirrmeister, Massagno
Mise en pages		Weber & Partner, Berne
Impression		Länggass Druck SA, Berne
Tirage		fr: 300 ex. | all: 1350 ex. | it: 250 ex.
Date de parution		Numéro 2 | 2021, juillet 2021

« La Suisse est-elle un Etat fouineur, Monsieur Schönenberger ? »

Dans cet entretien, le spécialiste informatique Eric Schönenberger parle de l'utilisation de différents dispositifs de surveillance tels que la conservation des données, l'exploration du réseau câblé ou encore la reconnaissance faciale. Il interroge aussi la légalité de ces pratiques. Monsieur Schönenberger est le directeur de *Société numérique*, dont il est aussi l'un des fondateurs.

La Suisse est-elle un Etat fouineur, Monsieur Schönenberger ?
Oui, on peut l'affirmer. Car la mise en place de dispositifs de surveillance de masse y progresse, avec la conservation des données et l'exploration du réseau câblé.

Comment fonctionne la conservation des données ?
Les données conservées permettent de retracer qui a appelé qui, quand et combien de temps a duré l'appel, qui s'est connecté à Internet, quand et pendant combien de temps, qui a envoyé un courriel ou un SMS à qui et quand. Si c'est un téléphone mobile qui est utilisé, les données de géolocalisation de l'appareil sont également stockées. Toutes ces informations doivent être conservées pendant six mois et communiquées sur demande aux autorités de poursuite pénale ou aux services renseignement.

Les fournisseurs sont donc tenus de conserver pendant six mois le protocole du comportement de leurs clients en matière de communication. À l'origine, l'enregistrement des communications était conçu afin de dépister des réseaux de contacts. Aujourd'hui, chaque communication au moyen d'un smartphone donne lieu à la collecte d'un ensemble de données, même lorsqu'une application vérifie en arrière-plan si un nouveau message est arrivé.


DR

Erik Schönenberger, spécialiste informatique et directeur de Société numérique.

Accéder aux données est admis en cas de simple présomption de crime ou de délit. De plus, les données enregistrées sont utilisées pour ce que l'on appelle la recherche par champ d'antennes, c'est-à-dire l'investigation par recoupement pour des présomptions contre inconnu. L'objectif est de déterminer qui se trouvait à tel endroit à un moment donné, et qui pourrait avoir commis un acte punissable. Cela peut obliger des personnes à devoir prouver leur innocence, dès lors que leur téléphone portable était connecté à l'instant «T» à l'une des cellules radio faisant l'objet d'une surveillance dans le cadre de l'enquête. Il existe un cas connu dans lequel l'opérateur de téléphonie mobile a fourni plus de 150 000 données de connexion.

Le fait est que la recherche par champ d'antennes n'est pas suffisamment encadrée juridiquement. La surveillance d'une personne peut être ordonnée uniquement s'il y a présomption de délit à son encontre. L'argument invoqué pour conserver les données est que les autorités chargées de l'enquête doivent pouvoir lutter «à armes égales» avec les délinquants dans le cas d'infractions commises sur Internet. Or, cette surveillance-là ne concerne précisément pas Internet. On crée donc des outils d'investigation supplémentaires faisant de nos smartphones des mouchards.

Et comment fonctionne la conservation des données sur Internet ?
La conservation des données sur Internet implique aussi une obligation d'identification. En outre, les adresses IP doivent être conservées pendant six mois. Elles sont nécessaires pour la communication sur Internet et sont attribuées à une connexion, par exemple à un modem ADSL ou un câble TV. Les adresses IP n'étant pas disponibles en nombre suffisant, elles sont généralement partagées avec les réseaux WIFI publics et les réseaux de téléphonie mobile. Cette technologie est appelée *Network Address Translation* (NAT). Les opérateurs doivent conserver ces tableaux de traduction pendant six mois. Avec pour conséquence que le volume de données explose lui aussi, avec un ordre de grandeur d'un milliard d'opérations de traduction NAT par réseau mobile et par jour !

123RF/Kheng Ho Toh

« La conservation des données concerne chacun de nous sans exception. »

Ce qui, à l'origine, était conçu pour permettre l'identification sert désormais à la surveillance de notre utilisation d'Internet, puisque le Service de surveillance de la correspondance par poste et télécommunication (SSCPT) exige que soient stockés aussi bien le processus de traduction lui-même que les adresses de destination. Avec ces données, il est possible de pister tous les serveurs consultés et les services Internet utilisés par une personne, ou de repérer tous les utilisateurs d'un service ou d'un serveur.

Mais ces données ne sont-elles pas utiles pour résoudre les affaires criminelles ?

Malheureusement, il existe peu d'études sur la nécessité de conserver les données pour lutter contre la criminalité. Dans une expertise commandée par le Ministère allemand de la justice, l'Institut Max Planck conclut que la conservation des données pratiquée en Suisse ne s'est pas traduite par une hausse systématique du taux d'élucidation des crimes et délits. Or il est illégitime de restreindre les droits fondamentaux dès lors que l'utilité d'une action n'est pas ou ne peut pas être prouvée !

Comme nous pouvons le constater, la conservation des données concerne chacun de nous sans exception. Elle constitue une atteinte grave et disproportionnée à la protection de la vie privée garantie par la Constitution et une violation du secret professionnel des avocats, des médecins ou des rédacteurs. Jusqu'à présent, tous les tribunaux constitutionnels européens et la Cour de justice européenne qui ont eu à juger des lois sur la conservation des données les ont annulées sans exception.

Pour ce qui est de la Suisse, *Société numérique* a saisi la Cour européenne des droits de l'homme de Strasbourg. Le traitement de la plainte intentée stratégiquement contre la conservation des données est en cours – avec de bonnes chances de succès.

Quittons, si vous le voulez bien, le terrain de la poursuite pénale. Qu'en est-il de la surveillance pratiquée par les services de renseignements ?

La mise en œuvre de la nouvelle loi sur le renseignement et l'introduction de l'exploration du réseau câblé a ouvert la porte à une nouvelle surveillance de masse. Ce dispositif dérivé de l'exploration radio était à l'origine une surveillance purement militaire des opérations menées à l'étranger. De la radio on est passé subrepticement à la surveillance par satellite, toujours pour les communications à l'étranger ; elle englobe néanmoins déjà la communication civile.

Puisqu'aujourd'hui la transmission des communications passe de plus en plus par la fibre optique, l'exploration du réseau câblé franchit une troisième étape. Contrairement aux satellites, les câbles étrangers ne peuvent pas faire l'objet d'une surveillance. Il faut donc exploiter les lignes transfrontalières du réseau de fibre optique. Or chaque communication transfrontalière implique une personne dans notre pays, car il n'existe pour ainsi dire pas de lignes qui ne font que traverser la Suisse.

En pratique, cela ressemble à ceci : les communications qui empruntent des lignes transfrontalières sont filtrées par le Centre des opérations électroniques de l'armée (COE) à l'aide de mots-clés prédéfinis. La loi permet l'utilisation des signaux captés si l'expéditeur et/ou le destinataire sont basés à l'étranger. Il s'agit des adresses IP.

123RF/pixinoo

« La reconnaissance faciale est de plus en plus utilisée dans les aéroports et les gares. »

Dans le cas de lignes transfrontalières, il arrivera pratiquement toujours qu'une adresse IP soit située en Suisse et une autre à l'étranger. En d'autres termes, nous sommes tous surveillés en permanence, et nos communications sont passées au crible. Cette surveillance, qui est en fait ciblée sur les opérations à l'étranger, sert aussi tout naturellement pour repérer des menaces à l'intérieur du pays.

Qu'en est-il de la surveillance ciblée, comme celle que permettent les chevaux de Troie d'État ?

L'utilisation de chevaux de Troie d'État *(govware)* est autorisée pour les autorités de poursuite pénale et les services de renseignement. Si les premières peuvent accéder aux données de communication, les services de renseignement, eux, ont le droit d'effectuer une recherche en ligne et de recourir à une caméra et à un microphone. Cela constitue une intrusion – tout au moins potentielle – dans la sphère intime numérique des personnes concernées, car nous stockons une quantité faramineuse d'informations très personnelles sur nos smartphones, nos ordinateurs portables et nos PC. Ces informations donnent des indications sur notre santé, nos opinions politiques ou encore nos préférences sexuelles. Mais nos appareils stockent aussi bien souvent des secrets professionnels ou de la correspondance avec notre avocat. C'est comme si quelqu'un s'introduisait secrètement dans votre logement pour y placer des micros.

Une telle façon de faire ne doit être autorisée qu'en dernier recours, en cas de menace concrète et immédiate de mise en danger de la vie, de l'intégrité corporelle, de la liberté ou de la sécurité nationale. Or, rien que la liste restreinte des infractions en recense déjà une centaine, dont le vol simple !

Quel est, selon vous, le principal problème lié à l'utilisation de govware ?

Outre la grave intrusion dans la sphère intime numérique se pose le problème de l'infection des systèmes qui, pratiquement toujours, survient à la faveur d'une faille de sécurité. Ces failles peuvent s'obtenir, directement ou indirectement, sur le marché noir, lequel se retrouve ainsi soutenu par l'argent public. De plus, circonstance aggravante, la faille de sécurité n'est pas comblée ; nous restons donc tous vulnérables.

Un exemple ?

Le logiciel malveillant *WannaCry* s'est propagé en 2017 via une faille utilisée et gardée secrète par la NSA pendant plusieurs années avant d'être exploitée par des criminels. Plusieurs centaines de milliers d'ordinateurs ont été touchés et mis hors service dans 150 pays. Parmi eux, des hôpitaux en Angleterre et en Écosse, mais aussi des sociétés comme Nissan, Renault et Deutsche

Société numérique

Société numérique est une association pour la protection des citoyens et des consommateurs à l'ère numérique à but non lucratif et à large assise. En tant qu'organisation de la société civile, elle s'engage depuis 2011 à assurer une société durable, démocratique et libre. Elle défend les droits fondamentaux dans un monde interconnecté.
www.societe-numerique.ch

Bahn. Il doit être dans l'intérêt de l'État de garantir sa sécurité et la nôtre en signalant aux fabricants les failles de sécurité afin qu'elles soient comblées. Il ne faut pas que ces failles soient gardées secrètes.

Quel bilan et quelles perspectives concernant la surveillance en Suisse ?
La surveillance se pense selon des critères de faisabilité. Rares sont les études sur son utilité. En outre, il n'existe pas de recensement global des profits et pertes de la surveillance qui tienne compte de l'ensemble des mesures sous l'angle de leur impact sur la démocratie et sur la société.

Circonstance aggravante, la Suisse n'a pas de tribunal constitutionnel compétent pour contrôler la proportionnalité des lois. Cela signifie que notre plainte de 2014 contre la conservation des données ne sera pas entendue à Strasbourg avant l'année prochaine au plus tôt. Notre deuxième plainte, devant le Tribunal fédéral, formée en 2017 contre l'exploration du réseau câblé, vient d'être renvoyée au Tribunal administratif fédéral pour examen matériel.

La voie judiciaire est de très longue haleine, tandis que la technologie et les dispositifs de surveillance évoluent de façon fulgurante. Nous le voyons, par exemple, avec la reconnaissance faciale. Elle est de plus en plus utilisée dans les aéroports et les gares. Il existe déjà d'énormes bases de données faciales, comme celle de *ClearView AI*. De fait, combiner les caméras de surveillance en réseau et l'apprentissage automatique pourrait conduire à une situation proprement dystopique où règne l'intrusion institutionnalisée.

Nous demandons donc – avec 60 autres organisations de défense des droits fondamentaux de toute l'Europe – l'interdiction de la surveillance biométrique de masse dans l'espace public !

Monsieur Schönenberger, un grand merci pour ces propos éclairants.

Surveillance par des drones et respect de la sphère privée

Depuis les débuts de la révolution numérique durant la seconde moitié du siècle dernier, les innovations technologiques se succèdent à un rythme effréné. L'invention du drone est un exemple qui illustre bien cette évolution. Ces engins aériens sans pilote, dont il existe un grand nombre de modèles, s'utilisent de multiples façons, par exemple dans l'agriculture, pour l'inspection d'infrastructures, mais aussi pour la surveillance de grandes manifestations par la police ou pour les loisirs. En regard des avantages indéniables qu'ils apportent, il faut aussi considérer leurs inconvénients.

