unine
Numéro 45

CONTRÔLE
de l'espace public

CONFIDENTIALITÉ
des données

SURVEILLANCE
au travail

Sécurité à l'ère des drones

UNIVERSITÉ DE NEUCHÂTEL

Les enjeux du *Big Data*

Traces numériques sur internet, caméras de surveillance dans les rues, drones dans le ciel : que devient la sphère privée à l'heure des grandes masses de données ou *Big Data* ? Comment la société perçoit-elle l'intrusion des technologies numériques dans notre quotidien ? Comment protéger ses données personnelles tout en profitant des avantages que nous offrent des outils informatiques sans cesse plus performants ? Telles sont quelques-unes des thématiques abordées à l'Université de Neuchâtel à travers de fructueuses recherches que nous vous invitons à découvrir dans ce numéro d'UniNEws.

Le professeur Francisco Klauser et ses collègues de la chaire de géographie politique étudient l'impact des technologies numériques sur la population, un domaine encore peu exploré par le biais des sciences sociales. « Avec ces technologies, notre quotidien – nos villes, nos systèmes de mobilité par exemple – se redéfinit, avec des conséquences en matière de sphère privée et de tri social, indique Francisco Klauser. Les données accumulées, combinées avec des algorithmes informatiques, permettent de cibler de manière de plus en plus automatisée des individus ou des groupes, pour les privilégier ou au contraire les exclure. Ce qui amène donc à d'importantes questions de pouvoir. »

De *Big Brother* aux *Little Sisters*

La réflexion des géographes de l'Université de Neuchâtel a donné naissance à un projet sur l'acceptation des drones par la population que finance le Fonds national suisse de la recherche scientifique (FNS). On estime à 22'000 le nombre de ces engins en Suisse, dont au moins 20'000 sont réservés à des usages privés, récréatifs ou commerciaux. « Il y a effectivement une immense généralisation de ces appareils, constate Francisco Klauser. On est typiquement dans un cas de technologie non centralisée. Soit le contraire d'une situation façon 'Big Brother', celle d'un Etat totalitaire tout puissant qui surveillerait toute sa population. Nous sommes plutôt face à des 'Little Sisters' : chacun peut s'approprier cette technologie. » Mais qu'en est-il vraiment ? C'est la question que se posent les chercheurs emmenés par Francisco Klauser.

On ne peut évidemment pas parler de technologie numérique sans évoquer l'informatique. Au Centre de compétences « Systèmes complexes et Big Data », on étudie les *clouds*, ces nuages virtuels permettant d'accéder via internet à des informations personnelles depuis n'importe quel point du globe. Comment techniquement concilier accessibilité et confidentialité d'informations qui touchent à la sphère privée ? Tel est le principal défi du groupe de Pascal Felber, professeur à l'Institut d'informatique. Deux projets européens auxquels participent des équipes neuchâteloises visent à rendre les systèmes de *clouds* les plus sûrs possibles, tant pour le transfert que pour le stockage de données.

Vient alors naturellement la question des limites de ce qui est permis ou non de faire avec des données personnelles, souvent sensibles car révélant notre personnalité intime, en matière de vie sociale, de religion ou de santé par exemple. Le professeur de droit Jean-Philippe Dunand livre quelques commentaires sur les limites de la surveillance des employés en milieu professionnel, à la veille d'une journée qu'il organise sur la protection des données en droit du travail. En marge de ce même événement, la professeure Anne-Sylvie Dupont, spécialiste en droit de la sécurité sociale, s'exprime sur la gestion des données personnelles par les compagnies d'assurance et les méthodes parfois intrusives dont elles font preuve à l'égard des assurés.

La protection des données se retrouve aussi dans une des facettes du travail de Gilles Labarthe, journaliste et ethnologue. Il évoque les difficultés croissantes des journalistes d'investigation face à la multiplication des vecteurs d'information sur internet et au pouvoir grandissant du secteur des relations publiques sur les médias. Un monde où il devient difficile de garantir la protection des sources d'information, argument au centre même de la déontologie journalistique.

Un regard aérien masculin

Désormais accessibles à tous les porte-monnaie, les drones posent la question de la démocratisation du ciel. Or un biais très clair apparaît dans l'enquête de l'Université de Neuchâtel. Les drones sont utilisés par une catégorie de population assez restreinte, à savoir des jeunes hommes friands de nouvelles technologies. « Le regard porté depuis le haut reste toujours masculin, à l'image des rois de naguère qui observaient l'ennemi en approche depuis la tour d'un château, ou des cartographes du prince », illustre Francisco Klauser. La société dans son ensemble est donc loin de s'approprier ce nouvel espace dans lequel les femmes demeurent les grandes absentes.

Une recherche sur trois ans

L'enquête par questionnaire s'inscrit dans un programme de recherche plus vaste sur les drones civils lié à la chaire de géographie politique dirigée par Francisco Klauser. Le projet *Power and Space in the Drone Age* bénéficie d'un financement du FNS de plus 440'000 francs sur trois ans. Il se terminera fin février 2019. Outre Francisco Klauser et Silvana Pedrozo, le postdoctorant Dennis Pauschinger a rejoint ce programme en mars 2017. Deux mémoires de master sont en outre actuellement réalisés en lien avec le projet FNS : l'un par Léa Stuber en géographie et l'autre par Raphaële Rasina en ethnologie.

Francisco Klauser,
professeur à la chaire de géographie politique

Ce qu'en pensent les gens

La population voit d'un bien meilleur œil l'usage des drones par la police ou l'armée que leur utilisation à des fins commerciales ou récréatives. C'est l'un des résultats du sondage réalisé par le professeur Francisco Klauser, la doctorante Silvana Pedrozo et une classe d'étudiants en master de l'Institut de géographie à Neuchâtel. L'enquête portait sur la perception des drones par la population vue sous l'angle des sciences sociales, une première du genre.

