



Le Temps
1211 Genève 2
022/ 888 58 58
www.letemps.ch

Genre de média: Médias imprimés
Type de média: Presse journ./hebd.
Tirage: 37'021
Parution: 6x/semaine

N° de thème: 844.003
N° d'abonnement: 844003
Page: 13
Surface: 76'362 mm²

La sécurité passe-t-elle avant la vie privée?

L'actualité de la lutte antiterroriste fait ressurgir ce dilemme de la démocratie: nos données personnelles sont-elles intouchables, ou faut-il se résoudre à les abandonner à l'intrusion policière au nom de la sécurité? Un parlementaire et un professeur débattent

La sécurité est aussi un droit

OUI Les circuits, les pratiques, les organisations criminelles ou terroristes évoluent sans cesse. La nouvelle loi permet aux services de renseignement de remplir leur mission à l'ère du numérique et de la communication sans fil. Ces actions sont encadrées et contrôlées strictement. Elles s'appliquent, de surcroît, à des cas bien précis.

La Déclaration universelle des droits de l'homme recense des droits «civils et politiques», qui visent à empêcher l'arbitraire des gouvernants et des Etats.

Depuis, on n'a cessé d'élaborer et de reconnaître de nouveaux droits: socio-économiques, environnementaux, au développement dans les années 1960. Depuis les années 1990, on assiste à la remise en cause de ces générations de droits par le relativisme culturel d'une part, ainsi que par le développement de droits dits «communautaires» qui, en s'opposant aux choix individuels, risquent d'affaiblir, voire de contredire les premiers.

Parmi tous ces droits, on pourrait s'étonner de ne pas trouver, explicitement, de droit à la sécurité. C'est que tous les droits et libertés dont il est question ne sauraient s'exercer que dans un Etat de droit. Car c'est l'Etat qui règle la vie en commun et est responsable de la sécurité de ses habitants.

La sécurité est une exigence fon-

damentale: un socle sans lequel l'échafaudage des droits n'est guère concevable. La Constitution rappelle les droits et les devoirs de chaque individu et établit les règles de la communauté. L'Etat est donc responsable d'assurer aussi bien la sécurité de l'ensemble que celle des individus, tout en étant garant des droits de ces derniers.

Le même corpus des droits de l'homme prévoit cependant que les libertés individuelles peuvent être limitées: là où ces libertés restreindraient ou blesseraient celles des autres; lorsque des situations ou un danger imminent nécessitent d'agir; enfin dans l'intérêt supérieur de l'Etat – à l'instar d'une catastrophe naturelle ou d'un conflit armé. La vulnérabilité de nos sociétés modernes et l'augmentation des risques justifient une réévaluation des droits et des devoirs, à la manière des contrôles de sécurité dans les aéroports ou les stades. De plus, on ne saurait imaginer que la liberté individuelle ou la sphère privée soient utilisées afin de masquer des actions délictueuses ou criminelles.

L'action du renseignement est préventive. En orientant l'action des forces de l'ordre, on peut faire en sorte qu'elles soient engagées de manière efficiente. On ne peut en effet garder en permanence toutes les infrastructures critiques et les places ou bâtiments publics du pays.

Evidemment, chacun aimerait

pouvoir prévenir la criminalité, le terrorisme ou encore l'espionnage. Dans la pratique, cependant, le renseignement est souvent utilisé de manière réactive: afin d'expliquer une situation, de déceler des actions hostiles, d'aider à la prise de décision politique, enfin d'éviter la répétition d'un phénomène. La majorité des actions dans le domaine du renseignement, aujourd'hui, concerne la criminalité transfrontalière et une de ses composantes, le terrorisme.

L'affaire dite «des fiches» en 1989 a décapité nos services de renseignement et a ramené leur action à l'ère préindustrielle. Les dernières lois ont réorganisé les structures et les collaborations des différents services. Il faut maintenant que ceux-ci soient en mesure d'utiliser les outils de notre temps: courrier électronique, transmissions sans fil notamment.