L'« industrie 4.0 » qui a pour but une numérisation globale de la production industrielle amène en permanence de nouvelles technologies sur le marché. Elles se caractérisent par l'« hyperautomatisation » et l'« hyperconnectivité », c'est-à-dire une automatisation accrue des processus et de la connexion des objets avec leur environnement. Les drones en sont une parfaite illustration. Toutefois, leur essor s'accompagne d'une problématique qui préoccupe de plus en plus les citoyennes et citoyens : la protection de leur sphère privée. Un exemple frappant est celui de la France où la police a utilisé des drones pour contrôler le respect des mesures imposées en raison de l'épidémie de COVID-19. Le présent article met en lumière les aspects juridiques du conflit d'intérêts qui oppose respect de la sphère privée et utilisation des drones.

Origine des drones

Les drones, ainsi nommés à cause du bourdonnement qu'ils émettent, ont d'abord été développés à des fins militaires, les applications civiles venant plus tard. Bien que l'engin soit très répandu, le terme de « drone » n'a toujours pas de définition légale. Les drones font partie des engins aériens sans pilote, soit télécommandés soit volant de manière autonome. On les appelle aussi UAV/UAS ou RPAS : UAV est l'abréviation de *unmanned aircraft vehicle,* UAS celle de *unmanned aircraft*

Auteures


DR

Amanda Boekholt est spécialiste en communication et responsable du *stakeholder management* à la Section Innovation et numérisation de l'Office fédéral de l'aviation civile (OFAC).


DR

Sandra Bodmer est juriste et travaille à la Section Innovation et numérisation de l'Office fédéral de l'aviation civile (OFAC). Elle est responsable de la mise en œuvre par la Suisse de la réglementation européenne sur les drones.

Adobe Stock/Iulia Sokolovska

« Qui donc en est le pilote et que cherche-t-il en faisant voler son drone au-dessus du jardin ? »

system, RPAS celle de *remotely piloted aircraft system,* ce dernier terme étant réservé aux engins sans pilote télécommandés.

Sphère privée

Grâce aux progrès technologiques, la taille des drones a fortement diminué. En outre, on peut les acheter librement à un prix très abordable dans le commerce de détail. Ces atouts ainsi que la diversité des utilisations possibles sont à l'origine de l'essor fulgurant de l'industrie du drone. En 2018, environ 80 entreprises employant près de 2500 personnes étaient actives dans la fabrication de drones en Suisse. Cependant, comme c'est toujours le cas lors de l'émergence d'une nouvelle technologie, l'enthousiasme ne gagne pas tout le monde. L'utilisation de drones dans l'espace privé suscite des peurs et des incertitudes qui engendrent souvent une attitude de rejet de ces engins. L'Office fédéral de l'aviation civile (OFAC) doit régulièrement traiter les demandes de citoyennes et citoyens qui se sentent observés ou importunés par des drones dans leur environnement. Qui donc en est le pilote et que cherche-t-il en faisant voler son drone au-dessus du jardin ? Prend-il des photos ? Si oui, qu'en fait-il ? En a-t-il d'ailleurs seulement le droit ?

Intérêt digne de protection (art. 667 CC)

Si un drone survole une propriété privée, il faut tenir compte du fait que la propriété foncière ne se limite pas au sol, mais comprend aussi l'espace situé au-dessus, les intérêts des propriétaires devant être déterminés au cas par cas. Le Tribunal fédéral ne s'est pas encore prononcé sur la hauteur maximale du survol d'une propriété, mais on trouve dans la doctrine des auteurs estimant qu'il existe un intérêt digne de protection lorsqu'un drone survole une propriété à très faible altitude (10–40 mètres). Avant d'aborder la question des atteintes à la sphère privée causées par les drones, nous exposons ci-après les différents aspects de la sphère privée.

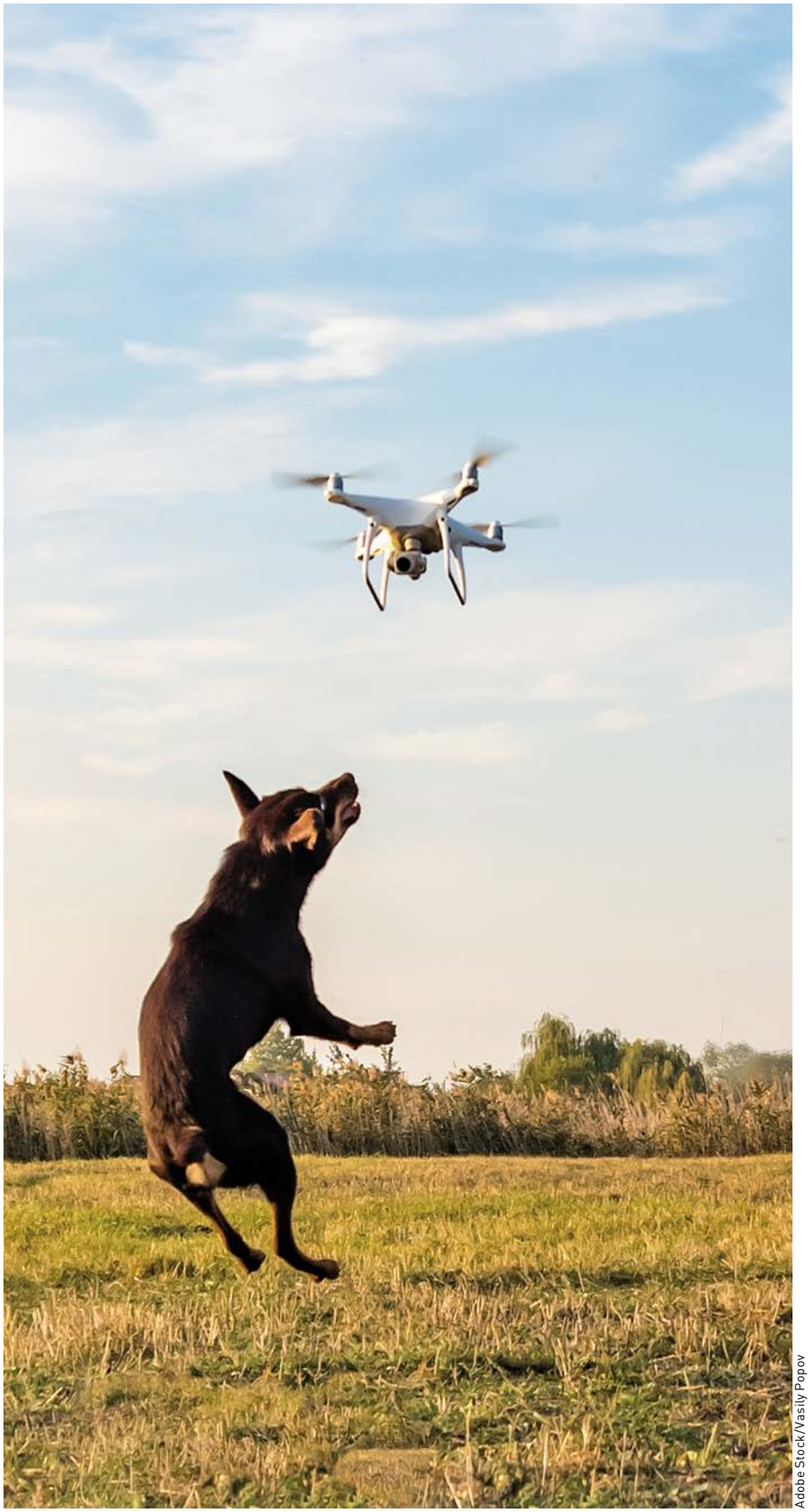
Protection de la personnalité

Plusieurs dispositions de la Constitution fédérale de la Confédération suisse (Cst.) sont consacrées à la protection

de la personnalité et à celle des données. Le droit à la liberté personnelle, notamment à l'intégrité physique et psychique ainsi qu'à la liberté de mouvement sont inscrits à l'art. 10, al. 2 Cst. En outre, à l'art. 13 figure le droit de toute personne à la protection de la sphère privée en général et à la protection contre l'emploi abusif des données qui la concernent en particulier.

Dans ses art. 28 ss, le Code civil suisse (CC) concrétise les art. 10 et 13 de la Constitution. L'art. 28 CC traite de la protection globale de la personnalité sans en énumérer les différents attributs. Pour qu'une atteinte à la personnalité au sens de l'art. 28 CC puisse être invoquée, le fait reproché doit revêtir une certaine gravité. Selon l'al. 2, une atteinte est illicite, à moins qu'elle ne soit justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi. Ainsi, prendre une photo sans le consentement de la personne concernée constitue déjà une atteinte à la personnalité au sens de l'art. 28 CC si aucun intérêt prépondérant ne peut être invoqué. Lorsque, sur les images d'une caméra de surveillance, le visage d'une personne peut être identifié par des tiers, il y a atteinte à la personnalité.

Dans sa décision du 18 avril 2018, le tribunal cantonal de Lucerne a procédé à une analyse approfondie de la question de la protection de la personnalité dans le cas d'images prises par des drones : les prises de vue aériennes des immeubles sur les berges du lac à Horw à des fins de surveillance de travaux ont été considérées comme illicites en raison de l'absence de base légale. Malgré l'annonce des travaux, les riverains ont eu, au bout d'un mois, le sentiment d'être surveillés ce qui, selon le Tribunal, a été considéré comme une limitation importante du droit à disposer librement des informations les concernant et constituait une atteinte au droit à la protection de la sphère privée au sens de l'art. 13 Cst. Les images captées par les drones devaient donc être effacées en raison de l'absence de base légale.



Adobe Stock/Vasily Popov

« Certains sont en outre d'avis qu'au vu de la tendance actuelle à publier des images sur les réseaux sociaux, une action rapide est clairement défendable et que tirer sur un drone ou l'attraper se justifierait selon les cas. »

Protection des données

Il faut enfin mentionner la loi sur la protection des données (LPD) qui vise à protéger la personnalité des personnes faisant l'objet d'un traitement de données. La LPD porte donc sur un des aspects essentiels de l'industrie 4.0. Elle s'applique lorsque des données personnelles sont traitées au sens de l'art. 3, let. a. Si toutefois des images prises par des drones sont destinées exclusivement à un usage personnel, les dispositions de protection des données ne s'appliquent pas comme le stipule l'art. 2, al. 2 de la LPD. La doctrine n'est cependant pas unanime. En effet, même lorsque des données sont destinées exclusivement à un usage personnel et que la LPD ne s'applique pas *de jure*, cela n'élimine pas la possibilité d'une atteinte à la sphère privée ni le sentiment d'être espionné. Un mémento relatif à la vidéosurveillance par des drones publié par le préposé fédéral à la protection des données (PFPDT) recense les différents points à respecter sous l'angle de la protection des données.[1] Le PFPDT considère que les prises de vue par des drones sont autorisées uniquement s'il y a un motif justificatif (le consentement de la personne concernée, un intérêt privé ou public prépondérant ou la loi).

DR

« Le service d'identification à distance permet d'identifier les exploitants de drones durant un vol grâce à leur numéro d'enregistrement (système similaire aux plaques d'immatriculation des véhicules). »

Actions contre les atteintes à la sphère privée

Les propriétaires et les détenteurs d'un bien disposent de plusieurs possibilités juridiques pour se défendre contre les nuisances subies :

Plainte pour violation du droit de propriété (art. 641, al. 2 CC)
En déposant une plainte pour violation du droit de propriété, le propriétaire d'un terrain peut se défendre contre l'auteur d'une atteinte injustifiée. Une telle atteinte est avérée si, lors du survol du drone, les limites horizontales ou la limite verticale – définie par l'intérêt digne de protection du propriétaire – ont été franchies contre la volonté de l'ayant droit.

Droit du voisinage (art. 679 s. CC)
La plainte relevant du droit du voisinage invoque les nuisances excessives causées par un voisin. Si le voisin possède un drone et qu'il se sert régulièrement de son terrain pour le faire décoller et atterrir, on peut considérer qu'il excède son droit de faire usage de sa propriété foncière.