« C'est la première fois en Europe qu'une enquête s'intéresse à l'acceptabilité sociale des drones civils et militaires », souligne Francisco Klauser. Elle se base sur un questionnaire envoyé à 3000 personnes du canton de Neuchâtel, et auquel 600 d'entre elles ont répondu. En voici les premiers résultats.

« L'utilisation de ces engins à des fins commerciales, comme les livraisons, reste très mal perçue : elle dérange près de deux personnes sur trois, poursuit le chercheur. En d'autres termes, les gens ne sont pas prêts à ce que cette nouvelle portion d'espace aérien soit utilisée pour faire de l'argent. » Et cela, même si 57% des gens interrogés considèrent que ce marché est appelé à se développer. La même proportion craint les accidents liés à ces engins, tandis que 72% des avis récoltés approuveraient leur interdiction à toute observation des espaces publics.

L'enquête montre que la plupart des gens ignorent souvent ce qu'il est permis ou interdit de faire avec un drone, tout comme les règles à adopter pour filmer un rassemblement de personnes. Même si, aux yeux des chercheurs, les dispositions légales sont suffisamment claires aujourd'hui, le problème se situe dans l'application de la loi. Par quelles mesures concrètes, applicables peut-on faire respecter la législation ? La question reste ouverte.

Quant à l'idée de s'acheter un drone de loisirs, elle est balayée par plus de 81% des personnes interrogées, qui n'envisagent pas du tout cette éventualité. C'est dire le peu d'intérêt que suscitent réellement ces engins. On peut même parler de sérieuse méfiance, puisqu'une personne sur trois désire carrément les interdire, tandis que 68% des personnes interrogées ont peur de les voir impliqués dans des actes terroristes. Enfin, plus de la moitié des avis recueillis redoute les accidents qu'ils pourraient provoquer.

Caméras mobiles

Cette inquiétude s'explique par le fait que 87% des gens interrogés perçoivent les drones comme des caméras de surveillance : on ne sait jamais où et quand elles vont s'enclencher. On craint ainsi l'éventualité d'apparaître sur une image dans un lieu privé, typiquement au travers d'une fenêtre, crainte qui motiverait le rejet d'une bonne partie de la population à l'égard de l'usage récréatif ou commercial des drones.

A l'inverse, sitôt qu'ils sont contrôlés par la police ou l'armée, les drones ont meilleure presse. Car nos autorités ont la responsabilité de protéger la population et l'usage de ces engins s'inscrit dans cette optique. Les drones peuvent notamment apporter leur aide dans les affaires de cambriolages, de transport de substances illicites, de recherche de personnes, de surveillance de grands événements.

En savoir plus :
Drones, pouvoirs, espace aérien :
www.unine.ch/geographie/home/recherche/drones_pouvoir_et_espace_aerien.html

Une technologie vieille de vingt ans

Depuis 2001, les gardes-frontières suisses utilisent des systèmes de drones datant de 1995 pour des missions spécifiques autour des zones frontières du territoire. La géographe Silvana Pedrozo décrit une manière d'opérer une surveillance élargie de la frontière, avec cependant des limites qui justifient le renouvellement de leur flotte prévu pour 2019.

Doctorante à l'Institut de géographie, Silvana Pedrozo a eu l'opportunité de suivre en 2014 un engagement de drone militaire suisse le temps d'une mission longeant le Jura helvétique. Ces engins n'ont rien à voir avec les quadricoptères actuels que l'on peut soulever d'une main. Il s'agit de véritables avions sans pilote de 5,7 mètres d'envergure, pesant 270 kg et construits par le fabricant suisse RUAG.

L'utilisation des quinze ADS 95 actuellement en activité s'inscrit dans un agenda tant civil que militaire visant à mieux sécuriser les espaces frontaliers, ainsi que certaines zones à l'intérieur du territoire. Grâce à des capteurs thermiques et des caméras, les drones recueillent tout un éventail d'informations que les douaniers peuvent difficilement obtenir par d'autres moyens. Ils complètent ainsi les renseignements provenant d'autres entités impliquées dans la sécurité du territoire (police, service du feu ou hôpitaux).

C'est un outil de reconnaissance précieux : moins coûteux qu'un hélicoptère, manipulable de nuit grâce à ses caméras infrarouges, bien adapté à la sécurisation de grands événements. « Notre objectif est de mieux savoir quoi et où aller regarder. Comme ça, on connaît mieux certaines zones, parfois difficiles d'accès et on peut y envoyer des officiers de terrains ou non », relève un des gardes-frontières interrogés par la chercheuse.

Les drones permettent aux gardes-frontières de localiser et de suivre des individus, ainsi que des groupes ou des véhicules. Leurs missions ont contribué à la poursuite de cambrioleurs dans des zones résidentielles, de véhicules en fuite prêts à traverser la frontière franco-suisse, ou encore à l'arrestation de migrants dans des trains désaffectés.

Missions risquées

Reste que le système présente des limites plutôt surprenantes. Alors que la plupart des drones militaires déployés offrent une mobilité totale au-dessus de leur territoire, ce n'est pas le cas en Suisse. La surveillance de l'ensemble des régions montagneuses est peu pratiquée, car elle demeure plus risquée pour ces appareils dont les possibilités de voler en altitude et l'autonomie restent faibles (maximum 4 heures).

De plus, chaque engagement de drone nécessite la mobilisation de quinze à vingt personnes. Autre problème : le bruit de l'engin qui rend la discrétion de l'intervention toute relative. Enfin, l'ADS 95 voit ses performances affectées par la pluie ou le brouillard, ce qui oblige les pilotes à modifier les trajectoires initialement prévues, voire à devoir clouer le drone au sol en automne et en hiver.

Tous ces points faibles ont mené les autorités fédérales à commander six nouveaux drones militaires. Ceux-ci pourront être engagés par tous les temps et disposer d'une meilleure autonomie dans les airs, avec des nuisances sonores réduites et des engagements ne nécessitant plus d'escorte aérienne.