Au moment où la Suisse, un des pays les plus numérisés du monde, compte des millions d'utilisateurs de services et d'applications permettant la géolocalisation, le stockage à distance, l'enregistrement des présences ou des achats, voire la revente de données à des fins commerciales, il est difficile d'imaginer que les utilisateurs-citoyens n'acceptent pas des règles et des conditions similaires, afin de contribuer à leur propre sécurité et à celle de leurs proches. ■

FACE-À-FACE

Date: 28.11.2015

LE TEMPS

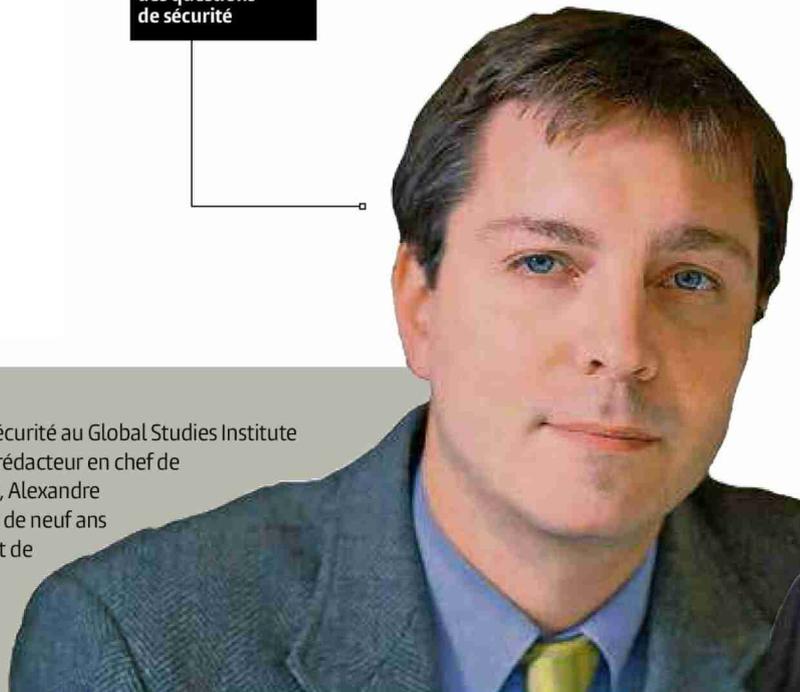


Le Temps
1211 Genève 2
022/ 888 58 58
www.letemps.ch

Genre de média: Médias imprimés
Type de média: Presse journ./hebd.
Tirage: 37'021
Parution: 6x/semaine

N° de thème: 844.003
N° d'abonnement: 844003
Page: 13
Surface: 76'362 mm²

**ALEXANDRE
VAUTRAVERS**
Spécialiste
des questions
de sécurité



PARCOURS

Spécialiste des questions de sécurité au Global Studies Institute (GSI, Université de Genève) et rédacteur en chef de la *Revue militaire suisse* (RMS), Alexandre Vautravers a été pendant plus de neuf ans professeur associé d'histoire et de relations internationales à l'université américaine de Genève.



Le Temps
1211 Genève 2
022/ 888 58 58
www.letemps.ch

Genre de média: Médias imprimés
Type de média: Presse journ./hebd.
Tirage: 37'021
Parution: 6x/semaine

N° de thème: 844.003
N° d'abonnement: 844003
Page: 13
Surface: 76'362 mm²

On a tort d'opposer l'un et l'autre

NON Non, la sécurité publique ne passe pas avant la vie privée. La sécurité publique passe par la vie privée. Et réciproquement. Sécurité et vie privée sont les deux faces d'une même pièce: la liberté. Sécurité, vie privée, liberté... Au lieu de les associer, ces jours, le monde politique oppose ces valeurs complémentaires et indissociables. Faire primer l'une sur l'autre est un non-sens, résolument contre-productif. Une fois de plus, le débat politique est dépassé par la révolution numérique en cours et la société du BigData. Les données que nous émettons massivement, toutes ces traces que laisse notre vie numérique, de notre dossier médical à nos derniers achats en passant par nos passions ou notre rythme cardiaque, sont des informations intimes, vitales ou potentiellement dangereuses. Il est impératif que cette société numérique repose sur une base de confiance des citoyens: nos données doivent être a priori inviolables. Sans quoi le système s'effondre.