Protection de la possession
(art. 926 et art. 928 CC)
Le possesseur d'une chose (par exemple le locataire d'une maison) dispose de certains recours similaires à ceux du propriétaire. En cas d'atteinte à sa possession, il peut faire usage de la force pour se défendre contre l'activité préjudiciable. Son action doit toutefois rester proportionnée à l'atteinte subie. Selon la doctrine actuelle, tirer sur le drone est un moyen à utiliser en dernier recours pour repousser par la force un acte d'usurpation (droit de se défendre selon l'art. 926 CC). Certains sont en outre d'avis qu'au vu de la tendance actuelle à publier des images sur les réseaux sociaux, une action rapide est clairement défendable et que tirer sur un drone ou l'attraper se justifierait selon les cas. Cela n'est toutefois valable que durant l'opération. Si le possesseur renonce à faire usage de son droit à la légitime défense, il peut faire valoir ses droits en déposant plainte.

Droit pénal (art. 179^{quarter} CP)
Le droit pénal offre également une protection contre les nuisances dues aux drones. On peut invoquer la violation du domaine secret ou du domaine privé au moyen d'un appareil de prise de vues lorsque celles-ci interviennent à un endroit qui est protégé des regards d'autrui d'une manière ou d'une autre.

En fin de compte, les procédures civiles tout comme les procédures pénales permettent rarement d'éviter à temps les dommages immédiats causés par des drones. Elles sont plus appropriées pour se défendre contre l'usage répété et planifié de drones et lorsque la personne à l'origine des nuisances est connue.

1 PFPDT, vidéosurveillance par des drones dans le domaine privé (www.edoeb.admin.ch → Protection des données → Technologies → Vidéosurveillance → Drones)

Mesures techniques

Il est très rare que l'identité du pilote soit connue dans les cas d'atteinte à la protection de la personnalité et des données, ce qui rend nettement plus difficile l'application du droit. En effet, il n'est pas aisé retrouver le ou la pilote pour lui enjoindre d'effacer l'enregistrement. Heureusement, les progrès de la technique et l'adaptation de la réglementation permettent de remédier à ce problème et facilitent les poursuites pénales.

D'une part, selon la nouvelle réglementation européenne sur les drones – dont la mise en œuvre en Suisse a été ajournée –, l'exploitant d'un drone doit figurer dans un registre national si son engin pèse plus de 250 grammes ou s'il est équipé d'un capteur capable de recueillir des données à caractère personnel. D'autre part, dans le cadre de la réglementation « U-Space », il est prévu d'introduire un service d'identification à distance *(network remote identification,* abrégé « Net-RID »). Ce service permet d'identifier les exploitants de drones durant un vol grâce à leur numéro d'enregistrement (système similaire aux plaques d'immatriculation des véhicules). La Suisse est en passe d'introduire l'identification à distance et procède à une phase de test sur une base volontaire dans le cadre du partenariat « Swiss U-Space Implementation » (SUSI).

Conclusion

Les différents recours juridiques que nous avons décrits et, surtout, les nouvelles prescriptions techniques devraient, espérons-le, produire deux effets : d'une part, générer une prise de conscience accrue des pilotes de drones pour les règles qu'ils doivent respecter et, d'autre part, prévenir les atteintes à la sphère privée de chacun ou du moins permettre qu'elles ne restent pas impunies. En outre, l'acceptation de ces nouveaux engins volants par la population devrait aller en s'améliorant. En fin de compte, l'objectif à atteindre est d'éviter que la problématique de la protection des données ou la peur d'une atteinte à la sphère privée compliquent voire empêchent la mise au point ou l'essor de technologies très prometteuses pour l'ensemble de la société.

Les cyberpatrouilles sont à l'affût

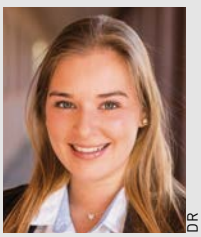
Pour lutter contre la criminalité numérique, la Suisse s'est dotée d'un réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique, le NEDIK. Les corps de police, qui en sont les parties prenantes, s'organisent en cyberpatrouilles chargées d'observer, de collecter et de mener des enquêtes préliminaires sur les agissements criminels commis sur Internet et sur le *darknet,* en application de la loi sur la police.

Un constat s'impose avec l'avancée du numérique : les activités en ligne n'ont pratiquement plus de limites. Internet satisfait tous les souhaits, même les moins avouables. Armes, contrefaçons d'articles de marque, changement d'identité, stupéfiants ou encore photos et vidéos prohibées : l'acheteur rentre rarement bredouille, pour peu qu'il sache comment s'y prendre. Confrontées à ce défi, les forces de police suisses se doivent de le relever. Il faut distinguer les délits qui leur sont signalés de ceux qu'elles doivent activement rechercher. On sait que les citoyens dénoncent en général uniquement les actes délictueux dont ils ont été eux-mêmes victimes. Il en va tout autrement avec les stupéfiants par exemple. Dans ce domaine, le *cyber patrolling* consiste pour la police, et plus généralement pour les autorités de poursuite pénale, à repérer et à cibler les actes punissables commis sur Internet. Cette méthode, calquée sur celle pratiquée sur le terrain, n'est pas nouvelle, elle est simplement transposée dans le cyberespace. L'objectif est que les cybercriminels sentent qu'ils ne peuvent pas agir en toute impunité. Internet ne doit pas être une zone de non-droit.

En ce moment, les forces de l'ordre suisses renforcent leurs divisions Cybercriminalité et forment leur personnel afin de se donner les moyens de lutter contre ce phénomène. Les équipes comprennent des spécialistes expérimentés : détectives, enquêteurs, informaticiens mais aussi collaborateurs scientifiques sans formation policière qui, ensemble, traquent les dealers, les escrocs, ou encore les pédocriminels

Auteure

Tamara Schmid
Analyste NEDIK
Police cantonale zurichoise



DR

123RF | Montage: Weber & Partner

« Le cyber patrolling *consiste pour la police, et plus généralement pour les autorités de poursuite pénale, à repérer et à cibler les actes punissables commis sur Internet. »*

qui sévissent sur Internet. La démarche anticipatrice adoptée par les cyberpatrouilles est capitale, car elle permet de repérer puis de prévenir les actes illégaux ou la préparation de ceux-ci. Les enquêteurs des corps de police suisses reçoivent aussi régulièrement des indices tangibles sur des actes illégaux commis sur Internet, auxquels ils donnent systématiquement suite.

Cas de figure

Au début d'une investigation sur un trafic de drogue présumé, les équipes de police observent les plaques tournantes en ligne pour voir si des délits sont en lien avec la Suisse. Elles ne ciblent pas un individu en particulier, mais effectuent des patrouilles pour cerner des phénomènes.

1. Les équipes de spécialistes passent au crible les plaques tournantes virtuelles connues et les profils des fournisseurs puis analysent les transactions.
2. Se fondant sur des critères précis, elles sélectionnent certains fournisseurs, puis examinent les procédures envisageables.
3. De cette analyse se dégagent des premiers indices sur l'identité potentielle des trafiquants.
4. Si les éléments de suspicion sont solides, une instruction est ouverte.

Les deux premières étapes illustrent bien la nature du travail préliminaire des cyberpatrouilles. A la troisième commence l'enquête préalable. Une fois ces trois étapes franchies, l'instruction (quatrième étape) a des chances d'aboutir.

Coordination

L'une des missions essentielles du NEDIK est de coordonner la collaboration en matière de lutte contre la criminalité informatique à l'échelon national et international. Des indices sont régulièrement fournis par la population et par des forces de police étrangères telles qu'Interpol ou Europol. Les signalements en provenance de l'étranger sont tout d'abord communiqués à fedpol, l'Office fédéral de la police, qui les transmet aux polices cantonales. Sans coopération très poussée entre les cantons, entre ceux-ci et la Confédération ainsi qu'entre cette dernière et l'étranger, les enquêtes n'ont pratiquement aucune chance de succès. Afin de lutter efficacement contre la criminalité numérique, le NEDIK a recours à des instruments d'analyse spécifiques et gère une base de connaissances centralisée, deux éléments qui permettent de partager de manière optimale les résultats des enquêtes avec les autres corps de police.

La coordination est cruciale. Comme dans d'autres pays, le risque existe aussi en Suisse que des enquêtes ou des opérations de cyberpatrouille soient menées en parallèle sans concertation. Les coordonner permet d'éviter cela et d'engager des ressources plus utilement ailleurs.

Lutte contre la pédocriminalité

Depuis le 1er janvier 2021, la police cantonale bernoise est responsable, au sein du NEDIK, de la coordination de la surveillance entre pairs ainsi que des mesures préventives secrètes nécessaires dans certains cas. La criminalité informatique en général, et la pédocriminalité en particulier, ne connaissent pas de frontières. Il est donc essentiel que les cantons, la Confédération, mais aussi les autres États, coopèrent étroitement. Fedpol traite et trie pour les cantons les agissements suspects communiqués par ses partenaires à l'étranger, par exemple ceux appelés NCMEC*, qui émanent des autorités américaines. Dès qu'un soupçon se confirme, le ministère public compétent à l'échelon des cantons peut engager une procédure. Dans le domaine de la prévention, chaque canton décide, en concertation avec le NEDIK, des enquêtes secrètes qu'il entend mener pour lutter contre la pédocriminalité et des ressources qu'il mobilise en conséquence. Les enquêteurs doivent bien connaître le mode opératoire et les intentions des pédocriminels. Ces derniers, souvent actifs à l'échelle internationale, sont de véritables experts dans leur domaine. Les cyberpatrouilleurs doivent être capables d'agir en conformité avec leur profil, une compétence par ailleurs indispensable aussi pour dépister les autres types de délits sur Internet.

Prévenir la criminalité grâce aux cyberpatrouilles

Les forces de l'ordre suisses ne sont pas seulement présentes de manière cachée sur Internet, mais aussi à visage découvert. Plusieurs plateformes policières fournissent aux citoyens des conseils pour éviter de tomber dans les filets des cybercriminels. Elles y font aussi de la prévention en répondant aux questions posées par la population et en collectant des indices et des informations sur la criminalité qui se pratique sur Internet. Patrouiller dans le cyberespace permet ainsi d'accomplir le travail policier en toute transparence et dans un but préventif, là où se trouvent les citoyens internautes, ceci afin les conseiller sur le comportement à adopter en matière de sécurité numérique.

Avec son site internet cybercrimepolice.ch, la Police cantonale zurichoise assure le suivi des dangers en temps réel. Ce site fait de ses visiteurs les meilleurs patrouilleurs, puisqu'elle leur offre la possibilité de signaler de manière simple et rapide les nouvelles formes de criminalité, afin de sensibiliser et de mettre en garde d'autres internautes.

Des coopérations

Les enquêtes préventives menées dans le cadre des cyberpatrouilles ont permis de clore bien des affaires. Pour différentes raisons, il est important de combiner mesures répressives et mesures préventives dans le domaine de la cybercriminalité. La mission centrale du NEDIK est d'encourager et de coordonner. Un volet de cette mission consiste à soutenir les actions de prévention et les organisations parties prenantes à la cyberprévention nationale. Le NEDIK a ainsi décidé début 2021 d'intensifier sa coopération avec la Prévention Suisse de la Criminalité, l'une des principales organisations de prévention du pays. Les deux entités échangent des informations au sein du réseau afin de coordonner les actions de prévention et de répression, de partager des informations et d'adapter leurs formations.

Grâce aux cyberpatrouilles réalisées en l'absence de soupçons, les forces de police suisses ont beaucoup de succès à leur actif. Ces opérations leur permettent d'identifier les individus qui participent à des transactions illégales, de les localiser, de les arrêter et de les faire juger. La combinaison de mesures répressives et de mesures préventives s'avère donc déterminante dans la lutte contre la cybercriminalité et le NEDIK y joue un rôle important, puisqu'il est chargé d'encourager la coopération en matière d'enquêtes. Pour que leur action porte ses fruits, les diverses autorités doivent s'épauler dans un souci d'efficacité et de pragmatisme. L'espace numérique mondialisé permet à ses usagers de se mouvoir à l'échelle planétaire. Les forces de police suisses doivent par conséquent elles aussi pouvoir puiser dans des ressources globalisées et coopérer de manière très étroite, tant sur le plan intercantonal qu'à l'international, afin de lutter résolument contre la cybercriminalité, cette nébuleuse qui ne connaît pas de frontières.