Dans un sondage réalisé par l'Université de Neuchâtel sur l'acceptation des drones par la population, commander de nouveaux drones militaires est approuvé par la moitié des répondants. Mais le fait qu'ils puissent être armés pose problème pour 60% des personnes interrogées, tout comme la décision de les acheter à Israël. Ce dernier point recueille 44% d'avis critiques, contre 28% qui n'y voient aucun inconvénient.

Silvana Pedrozo,
doctorante à l'Institut de géographie

Confidentialité garantie

Les interlocuteurs de Silvana Pedrozo se veulent rassurants quant à la protection des données récoltées. Premièrement, l'utilisation des drones militaires suisses reste ponctuelle et ne permet pas d'écoute à distance. Les données sont conservées par les Forces aériennes pendant 30 jours, puis sont supprimées à l'échéance à moins qu'elles puissent avoir une utilité a posteriori. Les capteurs actuels révèlent des formes et des silhouettes, sans possibilité de reconnaissance faciale. Finalement, l'armée est soumise à des ordonnances sur la sécurité militaire qui règlent les potentiels abus.

Image positive

La présence des caméras a eu des conséquences positives sur l'image des Pâquis, estiment 44% des personnes interrogées, contre 15% qui pensent le contraire. De manière générale, le caractère récréatif du quartier et sa vie nocturne – y compris la prostitution – ne sont pas considérés comme des générateurs de nuisances.

Ce sont les magasins ouverts 24h/24 (les « dépanneurs ») qui recueillent plus d'avis défavorables. Ces commerces vendent de l'alcool à toute heure et pratiquent des prix plus bas que les consommations pouvant être obtenues dans les débits de boissons patentés. Une fois l'achat effectué, les clients se retrouvent en général à consommer sur l'espace public, drainant un lot de nuisances qui vont du bruit aux états d'ébriété manifestes.

Raoul Kaenzig,
chargé de recherche à l'Institut de géographie

Quartier de Genève étudié à Neuchâtel

Pour la première fois en Suisse, l'effet des caméras de surveillance sur la vie d'un quartier a fait l'objet d'une étude approfondie et de longue durée. Suite à l'installation en octobre 2014 de 29 caméras aux Pâquis, un quartier de Genève réputé pour sa vie nocturne animée, Raoul Kaenzig et Francisco Klauser ont interrogé différentes franges de la population (habitants, gendarmes, commerçants, milieu de la prostitution). Sur mandat de l'Etat de Genève, les chercheurs de l'Université de Neuchâtel ont publié les résultats de leurs enquêtes en novembre 2016, après deux ans de travaux.

« Le plus marquant dans cette étude a été l'accueil finalement positif de la population par rapport à un tel projet de surveillance », note d'emblée Raoul Kaenzig, chargé de recherche à la chaire de géographie politique. Il y avait certes des craintes au début du projet, mais elles se sont rapidement estompées, puisque 59% des répondants estiment que le dispositif ne porte pas atteinte à la sphère privée. Seuls 15% des avis recueillis souhaitent la disparition des caméras du quartier.

Le sentiment de sécurité s'est indiscutablement accru aux Pâquis, en particulier pendant la nuit, avec près d'une personne sur trois qui s'y sent plus en sécurité depuis l'installation des caméras. Et même davantage lorsqu'il s'agit des habitants de la zone pilote pour lesquels cette proportion atteint 36%.

Si le système de vidéosurveillance est bien accepté, on ne parle pas pour autant d'un véritable engouement, nuancent les chercheurs. La préférence de la population va clairement vers des mesures humaines, ou d'aménagement de la voie publique, qui passent par la police de proximité, les liens sociaux via les associations et les animations de quartiers, ou encore par un meilleur éclairage public.

Outil complémentaire

S'agissant de l'élucidation des infractions commises, les caméras ne remplacent en aucun cas le travail de la police sur le terrain, mais sont utilisées comme un outil complémentaire. Pour preuve, le recours relativement discret à l'extraction d'images. On dénombre 89 extractions d'images réalisées pour la zone pilote, représentant seulement 3,1 extractions par caméra durant les deux années de l'évaluation. On observe un léger accroissement du taux d'élucidation pendant la durée du mandat, sans qu'il soit toutefois possible de quantifier la part des caméras dans cette évolution.

Sur le plan opérationnel, l'étude met particulièrement en évidence l'importance de la formation des opérateurs qui observent les images recueillies. « Leur sens de l'observation et leur faculté d'analyse, leurs connaissances du terrain et leur capacité à collaborer avec les autres acteurs de la chaîne sécuritaire sont décisives pour l'efficacité du système. Sans cet élément humain, les caméras sont inutiles », souligne Raoul Kaenzig.

L'effet préventif reste, quant à lui, mitigé. Les statistiques policières n'indiquent pas de baisse de la criminalité. Il y a bien une légère réduction des vols et agressions répertoriés, mais les infractions qui se déroulaient dans le champ des caméras ont paradoxalement augmenté (+15%) durant la période étudiée. La présence de la vidéo n'a en général pas engendré de déplacements de la criminalité dans les rues voisines, hors du périmètre surveillé, à l'exception du trafic de stupéfiants.

« Ce trafic n'a pas disparu de la zone équipée de caméras, mais les transactions dans les rues voisines sont de plus en plus nombreuses », relève Raoul Kaenzig. Les affaires se réalisent sur un territoire plus difficile à contrôler et plus étendu qu'en 2014. On observe également une adaptation des modes de transactions au sein de la zone filmée : dans des angles hors champ, dans des véhicules, dans des cours d'immeubles ou des halls d'entrées.