Or, cette confiance n'existe pas aujourd'hui. Il faut la mettre en place. La révision de la loi sur la protection des données doit aller dans ce sens. Elle doit renforcer notre sphère privée et consolider notre confiance dans ce nouveau monde, en commençant par admettre que nos données nous

appartiennent. Qu'il s'agisse de mes communications, de mon code génétique ou de mes prochaines vacances. Or, ce n'est pas le cas aujourd'hui. Mes données appartiennent à l'Etat, à Google, à tout le monde, en fait, mais... pas à moi. Cela doit changer. Nous devons redéfinir notre relation aux données. Plus qu'un simple toilettage de la loi, il faut un «new deal» sur les données. De nouvelles bases.

En parallèle, nous devons aussi assurer la sécurité des citoyens. En détectant par exemple les données suspectes. Nos entreprises sont quotidiennement attaquées par des cyberterroristes ou des cybermafieux. Les attentats de Paris se préparent – et se repèrent – numériquement. Les organisations terroristes recrutent et communiquent numériquement. Notre défense est donc forcément numérique, elle aussi. Notre sécurité passe ainsi par un traitement spécifique de ce que nous appelons nos «données», celles de nos voisins, ou celles de terroristes. La criminalité informatique croît à un rythme proportionnel à la numérisation de la société.

Nos données doivent être inviolables, disais-je plus haut. Ajoutons: «tant qu'on respecte la loi». Comme dans le monde non numérique. L'Etat et nos services de renseignement doivent disposer de moyens efficaces contre la criminalité. Le respect de ma sphère privée passe par une sécurisation de l'univers numérique. Les révisions législatives en cours vont

dans le bon sens, sans aller trop loin. Comme l'admet le suppléant du préposé à la protection des données, Jean-Philippe Walter, dans *Le Temps* du 24 août, «la loi sur le renseignement et la loi sur la surveillance de la correspondance par poste et télécommunication contiennent un certain nombre de garde-fous qui garantissent la protection des individus. Ces lois ne sont pas des blancs-seings donnés aux autorités de poursuite. Il y a tout un arsenal de contrôle politique et juridique mis en place en amont et en aval.» Dont acte.

Nous vivons une révolution numérique. De nouvelles libertés, de nouveaux espoirs, et de nouvelles menaces. Nous devons ainsi renforcer à la fois la protection des données et la lutte contre la cybercriminalité. Les deux ne sont pas incompatibles. Au contraire: elles sont complémentaires. Cette approche globale est indispensable pour apporter de vraies réponses aux défis du monde numérique dans lequel nous entrons. Malheureusement, le débat politique piétine, englué dans les dogmes, entre les «sécuritaires» et les «libertaires». Il faut dépasser ces oppositions stériles, et mettre en place un «new deal» pour les données. Dans un contexte vieux comme le monde: notre exigence de liberté et de sécurité. Ce n'est pas l'une ou l'autre, ni l'une contre l'autre. Mais les deux, ensemble. Les trois, même: liberté, vie privée, sécurité. ■

Date: 28.11.2015

LE TEMPS



Le Temps
1211 Genève 2
022/ 888 58 58
www.letemps.ch

Genre de média: Médias imprimés
Type de média: Presse journ./hebd.
Tirage: 37'021
Parution: 6x/semaine

N° de thème: 844.003
N° d'abonnement: 844003
Page: 13
Surface: 76'362 mm²



FATHI DERDER
Conseiller national
(PLR/VD)

PARCOURS

Fathi Derder est conseiller national (PLR), journaliste, chroniqueur au *Temps*. Spécialisé dans la formation, la recherche et l'innovation, il a publié *Le prochain Google sera suisse* aux Editions Slatkine, en septembre 2015.