123RF/Kirill Makarov

« Grâce aux cyberpatrouilles réalisées en l'absence de soupçons, les forces de police suisses ont beaucoup de succès à leur actif. »

* NCMEC = National Center for Missing and Exploited Children

Street-Art in Gloucestershire

« Les difficultés sont de deux ordres : premièrement, les difficultés d'ordre technique, deuxièmement la compréhension du contenu. »

Intercepter avec des médiateurs linguistiques – une pratique en quête de normes

Techniquement réalisable et licite, la surveillance des communications en temps réel permet de prévenir ou d'élucider des infractions. Or elle peut néanmoins échouer lorsque le contenu n'est pas compris. Les autorités de poursuite pénale sont fortement tributaires des interprètes. Pourtant, leur rôle est un champ d'étude peu exploré. Un projet de recherche de l'Université de Neuchâtel est consacré à cette problématique.

Pratiquer la surveillance secrète des communications est possible depuis que le premier poteau télégraphique a été planté en 1840. Depuis, chaque invention a permis le développement de nouveaux dispositifs de surveillance, alors que les progrès réalisés dans le même temps en matière de chiffrage constituaient de sérieux obstacles pour les autorités de poursuite pénale qui souhaitaient accéder au contenu des conversations. Aussi est-il spectaculaire que des enquêteurs de police étrangers parviennent à accéder à des réseaux cryptés tels que *IronChat*, *Sky ECC* et *EncroChat*. Les chiffres de l'opération *Sky ECC* sont époustouflants : plus de 170 000 utilisateurs dans le monde, basés en Europe, en Amérique du Nord, en Amérique du Sud et au Moyen-Orient, dont les enquêteurs auraient intercepté environ un milliard de messages cryptés. Pour les autorités chargées de l'enquête pénale, ce volume de données vertigineux pose à lui seul un problème de capacités à la limite du gérable.

Une question, cependant, est rarement soulevée dans ce contexte, malgré sa pertinence : que se passe-t-il

Auteure

Nadja Capus
Prof. Dr. iur.
Chaire de droit pénal et de procédure pénale Université de Neuchâtel

DR

VSI

« Les médiateurs linguistiques ont besoin de compétences très spécifiques : les communications se font dans le langage parlé, en recourant au dialecte ou à des régiolectes, aussi bien que dans le langage codé du milieu des personnes interceptées. »

(Photo: Nicole Kidman dans « L'interprète », 2005)

lorsque les messages sont échangés dans une langue inconnue de l'autorité compétente ? Il apparaît rapidement que les difficultés sont de deux ordres : premièrement, les difficultés d'ordre technique, deuxièmement – et surtout –, la compréhension du contenu. Ce second écueil est d'autant plus insurmontable lorsqu'il ne s'agit pas de communications écrites mais de conversations orales. Le premier et principal intercepteur est donc un ou une interprète ; pour notre part, nous désignons cette activité spécifique du terme de « médiateur ou médiatrice linguistique ». On ignore bien souvent combien les autorités de poursuite pénale sont tributaires de ces personnes.

Les conséquences fatales d'une médiation linguistique déficiente

Les conséquences d'une surveillance secrète des communications peuvent être fatales si les médiateurs linguistiques sont trop peu nombreux, s'ils sont mal ou pas du tout formés et/ou si les instructions qu'on leur donne sont insuffisantes ; que de temps perdu si la traduction doit être revue par une autre personne ou si les fautes commises rendent les séquences interceptées, enregistrées et traduites inutilisables comme moyens de preuve !

Il faut savoir qu'après le 11 septembre, l'enquête menée par le FBI sur les attentats terroristes aux États-Unis a marqué le pas en raison de trop faibles ressources en médiateurs linguistiques ; dans une affaire de passeur traitée par la justice autrichienne, il est ressorti que le médiateur linguistique, en concertation avec la police, avait en partie retranscrit dans le procès-verbal des déclarations complètement différentes de celles que l'on pouvait entendre dans l'enregistrement, afin que cela « fasse une meilleure impression » *(Der Standard,* 6 mai 2014). En Suisse, certaines affaires judiciaires ont montré que la coopération avait été infructueuse et que les prestations des médiateurs linguistiques étaient déficientes (voir les arrêts du Tribunal fédéral des 28 janvier 2005 et 23 septembre 2013) : des jugements ont été annulés et les affaires renvoyées à l'instance inférieure avec l'obligation, pour chaque enregistrement qu'elle souhaitait utiliser, de documenter la méthode appliquée pour convertir dans la langue de la procédure l'enregistrement de la conversation téléphonique en langue étrangère. En outre, l'instance était tenue d'indiquer l'identité des personnes impliquées dans l'enquête, ainsi que les instructions données à chacune d'elles, et enfin, de fournir la preuve que chacune des personnes concernées avait été rendue attentive aux sanctions pénales prévues à l'article 307 CP en cas de faux rapport ou de fausse traduction. En l'absence de ces informations, les traductions écrites des communications secrètes interceptées ne sont purement et simplement pas exploitables comme moyens de preuve.

Tels sont, en résumé, les éléments rudimentaires de la norme énoncée par le Tribunal fédéral en 2002 dans son

arrêt de principe ATF 129 I 85. Mais est-elle respectée par les cantons ? A-t-elle un sens ? Devrait-on l'étendre ? Que se passe-t-il dans la pratique, et qu'en disent les personnes concernées ? C'est à ces questions, entre autres, que se consacre notre projet de recherche.

Un objet d'étude peu accessible

Le recours aux services d'interprètes, de traducteurs et de médiateurs linguistiques n'est pas rare dans les procédures pénales. L'interprète restitue oralement dans la langue cible, en se pliant à de grandes contraintes temporelles, ce qui est dit ou écrit dans la langue source. L'activité de traduction, elle, revient par exemple à traduire directement par écrit des conversations interceptées ou des documents écrits. Dans le contexte de la surveillance secrète des communications, il peut s'agir de l'une et l'autre activité, raison pour laquelle nous utilisons le terme de médiation linguistique. Bien que cette activité intervienne à un moment crucial de l'enquête pénale, peu d'études primaires existent sur le sujet en dehors de la Suisse, parce que l'intérêt à garder le secret est évidemment considérable.

Depuis décembre 2019, le Fonds national suisse de la recherche scientifique finance notre projet interdisciplinaire qui se propose d'étudier les contributions d'intermédiation linguistique sous l'angle de leurs conditions de production et de l'usage qui en est fait dans le cadre de la surveillance secrète des communications. De fructueuses coopérations avec les autorités de police et le ministère public de différents cantons (mais pas avec le ministère public de la Confédération) nous ont facilité l'accès à ce domaine pour lequel les conditions de recherche sont difficiles à réunir.

Afin de pouvoir examiner plus en détail les activités des médiateurs linguistiques, nous menons des entretiens avec eux et avec des enquêteurs de police de certains cantons, ainsi qu'un sondage en ligne dans tout le pays auprès de médiateurs linguistiques recrutés par la police. L'objectif est de collecter des informations sur leur formation, leurs compétences linguistiques et de traduction, et leur expérience professionnelle. Les données collectées sont complétées par des observations directes sur le terrain. Par ailleurs, le projet se concentre sur les produits du travail des médiateurs linguistiques : se fondant sur l'analyse de 22 dossiers pénaux provenant de quatre cantons, il s'agit de déterminer, d'un point de vue juridique et juridico-sociologique, comment le travail des médiateurs linguistiques est intégré dans les enquêtes pénales et comment il est documenté. Enfin, des enregistrements audio et les procès-verbaux d'interception sont passés au crible de l'analyse traductologique. L'accent est mis sur les stratégies et les méthodes de travail des médiateurs linguistiques. Le projet retrace aussi les étapes du développement d'un moyen de preuve résultant d'une conversation interceptée et versé au dossier sous forme écrite.

Premiers constats

La conscience du problème s'est visiblement accrue ces dernières années puisque des efforts sont déployés tant au niveau européen que cantonal – la Confédération fait malheureusement exception – afin d'améliorer la qualité des prestations linguistiques et intégrer celles-ci dans les procédures pénales en termes de documentation, de vérification et de possibilité de contestation. Cependant, l'une de nos analyses montre que ces efforts se concentrent sur les interprètes les plus visibles, ceux qui sont présents lors des interrogatoires et des audiences. Or, l'activité de médiation linguistique exige des stratégies de traduction très différentes et des compétences très spécifiques : les communications se font dans le langage parlé, en recourant au dialecte ou à des régiolectes, aussi bien que dans le langage codé du milieu des personnes interceptées ; à noter que l'interception suppose de recourir à des dispositifs techniques dans des circonstances parfois difficiles, lesquelles peuvent altérer la perception acoustique. Il s'agit de dialogues téléphoniques ou (dans le cas de placements de micros dans des véhicules ou des locaux) de conversations entre plusieurs personnes que le médiateur linguistique ne voit pas pendant l'écoute. Sa capacité d'écoute est donc primordiale lorsqu'il s'agit de reconnaître des voix différentes ou un changement de langue. Le haut degré de spontanéité de ces mandats exige également des médiateurs linguistiques, outre le fait qu'il s'agit d'une activité hybride d'interprétation et de traduction, une faculté d'anticipation poussée et des connaissances spécialisées. Compte tenu de la diversité des compétences requises, il est surprenant qu'il soit communément admis (aussi par le Tribunal fédéral) qu'il suffise d'être bilingue pour exercer cette activité, pourtant si particulière et si exigeante.

Le traitement réservé aux informations et aux preuves ainsi obtenues ne tient pas compte de ces particularités, comme le montre l'analyse de la littérature consacrée à ce sujet, de la jurisprudence du Tribunal fédéral et des actes de procédure. Notre analyse de ces actes (dont la moitié a jusqu'à maintenant été réalisée) montre que les critères de validité établis par le Tribunal fédéral ne sont généralement pas remplis dans la pratique. Par exemple, l'identité des interprètes n'y est pas mentionnée, pas davantage que les informations sur la méthode appliquée pour l'interprétation ou les instructions données aux linguistes. Il est relativement rare de voir mentionné que les médiateurs linguistiques ont été rendus attentifs à l'article 307 CP, et encore plus rare qu'ils l'aient été concernant l'article 320.

Il convient de souligner que l'activité des médiateurs linguistiques intervient à un point de croisement sensible entre l'établissement des faits et leur interprétation juridique, raison pour laquelle les formes informelles de coopération peuvent rapidement revêtir un

poids considérable. Cependant, il ressort des données que nous avons déjà collectées que les divergences sont considérables concernant la répartition des rôles définie par les autorités, l'auto-évaluation des médiateurs linguistiques ainsi que la manière dont ils sont instruits sur le cas et la méthode de travail.

Il est intéressant de relever que le Tribunal fédéral, qui – comme nous l'avons vu – a joué un rôle important dans le développement normatif dans ce domaine, établisse une jurisprudence en partie contradictoire. En effet, celle-ci exige, d'une part, que l'identité des médiateurs linguistiques, les instructions reçues et la réalisation de leur travail soient plus visibles. D'autre part, les arrêts prononcés permettent de reléguer dans l'ombre la contribution des médiateurs à la collecte et à la sélection des informations jugées pertinentes pour la procédure, ainsi que la grande responsabilité qui leur incombe. Une grande partie des informations indispensables aux enquêteurs est donc échangée de manière informelle entre les médiateurs linguistiques et la police.

Perspectives

En résumé, les problèmes résultant de mauvaises interventions linguistiques peuvent entraîner des coûts, conduire à la perte de preuves, affaiblir les éléments à charge ou à décharge et contribuer ainsi à l'échec des procédures pénales, ou provoquer des retards qui augmentent le risque de prescription. Notre projet de recherche interdisciplinaire, qui s'achèvera en novembre 2022 au bout de trois ans, a pour objectif de contribuer à combler les lacunes de recherche susmentionnées et, en échangeant avec des représentants du terrain, de tirer des enseignements qui aideront la police et les ministères publics à mettre au point de bonnes pratiques en matière de sélection et de travail des médiateurs linguistiques dans le cadre de la surveillance secrète des communications. L'objectif est également d'informer les tribunaux sur les normes souhaitables en matière de collecte et d'utilisation des preuves. Pour sa réussite, le projet de recherche bénéficie de la généreuse coopération des autorités de police, des ministères publics et des tribunaux.

Pour plus d'informations, consulter le site Internet du Centre romand de recherche en criminologie de l'Université de Neuchâtel : www.unine.ch/crrc/intercept-interpret.