En savoir plus :

Raoul Kaenzig et Francisco Klauser, *Evaluation de la 'vidéoprotection' dans le quartier des Pâquis à Genève*, synthèse à l'attention des médias, 2016
www.unine.ch/geographie/home/recherche/paquis.html

Quand le smartphone dicte où aller

Comment le logiciel *Foursquare* influence-t-il les déplacements ? Durant sa thèse de doctorat à l'Institut de géographie, Sarah Widmer s'est intéressée à cette application pour smartphone dans la ville de New-York en 2013 où elle a procédé à des analyses approfondies d'une trentaine de témoignages d'utilisateurs. La géographe a mis en exergue les avantages et inconvénients de cette aide à la navigation.

Qu'est-ce que *Foursquare* ?
Il s'agissait au départ d'un réseau social basé sur la géolocalisation qui intégrait également une dimension ludique, et qui s'est transformé en un moteur de recommandations de lieux de loisirs (bars, cafés, restaurants). C'est une aide personnalisée à la navigation en ville, en fonction de l'historique des lieux dans lesquels l'utilisateur s'est rendu, des endroits que les membres de son réseau social ont fréquentés, ou encore en fonction des emplacements visités par des utilisateurs aux pratiques similaires aux siennes. Cela se traduit par des navigations « sur mesure » mais qui favorisent une forme d'entre-soi.

Que ressentaient les utilisateurs de *Foursquare*, se sentaient-ils manipulés ?
De façon assez intéressante, plusieurs personnes n'avaient pas conscience que les résultats étaient en fait personnalisés par un algorithme. D'autres utilisateurs étaient parfaitement conscients du fonctionnement de l'application et l'utilisaient justement pour recevoir ces conseils personnalisés. Bien souvent, les recommandations n'étaient pas suivies au pied de la lettre, mais comparées avec les résultats d'autres applications (Yelp ou Google Maps), affinées en ajoutant de nouveaux critères de recherche, ou critiquées pour leur peu de pertinence. On ne peut donc pas parler de pratiques complètement déterminées par cette technologie.

Il y a bien évidemment des personnes plus *geek* que d'autres, qui ont un usage plus stratégique de l'application. Elles l'utilisent dès lors consciemment pour accéder à des contenus personnalisés et pour éviter de se voir recommander certains lieux qu'elles considèrent ne pas leur correspondre. Ceci évidemment peut nous interroger sur nos façons actuelles de vivre en commun dans les villes.

En savoir plus :
Sarah Widmer, *Smartphone et big data*, GeoAgenda 2016/4, p. 10-12

Quels sentiments suscitait l'usage des données personnelles ?
Les utilisateurs étaient conscients des risques (la plupart de mes entretiens ont eu lieu quelques mois après les révélations d'Edward Snowden), mais ils avaient tendance à considérer que divulguer leurs données personnelles était le prix à payer pour recevoir le service personnalisé offert par l'application. Globalement, on peut parler d'une banalisation de ce type de risque qui est perçu comme quelque chose de quotidien et d'inévitable.

Quelle place occupent d'après vous ces logiciels dans la gestion de nos déplacements ?
Le fait d'avoir accès à l'internet mobile de façon si immédiate sur nos smartphones a un impact certain sur la façon dont nous vivons nos mobilités. Ça peut être des choses très simples, comme cette application parisienne « Paris-ci la sortie du métro » qui permet de savoir dans quel wagon de métro monter pour être en face de la sortie de métro à sa station de destination, ou ces applications des transports publics qui nous indiquent l'arrivée du bus en temps réel. Accéder à ce type d'informations permet de mieux gérer ses activités dans son budget temps/espace. Le smartphone nous offre une grande flexibilité et nous permet de nous adapter à une réalité qui, elle-même, est fluide, en mouvements, faite de changements et d'imprévus. Le sentiment d'assurance qu'amène cette technologie (mes interlocuteurs disaient souvent qu'ils ne se sentaient jamais perdus) a un important impact sur la façon dont nous gérons et vivons notre rapport à l'espace et nos mobilités.