Personnes de contact :
Prof. Dr. Nadja Capus, responsable du projet (nadja.capus@unine.ch, 032 718 13 05 ou 079 536 50 52),
Dr. Damian Rosset (damian.rosset@unine.ch),
Dr. Cornelia Griebel (cornelia.griebel@unine.ch),
Dr. Ivana Havelka (ivana.havelka@unine.ch),
MLaw Elodie Bally (elodie.bally@unine.ch).

La surveillance électronique en Suisse

En Suisse, la surveillance électronique est principalement utilisée pour appliquer des peines de privation de liberté. Ce faisant, elle permet surtout d'identifier a posteriori le non-respect des conditions imposées par les autorités et de tester la capacité de la personne condamnée à prendre des engagements et à les tenir. Elle représente donc actuellement une sanction de substitution et pas un outil servant à prévenir un délit, mais les choses sont en train de changer.

Depuis 1999 déjà, le port du bracelet électronique remplace en partie l'exécution de la peine dans un établissement pénitentiaire. Dans le cadre d'un projet pilote, la Confédération avait alors autorisé six cantons – Bâle-Ville, Bâle-Campagne, Berne, Genève, le Tessin et Vaud –, auxquels est venu s'ajouter Soleure en 2003, à exécuter certaines peines privatives de liberté au moyen de la surveillance électronique (SE). Après l'avoir expérimentée une dizaine d'années, ces cantons s'en étaient généralement dits satisfaits. Depuis le 1er janvier 2018, date à laquelle elle a

Auteur·e

Janine Repetti-Dittes
Secrétaire générale Association *Electronic Monitoring*


DR

Alain Hofer
Sercétaire général adjoint, Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP)


DR

123RF/stocksolutions

« La surveillance électronique n'est envisagée que lorsque le risque de fuite et de récidive est pratiquement nul. »

fait son entrée dans le code pénal, cette pratique figure dans le droit fédéral. Depuis lors, les cantons sont tenus de proposer la surveillance électronique comme mode d'exécution des peines privatives de liberté.

La surveillance électronique peut, à certaines conditions, être appliquée pour de brèves peines privatives de liberté allant de 20 jours à douze mois (SE dite *frontdoor).* Il est aussi possible d'y recourir pour une durée de trois à douze mois, pour des personnes qui sont sur le point de bénéficier d'une libération conditionnelle après avoir purgé une longue peine privative de liberté (SE dite *backdoor).* Elle n'est envisagée que lorsque le risque de fuite et de récidive est pratiquement nul. La personne condamnée doit avoir un domicile fixe et un quotidien structuré (travail ou formation) ; elle doit aussi approuver cette forme d'exécution de peine et le calendrier proposé, et se montrer capable de prendre des engagements et de les tenir. Enfin, le consentement des adultes de son ménage est aussi exigé. Si l'on peut s'attendre à ce qu'une personne représente toujours un danger, la surveillance électronique n'entre pas en ligne de compte.

Les objectifs et avantages recherchés en faisant exécuter des peines privatives de liberté au moyen de la surveillance électronique tombent sous le sens : quand elle remplace une peine privative de liberté de brève durée, ne dépassant pas l'année, elle évite en grande partie la stigmatisation que produit l'incarcération. La personne condamnée n'est en effet pas coupée de son cadre familier. Elle peut continuer à travailler et à fréquenter son milieu professionnel et privé. Comme elle n'est toutefois autorisée à quitter son domicile qu'à des heures précises et doit passer son temps libre en arrêts domiciliaires, la peine privative de liberté conserve son caractère punitif. Utilisée à la fin d'une peine longue, la surveillance électronique peut faciliter la réinsertion contrôlée dans la société. De la sorte, elle réduit nettement les coûts de réinsertion et d'exécution des peines, à charge de la collectivité.

Champs d'application

Depuis longtemps déjà, d'autres champs d'application de la surveillance électro-

nique se sont ajoutés à celui de l'exécution de peines privatives de liberté. Dès le 1er janvier 2011, le code de procédure pénale en a fait un moyen de surveiller les mesures de substitution, qui remplace la détention provisoire ou la détention pour des motifs de sûreté ; depuis le 1er janvier 2015, le code pénal la prévoit pour l'application d'interdictions de contact et d'interdictions géographiques ; et dès le 1er janvier 2022, le droit civil y aura recours pour protéger les victimes de violence. D'autres applications sont envisagées : une surveillance électronique est également prévue dans le cadre des mesures policières de lutte contre le terrorisme ; enfin, il en est aussi question pour le domaine des mesures de contrainte en application du droit des étrangers.

Exigences techniques et types de surveillance

Ces nouveaux champs d'application ont modifié les exigences et attentes d'ordre technique. Dans le cadre de l'exécution de peines privatives de liberté, on ne cherche généralement pas à savoir précisément où se trouve la personne surveillée quand elle n'est pas chez elle. On se limite à vérifier qu'elle est bien à son domicile aux heures déterminées, et donc à établir sa présence ou son absence à un endroit déterminé. Ce genre de surveillance ne nécessite donc pas de système de géolocalisation (GPS ou *global positioning system)* par exemple, puisque la localisation précise importe peu. Il suffit d'avoir recours au mode radiofréquence : le système mesure seulement la distance entre l'émetteur, qui est fixé à une cheville de la personne condamnée, et le récepteur, installé à son domicile. Le signal est transmis via le réseau téléphonique au service compétent, qui compare les données reçues avec le programme préétabli. Si les absences du domicile ne coïncident pas avec le calendrier fixé, ou si la personne surveillée tente de manipuler ou d'enlever l'émetteur,

Adobe Stock/toya_uz

« A l'avenir, le champ d'application de la surveillance électronique est appelé à s'élargir, surtout dans le domaine de compétence de la police, afin de prévenir la violence domestique et le harcèlement. »

une alarme s'enclenche. Actuellement, la radiofréquence est le mode de surveillance le plus utilisé en Suisse.

Dans les autres domaines, les exigences techniques sont quelque peu différentes. Lorsqu'on a recours à la surveillance électronique en application du droit civil, afin de protéger de potentielles victimes de violence par exemple, la localisation de la personne sous contrôle doit pouvoir être transmise et enregistrée en continu. La technologie GPS est alors nécessaire, puisqu'elle permet de contrôler de manière permanente les allées et venues de la personne et d'établir des profils de déplacement. Techniquement, il existe plusieurs possibilités d'exercer une surveillance par GPS.

Assurant une localisation en temps réel, la surveillance par GPS présente l'avantage d'avoir aussi un effet préventif, puisque la personne surveillée est consciente que la probabilité d'être découverte en cas d'infraction est très élevée.

Cependant, la surveillance par GPS a aussi ses limites techniques : dans certains lieux, comme les grands centres commerciaux, les caves ou les tunnels, la réception satellite est limitée. Le réseau mobile peut alors prendre le relais, en localisant la personne en fonction de sa distance d'avec le pylône de téléphonie mobile le plus proche. La précision de la localisation dépend alors de la densité du réseau.

La technologie GPS permet de contrôler a posteriori les déplacements d'une personne (surveillance passive) ou en temps réel (surveillance active). En cas de surveillance passive, les données des mouvements sont analysées par l'autorité compétente durant les heures de bureau principalement. En cas de surveillance active, ce contrôle se fait en temps réel, vingt-quatre heures sur vingt-quatre, et les alarmes sont immédiatement transmises à une centrale qui ordonne l'intervention prédéfinie en fonction du cas. Cette réaction peut aller de la prise de contact téléphonique avec la personne surveillée au déclenchement d'une intervention de police. On ne saurait toutefois voir dans le recours à la surveillance électronique un moyen fiable d'empêcher les délits : la surveillance active pouvant susciter des attentes qu'elle n'est pas à même de remplir, il convient de faire preuve de prudence en y recourant. Elle s'avère en effet problématique si les forces de police doivent intervenir immédiatement pour prévenir un éventuel délit lorsque la personne condamnée ne respecte pas le cadre fixé.

Collaboration intercantonale : le point de la situation

Les expériences faites ont montré qu'il n'est pas judicieux que chaque canton se dote de ses propres structures pour suivre les cas sous sa compétence. La Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) a par conséquent mandaté en 2013 déjà des travaux d'harmonisation de la surveillance électronique. Une association ayant pour but d'assurer les investissements et l'exploitation de la surveillance électronique en Suisse a finalement vu le jour en automne 2019. Cet organisme, qui regroupe 22 cantons actuellement, a pour mission de proposer à ses membres une solution nationale en la matière, qui prenne en compte les besoins de chacun d'entre eux pour ce qui est des différentes applications de la surveillance électronique.

En novembre 2020, lors de l'assemblée d'automne de la CCDJP, les cantons membres ont décidé de ne pas se doter, dans un premier temps, et dans le cadre du projet actuel, d'une centrale de surveillance unique. Le nouveau système ne permet donc pas, dans un premier temps, de pratiquer la surveillance active dans tous les cantons membres. A cette même occasion, la CCDJP a aussi tenu à ce que les dispositifs retenus permettent dans un second temps de le faire, estimant s'assurer ainsi de pouvoir introduire sans problème la surveillance active le moment venu, quand les cantons qui collaborent avec une centrale et pratiquent la surveillance active auront suffisamment d'expérience dans le domaine.

En février 2021, un appel d'offres public a été lancé afin de trouver un exploitant qui propose une solution nationale remplissant les exigences et conditions que les représentants des cantons et des divers groupes d'intérêt ont fixées lors de la conception du projet. Trois cantons pilotes effectuent en ce moment des tests avec les appareils de trois prestataires. Le nouveau système doit être mis en place au cours de l'année 2022 dans tous les cantons, et entrer en fonction au plus tard au 1er janvier 2023.

Conclusions et perspectives

A l'heure actuelle en Suisse, la surveillance électronique est utilisée avant tout dans le domaine de la privation de liberté. Elle y sert principalement à constater a posteriori les infractions au régime d'application fixé par les autorités et à tester la capacité de la personne condamnée à prendre et à tenir ses engagements. Toute violation est communiquée au service compétent et, si nécessaire, sanctionnée. Telle qu'elle est utilisée actuellement, la surveillance électronique représente donc une sanction de substitution et pas un outil de prévention.

A l'avenir, son champ d'application est appelé à s'élargir, surtout dans le domaine de compétence de la police, afin de prévenir la violence domestique et le harcèlement ; en l'espèce, l'idée est de tester l'utilisation conjointe de la surveillance électronique et d'autres outils de protection contre la violence. La stratégie qui semble la plus prometteuse est de combiner les mesures de surveillance électronique avec une gestion efficace de la menace.

L'association *Electronic Monitoring* proposera aux cantons une solution unique et pragmatique. L'objectif est que la surveillance électronique et les possibilités techniques qui lui sont liées soient utilisées dès lors qu'elles apportent une réelle valeur ajoutée.

« Il faut toujours faire la part des choses. »

PSC Info s'est entretenu avec Jürg Halter de la question des liens qui existent entre la surveillance privée ou étatique et la crise sanitaire, la numérisation, la démocratie, le besoin d'avoir des réponses simples et la langue en tant que telle.

© by Rob Lewis

L'écrivain et performeur Jürg Halter, lauréat de nombreux prix, vit et travaille à Berne. Il participe activement au débat public, notamment dans les médias sociaux Twitter et Facebook. Son recueil de poèmes Gemeinsame Sprache *est paru récemment aux éditions Dörlemann.*

Jürg Halter, au début de cette année, vous avez été invité à l'émission littéraire « Literaturklub » de la SRF où vous avez présenté une nouvelle traduction de « 1984 » de George Orwell, sans doute la plus célèbre des œuvres ayant pour thème la « surveillance ». Quels sont les aspects de cette problématique qui vous intéressent plus particulièrement ?

Le roman d'Orwell, paru en 1949, illustre de manière magistrale ce qui se passe lorsqu'un Etat se met à contrôler les faits et gestes et les propos de tout un chacun. Il décrit un monde où les gens sont surveillés 24 heures sur 24 ; un écran de télévision leur signale quand ils doivent aller se coucher, quand ils doivent se lever et ils sont aussi surveillés pendant leurs heures de travail ; il y a également une police de la pensée qui, au moyen des écrans de télévision, interprète les expressions du visage et détecte si quelqu'un est en train de penser quelque chose contre l'Etat ou contre l'une de ses lois. Dans un tel cas, les gens sont réveillés brutalement et arrêtés, avant de disparaître purement et simplement. Ou alors on leur fait un lavage de cerveau, dont ils ressortent prétendument purifiés mais plus exactement hébétés, avant de les réinsérer dans la société. On pourrait dire qu'il s'agit d'une exagération, pourtant, Orwell s'est évidemment inspiré des dictatures bien réelles de son époque, du stalinisme surtout, mais évidemment aussi du nazisme. Ce qui rend ce roman à la fois fascinant et effrayant, c'est qu'il est toujours d'actualité.