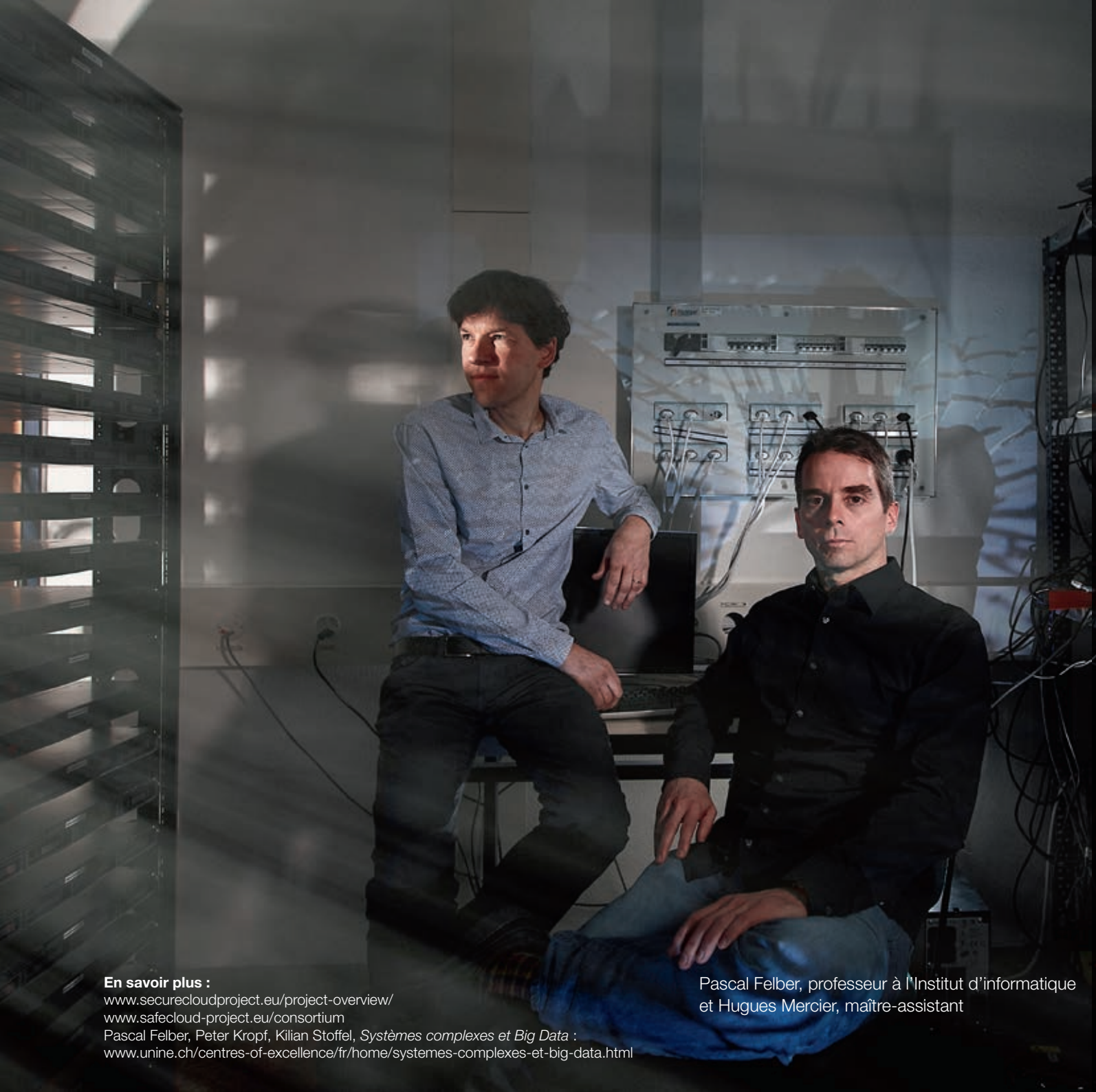
Et le revers de la médaille ?
Forcément, dans ma thèse, j'ai un regard assez critique sur ces technologies et pointe en particulier sur deux problématiques : la « dataveillance » et donc les risques encourus en termes d'atteintes à la sphère privée ; et le « tri social » automatiquement réalisé par ces algorithmes qui priorisent, différencient, classifient sans cesse leurs utilisateurs.

Sarah Widmer entreprend une thèse
de doctorat sur les usages urbains du smartphone

Collaborations internationales

SecureCloud regroupe 14 partenaires provenant d'Allemagne, d'Angleterre, du Brésil, du Danemark, d'Italie, d'Israël et de Suisse. Sa coordination locale est assurée par Marcelo Pasin, chercheur à l'Université de Neuchâtel et professeur à la HE-Arc. Les activités du projet ont démarré début 2016 pour une durée de trois ans. *SecureCloud* a permis au groupe de recherche en systèmes complexes de l'Université de Neuchâtel d'empocher une contribution de 600'000 francs.

SafeCloud comprend sept partenaires académiques et industriels dans un consortium international incluant l'Allemagne, l'Estonie, le Portugal et la Suisse. Le projet a démarré début septembre 2015. Il est financé pour une période de trois ans, avec une part d'environ un million de francs revenant à l'Université de Neuchâtel. Maître-assistant aux instituts d'informatique et de mathématiques, Hugues Mercier en assume la coordination scientifique.



Pascal Felber, professeur à l'Institut d'informatique et Hugues Mercier, maître-assistant

En savoir plus :
www.securecloudproject.eu/project-overview/
www.safecloud-project.eu/consortium
Pascal Felber, Peter Kropf, Kilian Stoffel, *Systèmes complexes et Big Data* :
www.unine.ch/centres-of-excellence/fr/home/systemes-complexes-et-big-data.html

Données privées et intérêt public

Qu'on parle de santé, de relations bancaires, ou encore de vote sur internet, le *cloud computing* est une solution avantageuse pour les entreprises. Mais comment bénéficier de ces services sans dévoiler nos informations personnelles ? Des réponses technologiques sont développées à l'Institut d'informatique de l'Université de Neuchâtel via des projets de recherche internationaux.

La généralisation des *clouds*, ces nuages informatiques virtuels, permet à n'importe qui d'accéder de manière fiable à des données 24h/24 depuis n'importe quel lieu connecté du monde. Mais comment en assurer la confidentialité ? C'est tout l'enjeu des recherches menées par l'équipe de Pascal Felber, professeur à l'Institut d'informatique de l'Université de Neuchâtel. « Nous traitons essentiellement deux aspects liés à l'utilisation des *clouds* : la sécurisation du transfert de données d'une part, et celle de leur stockage d'autre part », indique le professeur, spécialiste en systèmes complexes.

Dans le domaine médical, il est fréquent de communiquer certaines informations issues des dossiers des patients à des fins statistiques ou de surveillance d'une épidémie. Dans le même temps, on souhaite qu'il soit impossible d'identifier les dossiers médicaux dont proviennent ces informations. C'est un peu comme si on demandait à des prestataires extérieurs, auxquels on ne fait pas confiance, de lire un texte sans y avoir accès. Le défi peut sembler paradoxal, mais c'est exactement l'objectif du projet de recherche *SecureCloud*, à l'image de ce qui se passe dans une banque lorsqu'un client désire accéder à un coffre : il se fait accompagner par un employé de l'établissement qui se retire pendant que le client examine le contenu déposé.

« Le propriétaire des données, un hôpital par exemple, les conserve sur ses propres ordinateurs. Lorsqu'il doit en transférer une partie vers des partenaires externes, l'hôpital le fait via une enclave sécurisée dans le *cloud*, un blindage virtuel qui le protège de toutes les intrusions possibles venant de l'ordinateur du destinataire. Ainsi nous sommes sûrs que ces données ne seront ni lues, ni altérées, sans que le propriétaire ne soit averti, ce qui permet de préserver la confidentialité du transfert », explique Marcelo Pasin, qui assure la coordination locale du projet *SecureCloud*.

Quant au volet stockage, il repose sur une stratégie de partition des fichiers. Imaginons qu'on veuille stocker une photo dans un *cloud*. L'opération consiste à crypter puis à fragmenter la photo pour en déposer chacune des parties dans divers lieux géographiques et chez des prestataires différents (comme Dropbox, Google Drive ou Amazon).

« De cette façon, il devient impossible à l'un ou l'autre des prestataires de savoir ce que contiennent les données stockées », résume Hugues Mercier, maître-assistant à l'Université de Neuchâtel, coordinateur scientifique de *SafeCloud.*

Résultat : le fichier demeure inexploitable non seulement par les pirates informatiques, mais également par toute autorité (administrateur de réseau, agence gouvernementale) qui aurait un accès privilégié aux serveurs où est stockée cette information. Seuls les ayants droit légitimes qui ont accès à tous les fragments peuvent les grouper à nouveau et révéler ainsi tout leur sens. Ici, en l'occurrence, la photo d'origine.

Droit à l'oubli

Parallèlement à l'aspect technique de la confidentialité, le projet *SafeCloud* comporte un volet juridique qui est traité par le Pôle de propriété intellectuelle de la Faculté de droit où Yves Bauer et la professeure Nathalie Tissot s'attachent notamment à l'étude du droit à l'oubli.

Il s'agit de veiller à ce que les solutions techniques mises en place respectent cette notion fondamentale qui permet à n'importe qui, après un certain temps, d'exiger la suppression de toute trace d'actes susceptibles de nuire à sa réputation. Or, la manière dont les données sont travaillées pour les rendre confidentielles suppose de les graver en quelque sorte dans le marbre, rendant leur effacement quasiment impossible. « Il faudrait pouvoir parfois écrire certaines informations 'à la craie' pour les rendre effaçables, mais uniquement par les personnes autorisées », illustre Hugues Mercier. C'est donc sur l'équilibre à trouver entre ce qui peut être supprimé ou non que reposent ces recherches juridiques.

Gilles Labarthe,
journaliste et ethnologue

Développement exponentiel

Ces vingt dernières années, les informations disponibles sur internet ont suivi un développement exponentiel, tant par la multiplication des sources (administrations, ONG, associations, blogs, etc.) que de celles de leurs vecteurs (médias en ligne, réseaux sociaux). Les capacités de traitement et de présentation (comme la cartographie) ont aussi ouvert la voie à de nouvelles possibilités de production journalistiques, sur un mode collaboratif ou participatif.

On pense ici aux enquêtes collectives impulsées par des réseaux transnationaux de journalistes d'investigation. Elles exploitent des fuites (les fameux *leaks)* et des informations confidentielles dévoilées par des lanceurs d'alerte. Parmi les exemples les plus actuels, citons l'affaire des « Panama Papers » : des millions de données transmises au printemps 2016 par l'*International Consortium of Investigative Journalists* (ICIJ), révélant des pratiques d'évasion fiscale. Ou encore, la divulgation des « Football Leaks » : 18,6 millions de documents mettant en exergue des affaires de blanchiment d'argent, de prostitution et de réseaux mafieux dans l'industrie du football. (GL)

Investigations sous influence

Dans sa thèse de doctorat qu'il poursuit à l'Académie du journalisme et des médias de l'Université de Neuchâtel, le journaliste et ethnologue Gilles Labarthe s'intéresse aux impacts des technologies numériques (NTIC) sur les méthodes d'enquête des journalistes d'investigation en Suisse romande. Ces nouveaux outils présentent des avantages, mais aussi des problèmes : intox, cybersurveillance, risques liés aux traces digitales…

Dans les pays d'Europe occidentale, les journalistes d'investigation n'auraient jamais été aussi bien outillés et connectés pour accéder à des informations, mener des enquêtes et les publier. Des drones ont même été utilisés dans certains pays pour illustrer le patrimoine immobilier luxueux de fonctionnaires corrompus, de dirigeants contestés, pour dénoncer leur train de vie sans rapport avec leur salaire officiel, ou encore pour montrer le nombre de manifestants réellement mobilisés dans des marches de contestations.

Moins spectaculaire, la caméra cachée et celle, discrète, de nos smartphones représenteraient d'autres « outils idéaux » pour mettre en scène avec un temps de préparation très court et à peu de frais, des effets de dramaturgie, de divertissement et d'émotion, essentiels pour capter l'attention des téléspectateurs. La banalisation de leur usage est devenue très marquée dans les émissions d'investigation en France. Pour la justifier, les producteurs et journalistes invoquent la difficulté toujours plus grande à « passer la barrière des communicants », à savoir l'emprise croissante du secteur des relations publiques sur les médias.

Le « cinquième pouvoir »

Des chercheurs anglo-saxons ont d'ailleurs proposé la notion de « 5e pouvoir » pour la définir. Fonctionnaires de l'administration, politiciens, porte-paroles de lobbies… tous communiquent via internet et les réseaux sociaux, pour influencer les productions journalistiques et développer des stratégies de *gatekeeping*, imposant un contrôle de l'information.

En Suisse romande également, les journalistes rencontrés pour cette étude soulignent un net renforcement depuis les années 2000 des effets de ce « 5e pouvoir ». Une majorité estime que les NTIC comportent désormais plus de risques que d'avantages dans l'exercice de leur métier. Plus de la moitié d'entre eux ont cessé de publier des enquêtes dans les médias en Suisse romande.

Parmi les raisons invoquées : les risques de manipulation par des acteurs externes diffusant sur internet des documents falsifiés et exerçant des pressions, mais surtout la difficulté à garantir la protection des sources. En effet, comment gérer les traces digitales ? Certains recommandent le cryptage ; d'autres, un retour à « l'analogique » (stylo, prises de notes, rencontres informelles en tête-à-tête avec des informateurs…) pour limiter les risques liés à la cybersurveillance et au *hacking* de leurs outils numériques.