… ou qu'il l'est de nouveau ou plutôt que les possibilités techniques n'ont jamais été aussi proches du récit ; la surveillance des micro-expressions du visage, par exemple, sera peut-être bientôt une réalité.

Exactement. Le roman reflète non seulement l'époque à laquelle il a été écrit, mais il fait aussi des prédictions si pertinentes qu'elles donnent froid dans le dos. Et cela devient encore plus cauchemardesque si l'on considère que la technologie est bien plus avancée aujourd'hui que tout ce que l'on aurait pu imaginer à l'époque. Je pense par exemple aux *deep fakes* (hypertrucage), c'est-à-dire la possibilité, à partir de quelques fichiers vidéo, de reproduire la voix d'une personne pour lui faire dire des choses qu'elle n'a jamais dites et d'utiliser ses prétendus propos pour l'incriminer. Mais à la différence de ce qui se passe dans le roman, aujourd'hui, un grand nombre de gens se surveillent eux-mêmes de leur plein gré (ou par consentement tacite) au moyen de leur smartphone ou de leur montre connectée, par exemple lorsqu'ils font du jogging, qu'ils mesurent leur pouls, leur fréquence cardiaque, etc., et transmettent ces informations à leur assurance qui leur accordera ou non une réduction de prime. Mais, ce n'est que dans un avenir indéterminé que les données qui sont recueillies au moyen de nos smartphones, ordinateurs, etc. seront potentiellement utilisées pour ou contre nous. Pour l'instant, la majeure partie de ces données n'ont même pas été analysées.

Nous vivons pourtant en Suisse dans – j'aurais envie de dire – l'un des derniers

pays démocratiques et nous sommes loin d'une société orwélienne dystopique. Quel est donc le degré de gravité du problème dans notre cas ? Risquons-nous d'assister à un brusque démantèlement de nos acquis démocratiques par des voies technologiques détournées ?

Je vois principalement deux sortes de menaces : l'une vient des géants de la technologie globalisée qui récoltent continuellement des données et l'autre vient de l'Etat, mais il s'agit ici de sa passivité : en effet, l'Etat se montre totalement impuissant face aux groupes internationaux, alors qu'il existe des possibilités légales de limiter la surveillance opérée par ces groupes technologiques. Toutefois, cela ne peut fonctionner que si l'ensemble de l'Union européenne prend les décisions qui s'imposent ; seul, un pays ne peut pas faire grand-chose. Un danger majeur réside aussi dans l'attitude naïve de beaucoup de gens qui ont tendance à affirmer que « si on n'a rien fait de mal, il ne peut rien nous arriver ». Mais il faut pourtant toujours se poser la question de savoir qui définit ce qui est bien ou mal. En effet, lors d'un changement de système, il peut vite arriver que ce qu'on croit encore être bien est brusquement devenu mal, et là ça devient vraiment dangereux. À mon avis, on présente la numérisation de manière bien trop positive, en parlant exclusivement de liberté accrue. C'est pourtant la numérisation qui rend toujours plus transparent et donc toujours plus vulnérable. Et si les individus sont vulnérables, alors la société dans son ensemble et la démocratie sont de plus en plus menacées, car la démocratie prospère grâce à la confiance.

Quel est exactement le lien entre la numérisation croissante et la perte de confiance ? On observe qu'avec la crise sanitaire, la confiance dans les mesures prises par l'Etat fait souvent défaut. Plusieurs de vos collègues du monde culturel se montrent sceptiques, ils voient des complots ou parlent même de dictature. Quel est votre sentiment ?

Tout d'abord, lorsqu'on leur tend un micro et qu'on leur pose une question, bien des gens ont tendance à répondre, même s'ils ne sont pas qualifiés pour le faire. Les acteurs culturels ne sont pas à l'abri de la bêtise et ils sont aussi susceptibles que d'autres de croire à des réponses simplistes, à des ennemis supposés et à des théories du complot. Il y a certes quelques Etats qui ne pouvaient pas passer pour des démocraties avant la crise sanitaire et qui ont profité des mesures de lutte contre la pandémie pour limiter encore plus la liberté de leurs citoyens. C'est une réalité. En revanche, parler d'une dictature en Suisse n'est pas sérieux, car les mesures prises sont largement compréhensibles et elles ont été communiquées clairement. On ne peut toutefois pas s'attendre à ce que chacune des mesures prises soit adéquate et n'ait pas d'alternative, car la crise sanitaire est quelque chose de nouveau pour tout le monde et il faut pouvoir réagir souplement. Bien des gens ne se rendent même plus compte de l'existence de l'Etat à part lorsqu'ils doivent payer leurs impôts ; alors, la puissance avec laquelle il s'est manifesté presque d'un jour à l'autre a été une surprise, mais il n'y a pas d'autre manière de réagir à une catastrophe naturelle. Si l'on avait dû organiser une votation au sujet des mesures, le nombre de morts aurait été bien plus élevé et la catastrophe bien plus grave. Pourtant bien des gens cherchent des explications simplistes, ils imaginent que des forces maléfiques sont à l'œuvre et croient que la pandémie n'est qu'une manœuvre de diversion, etc. Il y a toujours eu des théories du complot de ce style, mais aujourd'hui, avec la numérisation, elles se propagent beaucoup plus vite et les gens qui y croient entrent en contact avec davantage de facilité.

Quel rôle jouent les médias ?

Les médias ont, bien sûr, toujours un œil sur les clics qu'ils génèrent et sont enclins à accorder davantage d'espace à ceux qui parlent le plus fort même si ces derniers représentent rarement la majorité de la population. Les médias ont à mon sens aussi une responsabilité, par exemple parce qu'ils utilisent de manière erronée le terme de sceptique qui a une définition claire. Celui qui nie l'existence ou la dangerosité du virus n'est pas un sceptique, mais quelqu'un qui nie la réalité. Celui qui critique les mesures à l'aide d'arguments étayés est un sceptique. Mais, dans les médias, il y a une totale confusion entre ces deux termes. Voici ce que je voudrais dire aux médias : donnez davantage d'attention aux personnes qui s'expriment de manière critique, mais qui avancent des arguments rationnels à l'appui de leurs dires, donnez-leur davantage d'espace qu'à ceux qui mentent et qui diffusent des théories du complot. Les gens qui disent sérieusement que nous vivons ici dans une dictature, je les enverrais volontiers voir ce qui se passe en Biélorussie ou en Corée du Nord afin qu'ils expérimentent leur conception de la liberté.

Ou en Autriche ? Plaisanterie mise à part, il semble que, par le passé, il était plus facile de se mettre d'accord sur ce qui était un fait et ce qui n'en était pas un et de discuter ensuite de la manière d'évaluer ces faits. Aujourd'hui, il semble que pour chaque fait, il existe un fait alternatif ; chacun peut croire ce qu'il veut et déclarer qu'il s'agit d'un fait. Comment en sommes-nous arrivés là ?

La technologie numérique donne à beaucoup le sentiment qu'ils peuvent légitimement prendre part à la discussion alors qu'avant, seules les élites étaient autorisées à le faire. C'est une chose positive sur un plan et hautement problématique sur un autre plan, car il n'y a pratiquement plus d'inhibition à s'exprimer. Par le passé, il fallait par ex. se donner la peine d'écrire une lettre de lecteur, à la machine ou à la main, l'affranchir et l'envoyer ; il y avait donc plusieurs obstacles à surmonter. Ensuite une rédaction décidait si la lettre devait être publiée ou non. Aujourd'hui il suffit d'un clic pour publier

ses propos, ce qui est très tentant. Chacune et chacun devient son propre média. On en arrive d'ailleurs à certaines contradictions : des personnes qui ne cessent de publier des informations et des photos sur tous leurs faits et gestes sur les réseaux sociaux se fâchent lorsqu'elles doivent laisser leurs coordonnées au restaurant, car cela menacerait leur liberté. Ces contradictions nous concernent tous un peu : nous exigeons le respect de notre anonymat et de notre sphère privée d'une part et notre propre comportement nous trahit d'autre part.

En ce qui concerne l'opposition entre faits et affirmations, opinions, *fake news*, etc. J'ai le sentiment qu'on assiste à une évolution problématique, car ici aussi, aucune différenciation n'est faite : on peut pourtant être du côté de la science, croire aux faits et malgré tout porter un regard critique sur certaines évolutions scientifiques. Par exemple, si on lit une étude portant sur la teneur en sucre des aliments et qu'en s'informant un peu plus, on constate que cette étude a été mandatée par une entreprise agroalimentaire, alors il faut se montrer critique vis-à-vis de cette étude. Il faut toujours faire la part des choses. Mais beaucoup de gens veulent des réponses claires et ne supportent pas les points de vue contradictoires. Comme s'il n'y avait jamais que le juste et le faux, le pour et le contre, l'un ou l'autre.

On retrouve là le principe binaire du monde numérique : oui ou non, des zéros et des uns ! Des personnes visionnaires craignaient déjà dans les années septante et quatre-vingt qu'après avoir laissé l'informatique imprégner notre vie et notre pensée, nous en devenions victimes en ce sens que nous ne pourrions même plus imaginer qu'il est indispensable d'avoir aussi « l'un et l'autre », le « ni, ni » et le « peut-être ».
C'est une chose grave que la numérisation déteigne sur notre pensée. On le voit par exemple dans le système éducatif avec les tests à choix multiple : on ne doit plus formuler et évaluer les choses soi-même, mais simplement cliquer ceci ou cela, et c'est tout. C'est dangereux, car une démocratie digne de ce nom se nourrit de la diversité, des différences, de la tolérance et du respect des opinions et points de vue des autres. La démocratie a aussi besoin qu'on trouve des consensus sur certains éléments, par exemple sur le fonctionnement de la démocratie elle-même ! C'est de tout cela que vit un Etat de droit. Mais la numérisation, telle qu'elle s'est développée, nous amène à croire que nous devons toujours prendre parti pour un côté ou pour l'autre. Cela conduit, en fin de compte, à une fragmentation de la société en bulles toujours plus étanches de personnes qui partagent les mêmes opinions.

Jean Ziegler vous a cité comme une voix politique de premier plan dans notre pays. Quel est le lien entre votre activité d'écrivain et votre engagement politique ?
Etant donné que la langue est mon mode d'expression, j'essaie d'être toujours conscient de ce qu'on peut en faire, non seulement dans l'art, mais aussi d'une manière plus générale dans la société. La langue est souvent le moyen par lequel une démocratie est attaquée, mais elle sert aussi à la défendre. Puisque la langue peut servir à la propagande, je ne cherche pas uniquement à écrire de beaux livres ou de beaux poèmes, mais je m'intéresse aussi à son fonctionnement en général : ce qui est dit ou non, par qui et comment ; ce qui est nommé et ce qui est évité dans une formulation. Voilà pourquoi j'aime analyser les discours des hommes politiques et des chefs d'entreprise, par exemple. C'est précisément ce qui n'est pas dit qui en dit souvent plus que ce qui est dit. Les juristes sont aussi des personnes dotées d'une grande sensibilité linguistique, car dans le langage juridique, la manière de formuler les choses est d'une importance cruciale. Prenons par exemple le terme de « personne dangereuse » : il s'agit d'une notion très vague et, suivant le système dans lequel on se trouve ou la manière dont le terme est défini, une « personne dangereuse » peut être comprise comme quelqu'un qui a simplement une pensée critique. Et l'on pourrait ensuite en déduire que la surveillance de cette personne est nécessaire.