La réorganisation de structures professionnelles aux niveaux régional et national serait un autre moyen de répondre à l'inversion des rapports entre journalistes et communicants. Aujourd'hui, ces derniers sont jusqu'à dix à vingt fois plus nombreux que les quelque 4600 membres inscrits à la Fédération suisse des journalistes.

Il s'agirait de compenser dans une certaine mesure la disparition progressive des unités se consacrant à l'enquête, dans les principaux titres de la presse quotidienne et hebdomadaire suisse romande – à l'exception de la « cellule enquête » du *Matin Dimanche* et de *SonntagsZeitung*, créée en 2012. C'est aussi l'une des raisons du lancement depuis une dizaine d'années du « réseau suisse de journalistes d'investigation » qui permet notamment un accès à des réseaux d'enquête transnationaux. (GL)

En savoir plus :

http://www.investigativ.ch, réseau suisse des journalistes d'investigation

Les limites de la surveillance au travail

A l'heure des usages généralisés de l'informatique dans tous les milieux professionnels, que dit la loi en matière de surveillance du personnel ? Spécialiste du droit du travail, le professeur Jean-Philippe Dunand a rédigé un commentaire des dispositions légales concernant la protection des données des employés. Il a par ailleurs co-édité avec son collègue Pascal Mahon un ouvrage de 380 pages consacré à cette thématique qui vient de sortir de presse.

Si la surveillance des travailleurs par les employeurs n'est pas une problématique nouvelle, elle peut prendre des dimensions sournoises à l'ère numérique. Comme l'installation de cette caméra qui, sous couvert de veiller au bon fonctionnement d'une machine automatique, pointait en réalité vers la place de travail d'un employé situé juste à côté. Si ce cas paraît évidemment illicite, la question générale de l'interdiction ou non de surveiller des employés doit être nuancée. « D'abord parce qu'il est dans la nature même des relations de travail que l'employeur puisse exercer un certain contrôle sur l'activité de son personnel, en vérifiant si des directives ont été bien suivies », note Jean-Philippe Dunand.

C'est d'ailleurs selon cet argument qu'une surveillance de courriels ou de l'utilisation d'internet peut être envisagée, en la motivant par une volonté de contrôler la bonne exécution d'une prestation de travail, mais aussi pour s'assurer du respect de la confidentialité, de la sécurité et de la réputation de l'entreprise. L'employeur est toutefois tenu d'informer son personnel de l'existence d'une telle surveillance. Il doit également respecter certains principes inhérents au traitement des données du travailleur, comme ceux de la bonne foi et de la proportionnalité. « Mais lorsqu'une utilisation privée est autorisée ou tolérée, l'employeur ne doit pas avoir accès aux courriels privés des employés », nuance le professeur de droit.

A ceci s'ajoutent d'autres types de surveillance par des moyens électroniques couramment admis en milieu professionnel. Il en est ainsi de la vidéosurveillance d'endroits stratégiques ou sensibles d'une entreprise, qui vont des parkings à la salle des coffres, en passant par les entrées, les guichets, les étals d'un magasin. De même, dans une logique de prévention des accidents, il est possible de surveiller des lieux abritant des machines ou des produits dangereux.

Les véhicules peuvent aussi faire l'objet d'un suivi par GPS. Ceci est le cas notamment pour des agences de sécurité, des entreprises de transport routier, ou encore les taxis. « Le Tribunal fédéral a admis qu'un tel dispositif permettant de localiser en tout temps la position de chacun des véhicules en service, afin de surveiller l'emploi du temps des employés, ainsi que pour des motifs de sécurité et d'efficacité, pouvait être justifié à certaines conditions », indique Jean-Philippe Dunand.

Plus précisément, l'installation d'un système de géolocalisation est autorisée si l'employeur démontre que les employés ne sont pas surveillés en temps réel, c'est-à-dire que le contrôle n'a lieu qu'a posteriori, après la fin de la journée de travail. En effet, selon le Tribunal fédéral, « la possibilité de suivre en temps réel le trajet des véhicules durant la journée comporte le risque que l'employeur demande de manière répétée et inopinément à ses collaborateurs leur position ou le choix de leur itinéraire, perturbation qui viendrait alors s'ajouter au stress provoqué par le sentiment d'être constamment surveillé ».

En revanche, le Tribunal fédéral considère que l'installation d'un logiciel espion *(spyware)* dans l'ordinateur d'un employé est en principe illégale. Car il s'agit d'une mesure trop intrusive et disproportionnée, contraire autant aux règles de protection des travailleurs qu'aux dispositions légales en matière de protection des données.

droit

En savoir plus :

Jean-Philippe Dunand et Pascal Mahon (éds), *La protection des données dans les relations de travail*, Genève/Zurich/Bâle, éditions Schulthess, 2017

Personnalité à protéger

Tout individu a droit à la protection de sa personnalité. Cette notion comprend l'intégrité physique, la santé physique et psychique, l'intégrité morale et la considération sociale, les libertés individuelles, ainsi que la sphère privée. Quant aux données personnelles, elles concernent toutes les informations susceptibles de rendre une personne identifiable. « Même à partir d'un numéro AVS, il est envisageable d'identifier une personne au sein d'une entreprise », illustre Jean-Philippe Dunand. Dans les relations de travail, les données personnelles comprennent toutes les indications concernant la personne du travailleur, et qui portent tant sur sa vie privée que professionnelle. La loi distingue encore, au sein des données personnelles, les données sensibles qui regroupent « les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, des poursuites ou sanctions pénales et administratives. »

Jean-Philippe Dunand,
professeur en droit du travail

Anne-Sylvie Dupont,
professeure en droit de la sécurité sociale

Des assurés pris en otage

Dans le secteur de la santé, les assurances imposent en général de lever le secret médical sur les dossiers des assurés. En cas de refus, il n'est pas possible de toucher de prestations. Titulaire de la chaire de droit de la sécurité sociale à Neuchâtel, la professeure Anne-Sylvie Dupont relève le déséquilibre existant entre les assureurs qui détiennent les cordons de la bourse et les assurés à qui on impose des règles excessivement intrusives.

La gestion des données des patients ou des demandeurs de prestations sociales est un secteur délicat des assurances privées et sociales. En théorie, le cadre juridique impose aux assureurs de ne demander que les données pertinentes permettant de se prononcer sur le droit aux prestations d'un assuré. « En pratique, l'assureur demande en règle générale à l'assuré de délier les médecins du secret médical à son égard, afin qu'il puisse se renseigner directement auprès d'eux », indique Anne-Sylvie Dupont.

L'inconvénient majeur de cette situation est qu'on donne pour ainsi dire carte blanche à l'assureur qui, bien souvent, fait signer aux assurés des procurations libellées en des termes très généraux. « Sont ainsi non seulement déliés du secret médical les médecins, hôpitaux et autres professionnels de la santé qui connaissent le cas, mais aussi les autres assureurs privés, les assureurs sociaux, les services sociaux, l'employeur, etc. »

Cette situation fait que des informations sur un demandeur de prestation circulent beaucoup trop et pas toujours à bon escient. C'est flagrant dans les groupes qui exploitent plusieurs formes d'assurances, sociales et privées, où les données sensibles font régulièrement des allers-retours.

Parfois, cela peut se retourner contre l'assureur. C'était le cas dans une affaire où la compagnie voulait invalider un contrat qui relevait d'une assurance privée au motif que l'assuré avait omis de mentionner certains faits au moment de conclure le contrat. Le Tribunal fédéral lui a donné tort, jugeant que la compagnie devait nécessairement avoir connaissance de ce fait puisqu'elle était aussi l'assureur-maladie obligatoire (LAMal) de l'assuré.

« Dans d'autres branches d'assurances, par exemple l'assurance-invalidité et l'assurance-accident, le fait que les données sensibles soient archivées dans un dossier 'global' de l'assuré, auquel presque tout le monde peut avoir accès, est un problème », note encore Anne-Sylvie Dupont. Pour leur défense, les compagnies avancent la volonté de mieux lutter contre les abus, en se fondant sur une pesée des intérêts. Ainsi, tout faire pour ne pas verser des sommes indues doit systématiquement l'emporter sur l'intérêt de l'assuré à conserver pour lui seul certains pans privés de son existence.

Dans ce contexte, il paraît très difficile de contraindre les compagnies d'assurances de réserver l'accès aux données d'un patient aux seules personnes impliquées dans l'attribution ou non de prestations. Seule exception : l'assurance obligatoire des soins qui travaille avec un médecin-conseil. Son rôle est de filtrer les données sensibles, afin de ne fournir à l'assureur que les renseignements dont il a besoin pour statuer sa décision d'octroyer ou non des prestations. « Actuellement, ce système ne marche pas complètement, estime Anne-Sylvie Dupont, car il n'est pas toujours étanche. Mais au moins il a le mérite d'exister, contrairement à ce qui se passe dans les autres assurances sociales, comme l'AI. »

« Pour mieux défendre le secret médical des assurés, il faudrait une démarche politique, recommande encore la professeure de droit. Ou en tout cas militante, par le biais de signalements au Préposé fédéral à la protection des données. Les pratiques des assureurs sont régulièrement épinglées dans ses rapports. »

santé

En savoir plus :

Anne-Sylvie Dupont, « La protection des données confiées aux assureurs », in Jean-Philippe Dunand et Pascal Mahon (éds),
La protection des données dans les relations de travail, Genève/Zurich/Bâle, éditions Schulthess, 2017

Café scientifique – tous publics

Les drones : amis ou ennemis ?

Mercredi 22 mars 2017 de 18h à 19h30
A la cafétéria du bâtiment principal de l'Université
Av. du 1er-Mars 26, Neuchâtel

En Suisse, on estime à 22'000 le nombre de drones civils susceptibles de voler au-dessus de nos têtes. Quels sont les chances et les risques liés à l'utilisation des drones civils en Suisse ? Quels sont les enjeux en termes de sécurité et de surveillance ? Qu'en pense la population suisse ?
Entrée libre
www.unine.ch/cafescientifique/

Colloque spécialisé

La protection des données en droit du travail

Vendredi 17 mars 2017 dès 8h15
Aula des Jeunes-Rives, Neuchâtel

La protection des données dans les relations de travail est un thème auquel les employés et les employeurs sont de plus en plus sensibles, entraînant des consultations de juristes et d'avocats. Ce colloque en rappelle les principes, les actions en justice, et le traitement des cas d'application les plus importants. Il présente aussi les principaux axes du projet de révision du Conseil fédéral en la matière.
www.unine.ch/cert/

Filières de l'UniNE en rapport avec le *Big Data* :

Master en sciences sociales, spécialisation en géographie humaine

Master en informatique

www.unine.ch/formation

UniNEws est un dossier de l'Université de Neuchâtel. Av. du 1er-Mars 26, 2000 Neuchâtel. Tél. 032 718 10 40, bureau.presse@unine.ch, www.unine.ch.
Impressum : Bureau presse et promotion de l'Université de Neuchâtel. Rédaction : Igor Chlebny ; sauf p. 14-15 : Gilles Labarthe
Photos : Guillaume Perret ; sauf p. 1 & 2 : Bernard Léchot et p. 11 : Anna Montemayor
Layout : Leitmotiv ; Impression sur papier recyclé FSC : IJC
Parution : mars 2017. Paraît au moins quatre fois par an.