S'agit-il uniquement de propos formulés de manière vague ou pas formulés du tout ? Ou nous trouvons-nous déjà un peu plus loin, à un stade où de nombreux mots ont pris une signification nouvelle ? Je pense à cette phrase attribuée à Adorno : « Je ne crains pas le retour des fascistes sous le masque des fascistes, mais sous le masque des démocrates. » C'est exactement ce qui se passe maintenant avec le terme « terrorisme » : les dictateurs et les autocrates qui nous entourent accusent désormais par réflexe les manifestants pacifiques, les journalistes d'investigation et les autres opposants politiques de « terrorisme », car arrêter des terroristes est forcément une bonne chose. Mais en réalité, il s'agit d'une redéfinition éhontée du terme, ce n'est pas quelque chose de vague, mais un mensonge formulé avec précision. Que peut-on faire contre cela ?
Je trouve très dangereux qu'on détourne des termes de leur sens ou, pire, qu'on leur attribue le sens contraire dans le but de restreindre les libertés. Cela peut se passer à des niveaux très différents, par exemple lorsqu'on décrit la surveillance toujours plus intensive comme une défense de la liberté en oubliant tout simplement de dire l'autre moitié de la vérité. Ma mission en tant qu'écrivain, ou en tant que personne qui exprime publiquement des critiques, consiste à écouter avec attention – et à nommer – ce qui est réellement dit : est-ce que ce que l'on comprend ce qui a vraiment été dit ou est-ce que c'est le contraire qui est suggéré sans être exprimé ? Pour se prémunir des critiques déplaisantes, on utilise souvent des termes permettant de discréditer leur auteur, de le dépeindre comme une mauvaise personne, ou, face à des faits désagréables, on noie le langage sous

les mots. Ainsi, une critique portant sur la restriction des libertés sera réinterprétée comme une attaque contre la liberté. La meilleure façon de contrer ce phénomène est de dénoncer sans relâche les manipulations et distorsions linguistiques et d'en expliquer le mécanisme aux gens.

Encore une question personnelle : vous sentez-vous surveillé ?

Je sais que je me rends très vulnérable à la surveillance, ne serait-ce qu'à travers les ordinateurs que j'utilise, et, chaque fois que j'y pense, je suis effrayé de voir à quel point je suis probablement surveillé. Sachant la quantité de données que je livre, je suis en fait très peu prudent. C'est pourquoi je pense qu'il n'est pas bon que l'Etat transfère cette responsabilité aux citoyens. C'est à l'Etat qu'il incombe de restreindre la marge de manœuvre des entreprises technologiques, afin qu'elles n'aient pas la possibilité d'en savoir davantage sur les gens que ce qui est légalement autorisé. Il est illusoire de penser que l'utilisateur porte cette responsabilité. Et il faut également que l'Etat soit surveillé par des organismes indépendants qui contrôlent comment il utilise les données des citoyens. Si l'Etat surveille, il doit être surveillé aussi. Plus un Etat surveille, plus il est paranoïaque et moins il fait confiance à ses citoyens.

La surveillance, c'est bien, mais la confiance, c'est mieux ?

Pour justifier la surveillance, on invoque souvent la nécessité d'assurer la sécurité. Un équilibre doit être trouvé entre sécurité et liberté. Il est peut-être possible de garantir une sécurité absolue, mais cela signifie qu'il n'y a plus de liberté. Évitons d'entrer dans la logique de « l'un ou l'autre » et pensons « l'un et l'autre » ! Je suis bien sûr favorable à ce que cette question soit discutée de manière démocratique et transparente.

Jürg Halter, je vous remercie pour cet intéressant entretien.

Weber & Partner

Tags sur une affiche de l'OFSP dans la vieille ville de Berne, avril 2021.

Population et police : qui peut filmer qui dans l'espace public ?

En Suisse, la caméra piéton *(bodycam)* fait polémique et ne figure pas encore dans l'équipement policier réglementaire d'intervention, contrairement aux Etats-Unis. Dans notre pays, le principe de la transparence ne s'applique pas aux enregistrements vidéo. En outre, quiconque, y compris la presse, filme des opérations policières s'expose à des sanctions. C'est pourquoi, à l'ère de l'omniprésence des caméras dans l'espace public, il serait utile, pour toutes les parties concernées, de renforcer et d'affiner le dispositif légal.

Connaissez-vous *« Audit the Audit »,* la chaîne YouTube américaine qui analyse les interventions policières ? Sur la base d'enregistrements vidéo, elle évalue le comportement des personnes impliquées – policiers et autres représentants des pouvoirs publics d'une part, et citoyens d'autre part. Les interactions sont commentées en se référant aux bases légales et à la jurisprudence pertinente. Enfin, les personnes sont notées. Ainsi, une policière qui se comporte de manière exemplaire et conforme à la loi peut recevoir la note maximale de A+, tandis qu'un citoyen qui se comporte de manière incorrecte se voit attribuer un F, autrement dit insatisfaisant.

Le droit de filmer la police aux Etats-Unis

Les enregistrements vidéo proviennent de smartphones et caméras vidéo de citoyens, ainsi que de caméras piétons et caméras embarquées *(dashcams)* de la police. Les citoyens ont le droit de filmer les interventions policières même s'ils sont directement impliqués, par exemple lors d'un contrôle routier. En même temps, beaucoup de corps de police filment systématiquement leurs interventions avec leur propre caméra. Ces enregistrements sont considérés comme des archives publiques et sont donc accessibles à tout un chacun. Cela vaut aussi pour les photos et les enregistrements sonores. La base légale est fournie par le *Freedom of Information Act* (FOIA) au niveau fédéral et par des lois similaires dans les différents Etats. Filmer la police est un droit relevant du premier amendement et fait partie de la liberté d'opinion et de parole aux États-Unis *(« Freedom of Speech »).* C'est du reste grâce à ce droit de contrôle du premier amendement que certains militants – au comportement plus ou moins « sympathique » – vérifient si leur liberté d'expression est bel et bien garantie.

L'importance de ces vidéos a été récemment démontrée avec la mort de George Floyd survenue lors d'une opération policière à Minneapolis. Les enregistrements réalisés par des témoins et par la police ont fait le tour du monde et ont été versés au dossier lors de la procédure pénale.

En Suisse, les caméras piétons font l'objet d'une controverse politique et ne sont pas encore utilisées officiellement. D'ailleurs, contrairement aux Etats-Unis, le principe de la transparence ne s'applique pas aux enregistrements vidéo, que ce soit au niveau fédéral ou cantonal.

En outre, quiconque, y compris la presse, filme une intervention policière s'expose à des sanctions. Il arrive fréquemment que des personnes filmant ce genre d'opération soient appréhendées et contraintes d'effacer leurs enregistrements, voire de remettre leur smartphone. Ainsi, le 1er mai 2021, on a vu des professionnels des médias partiellement empêchés d'exercer leur métier d'information à Zurich.

Filmer en public : une pratique à l'encontre du droit

D'une manière générale, et indépendamment des opérations policières, filmer en public est une activité de plus en plus répandue : presque tout le monde possède, grâce à son smartphone, une caméra très perfectionnée, et il est possible de créer le buzz en publiant des enregistrements publics sur TikTok et d'autres médias sociaux – comme l'illustrent les nombreuses chaînes dédiées en plein essor (de type *Szene isch,* par exemple). Les caméras embarquées sont également de plus en plus populaires. Du reste, cette catégorie comprend désormais plus de cent produits livrables à tout moment via le commerce en ligne.

Or filmer en public et publier ces enregistrements sont des pratiques qui vont à l'encontre de l'ordre juridique suisse. La police peut en général compter sur la jurisprudence qui non seulement interdit que ses opérations soient filmées, mais qui rejette aussi l'utilisation des enregistrements de caméras embarquées pour poursuivre les infractions et les délits – et donc la grande majorité des infractions présu-

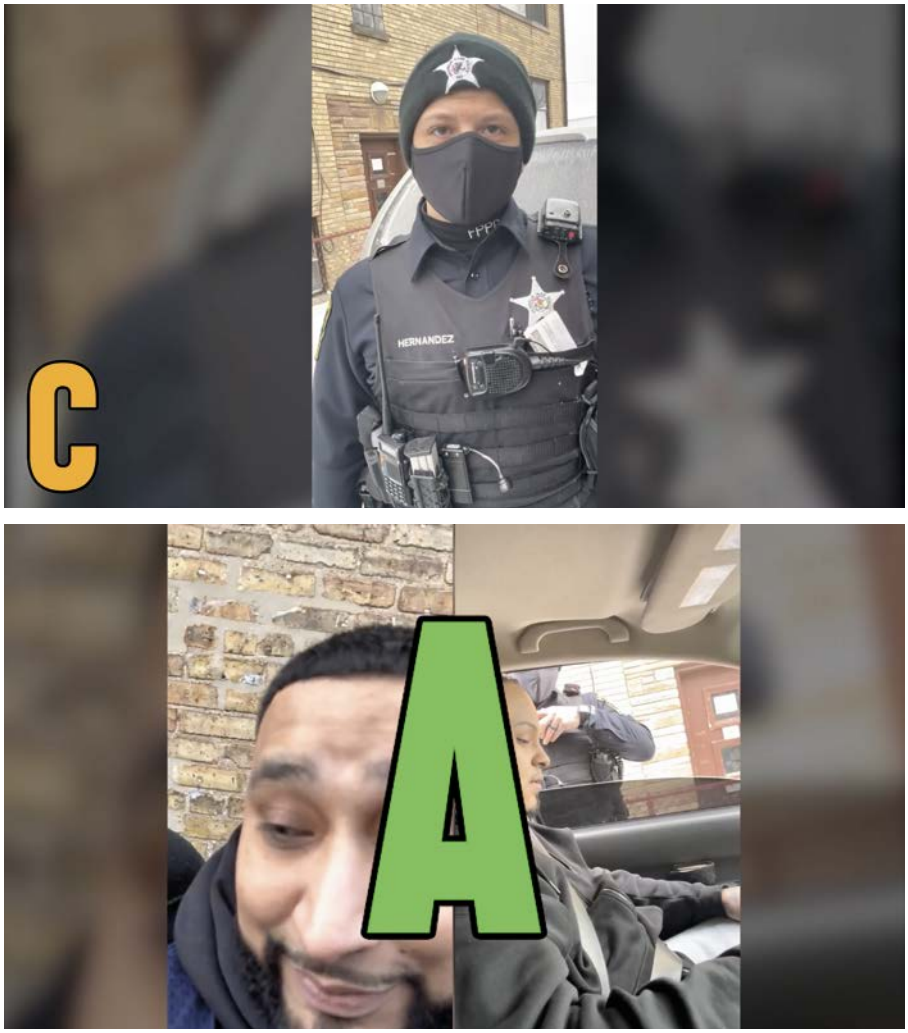
Auteur

Martin Steiger
Lic. iur. HSG
Avocat spécialiste du droit dans l'espace numérique, Zurich

DR

mées au Code de la route. Le seul fait de filmer, même sans publication ultérieure, peut violer les principes de la protection des données et de la protection des droits de la personnalité, en particulier avec le «droit à l'image». Depuis l'arrêt du Tribunal fédéral dans l'affaire Google Street View en 2012, il est clair que même les personnes «accessoires» doivent en principe consentir à être filmées dans le cas d'enregistrements numériques.

Etant donné qu'il est très compliqué pour les personnes filmées contre leur gré de porter plainte, la protection des droits de la personnalité ne peut pratiquement être invoquée que par l'avocat de la défense dans le cadre d'une procédure pénale. C'est probablement une des raisons pour lesquelles de nombreux policiers tentent d'empêcher dès le départ que leurs opérations soient filmées. Tout comme le fait que le «droit à l'image» ne bénéficie d'aucune protection en droit pénal, mais qu'il doit être appliqué dans une action civile, qui est – selon une volonté politique explicite – coûteuse et ne fonctionne pas sans l'assistance d'un avocat.



«Connaissez-vous ‹Audit the Audit›, la chaîne YouTube américaine qui analyse les interventions policières?»

Prolifération des enregistrements dans l'espace public

Les enregistrements vidéo dans l'espace public se multiplient, notamment lors d'interventions policières. Il est désormais évident que la police adopte des approches très différentes face aux violations présumées des droits. Ainsi, en présence de manifestants de gauche, il y a toujours des sanctions considérables – y compris à l'encontre des représentants des médias – alors que pour certaines manifestations contre les mesures de protection anti-COVID-19, non seulement il n'y pas eu de sanctions, au nom de la prétendue «proportionnalité», mais les forces de police ont dû, dans certains cas, se laisser littéralement défier par les manifestants, tandis que dans d'autres, il y a eu des scènes de fraternisation. Les enregistrements vidéo permettent d'ouvrir le débat sur cette inégalité de traitement, débat qui devrait aller de soi dans un État de droit démocratique, mais qui trop souvent n'a lieu que sur la base des «preuves» constituées par la publication desdits enregistrements vidéo.

Ce débat est utile, entre autres, à tout représentant de l'ordre qui n'est pas d'accord avec la procédure choisie, mais qui ne peut ou ne veut pas s'exprimer de manière critique.

Pour moi, il est clair que les opérations policières dans l'espace public doivent pouvoir être filmées, pour autant qu'il n'y ait pas de violation du droit de la personnalité. Du point de vue juridique, l'intérêt public supérieur justifie un contrôle rigoureux des activités de la police. Par ailleurs, il n'y a pas lieu de privilégier inutilement les professionnels des médias, car dans l'espace numérique, tout un chacun peut se coiffer de la casquette du journaliste, tandis que dans les médias traditionnels la frontière entre les rôles professionnel et privé devient floue. Cela dit, filmer et publier atteint ses limites lorsque des policiers se retrouvent à leur détriment sous le feu des projecteurs en tant que personnes, c'est-à-dire uniquement en raison de leur profession. Bien que certains d'entre eux aient beaucoup de pouvoir et représentent le monopole de la violence étatique, ils appartiennent fondamentalement aux forces de l'ordre dans leur globalité, dès lors qu'ils sont engagés sur le terrain. A l'inverse, les policiers devraient être autorisés à filmer leurs

«En ce qui concerne les opérations policières, il conviendrait de préciser – sur le plan légal ou judiciaire – qu'il existe un ‹droit de filmer la police› selon le modèle américain.» (Photo: 1er mai 2021 à Zurich, vidéo sur YouTube de Harp Lover)

opérations avec une caméra piéton – dans le cadre de règles strictes – voire être obligés de le faire. Tout enregistrement devrait être soumis au principe de la transparence: les droits des personnes filmées pourraient être examinés et garantis de manière adéquate au moment de la publication.

Sécurité juridique pour les prises de vue dans l'espace public

Pour que la population en général soit autorisée à filmer dans l'espace public, il faut établir une sécurité juridique au moins dans un certain nombre de domaines. Par exemple, l'utilisation des caméras embarquées pourrait être réglementée de manière constructive au bénéfice de la sécurité routière. Certes, les critiques à l'encontre des enregistrements vidéo ou de la vidéosurveillance sont le plus souvent justifiées, car le fait de se savoir filmé ou même de se croire filmé influence les comportements. Une telle «pression de surveillance» n'est pas tolérable dans une société libre, sauf peut-être dans certains cas, comme dans la circulation routière par exemple. Encadrer légalement l'usage des caméras embarquées pourrait consister à ce que seuls certains événements d'une durée de quelques minutes puissent être stockés et utilisés par les autorités. Par contre, le stockage infondé d'enregistrements de plusieurs heures, comme cela est courant aujourd'hui, serait interdit.

En légiférant, il serait possible de définir qui est autorisé à filmer qui dans l'espace public, et à quelles conditions. En outre, en tenant compte du nouveau consensus social créé par l'omniprésence des smartphones, l'action juridique serait bien plus efficace qu'une vaine interdiction. Car ceux qui sont privés du droit de filmer trouvent toujours un moyen de le faire. A ce propos, les manifestants commencent quand même à comprendre qu'il n'est pas judicieux de filmer l'événement auquel ils participent avec leur propre smartphone. Pour être sûrs de pouvoir publier leurs enregistrements et éviter que la police ne les saisisse, ils doivent les diffuser en direct sur Internet, ou alors filmer en cachette. Mais s'il s'agit de faire un reportage proprement dit et en toute sécurité, il vaut mieux faire appel à des équipes spécialisées qui garderont leurs distances, à l'instar des forces de police lors de certains événements.

En ce qui concerne les opérations policières, il conviendrait de préciser – sur le plan légal ou judiciaire – qu'il existe un «droit de filmer la police» selon le modèle américain. Quiconque n'interfère pas avec les opérations et ne met en danger ni soi-même ni les autres doit être autorisé à filmer. Quant à la publication, elle est soumise aux critères habituels en matière de droit de la personnalité, c'est-à-dire qu'en cas de litige, il convient d'effectuer une pesée des intérêts. Il devrait dès lors être plus facile pour les personnes concernées d'intenter une action en justice, ce qui permettrait, d'une part, de protéger efficacement les droits des individus et, d'autre part, d'affiner la pratique juridique par une jurisprudence différenciée. Quant aux policiers, ils doivent bien sûr pouvoir compter sur le soutien de leur corps de police s'ils souhaitent se défendre.

Le suricate et le chien…

…nous montrent bien qu'on peut être très concentré et vigilant, mais ne rien comprendre quand même. Le suricate, dressé sur ses pattes arrière, survole du regard toute l'étendue de la savane par petits mouvements furtifs et saccadés, avant de s'effondrer, épuisé. Le chien aboie de frustration, ayant cru à tort qu'on lui avait lancé un bâton pour jouer. Il faut nettement plus d'évidences pour une surveillance effective.

Il y en a toujours un qui veille pendant que les autres dorment : il s'agit probablement d'un impératif de survie venu du fond des âges, et donc d'un aspect positif de la surveillance, promesse de sécurité. Celui qui veille le fait pour ceux qui dorment, il veille donc sur eux à proprement parler. Surveiller, c'est ici protéger. Il doit être capable d'identifier les dangers, et d'agir quand le danger se fait menace ; et avant tout : il doit réveiller les dormeurs. A cette image de veille – on pourrait dire bienveillante – on associe le bon vieux vigile, le garde de nuit qui fait sa ronde, comme dans un tableau du 19e siècle.

Le terme « surveillance » contient la notion de veille, d'éveillé. Dans « sur », on pourrait entendre l'excès, le trop-plein, le dépassement des limites comme dans le mot « surcharger » ou « surinterpréter », mais en l'occurrence il est plutôt le marqueur de la maîtrise et de la large échelle, comme dans les mots « survoler » ou « surpasser ». Notons que la tentation de l'excès est toujours possible quand on survole ou que surpasser peut facilement conduire à outrepasser. Aussi peut-on légitimement se demander, en matière de surveillance, s'il y a suffisamment de « terres rares » pour se permettre de collecter des données encore pendant des décennies comme nous le faisons aujourd'hui à large échelle. En soi, la collecte ne relève pas de la surveillance, elle n'en est qu'un des outils. La surveillance débute quand on veut savoir quelque chose de bien précis sur quelqu'un d'autre, par ex. à l'aide des données collectées. L'objectif (et le pouvoir !) consiste à sanctionner cette personne d'une manière ou d'une autre lorsqu'on a trouvé ce qu'on recherchait.

Voilà bien le problème : s'il s'agit de démanteler un réseau de narcotrafiquants, tant mieux si les enquêteurs disposent des meilleurs moyens techniques et des médiateurs linguistiques (voir p. 13) les plus affûtés, afin de faire toute la lumière, d'arrêter les trafiquants et de les juger. Par contre, lorsque des régimes totalitaires se servent des données pour en faire une pieuvre tentaculaire qui piste, arrête et torture ses opposants et tous ceux qui pensent autrement, on souhaiterait peut-être que cette technique n'ait pas atteint un si haut degré de perfection. Jusqu'à présent, chaque avancée technologique peut être utilisée à bon escient (comme une mesure de bienveillance) ou donner lieu à des abus (cela devient de la malveillance).

Un autre aspect mérite d'être mentionné, celui de la *connaissance* d'être surveillées qu'ont, ou non, les personnes surveillées. Sur la route, par exemple, radars et détecteurs de radar se livrent depuis des années à une compétition acharnée. De même, les personnes surveillées qui se savent surveillées pourraient développer des stratégies pour mettre les surveillants sur une fausse piste ou les attirer dans un piège. Les séries policières « Sur écoute » *(The Wire)* ou « Narcos » nous ont familiarisés avec les stratagèmes spectaculaires mis en place pour se livrer au trafic de stupéfiants. Dans un autre registre, en RDA, les artistes critiques envers le régime savaient que la censure les lisait ; leur stratagème à eux s'appelait les « éléphants roses », c'est-à-dire des contenus si ostensiblement critiques envers le régime qu'ils étaient assurés de passer à la trappe, immédiatement suivis de critiques bien plus subtiles qui échappaient alors à l'œil de la censure.

Les détenteurs d'une carte Cumulus de la Migros ou d'une Supercard de la Coop n'ont pas encore besoin de craindre que la police soit soudainement sur le pas de leur porte à cause de leurs dernières emplettes. Ils feraient néanmoins bien d'avoir à l'esprit que toutes leurs opérations d'achat sont consignées pour une durée indéterminée. Ainsi, le consommateur qui aurait toujours jeté son dévolu sur des produits « M-Budget » et « Prix Garantie » pourrait passer pour un avare ou un indigent, et ça pourrait devenir un problème si la Suisse décidait un jour de mener des actions ciblées contre l'avarice (une caractéristique des riches, au demeurant) ou contre la pauvreté qui sévit dans sa population. Mais nous pouvons dormir sur nos deux oreilles, ce n'est pas pour demain.

Volker Wienecke
Contact : redaktion@skppsc.ch

TOUTE L'ACTUALITÉ PSC

Courage civique – nouveau lancement

En 2019, la PSC a lancé sa campagne de sensibilisation «Courage civique – sur la bonne voie». Dans de courtes séquences vidéo, différents membres des corps de toute la Suisse expliquent comment faire preuve de courage civique, et quand il est nécessaire d'intervenir ou pas. Ce sujet n'ayant rien perdu de son actualité, la PSC a décidé de le relancer. De début juin à fin 2021, l'accent sera donc mis chaque semaine sur l'une des vidéos de notre répertoire thématique. Seront publiés aussi dans les médias sociaux des sondages sur les différentes attitudes que l'on peut adopter selon les situations. Le lancement est accompagné d'illustrations en noir et blanc, composées spécialement pour l'occasion, et conçues de façon à être aisément identifiables.

ÇA RIME AVEC CRIME

A VENDRE :

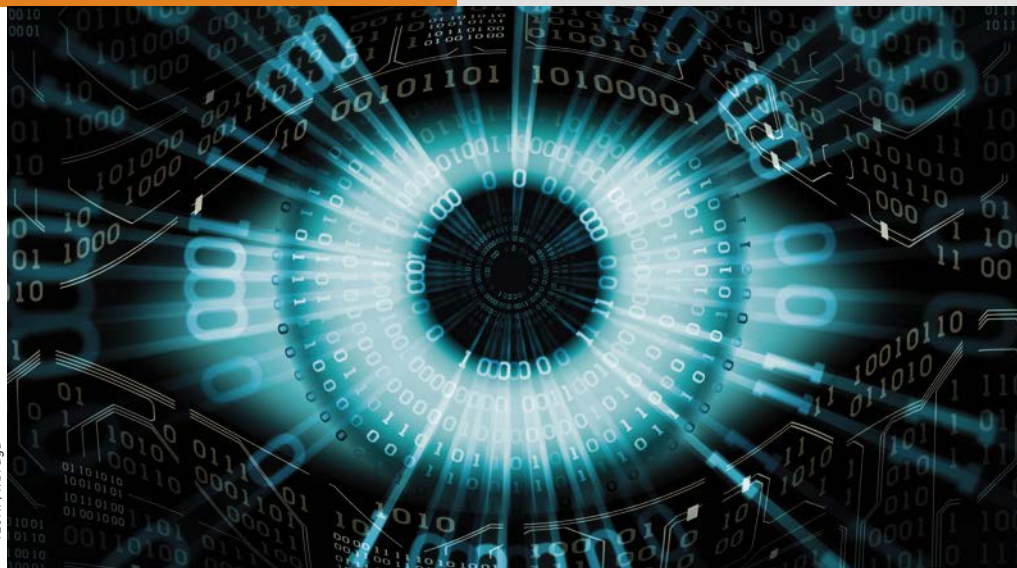
3 caméras
de surveillance,
modèles anciens,
mais en parfait état

Dessin : Agnes Weber

SKPPSC

Prévention Suisse de la Criminalité
Maison des cantons
Speichergasse 6
Case postale
CH-3001 Berne

www.skppsc.ch



123RF/wbraga