unine
Number 45

public space
MONITORING

data
CONFIDENTIALITY

workplace
SURVEILLANCE

Security in the Drone Age

UNIVERSITÉ DE NEUCHÂTEL

Big Data Issues

Digital traces on the Internet, CCTV cameras in the streets, drones in the sky: what is becoming of our privacy in the era of Big Data? How does society perceive the intrusion of digital technologies in our everyday lives? How can we protect our personal data and still benefit from IT tools with ever higher performance? These are some of the topics addressed by revealing research conducted at the University of Neuchâtel, which we invite you to discover in this UniNEws issue.

Professor Francisco Klauser and his colleagues from the Chair of Political Geography are investigating the impact of digital technologies on the public, a topic still little explored in social sciences. “These technologies redefine aspects of our everyday lives, such as our cities and transportation systems, with consequences in terms of privacy and social sorting”, says Francisco Klauser. The data accumulated, combined with computer algorithms, makes it possible to target individuals or groups in an increasingly automated way, to favour them, or on the other hand exclude them. This in turn gives rise to important issues of power.

From *Big Brother* to *Little Sisters*

The reflections of the geographers of the University of Neuchâtel gave birth to a research project funded by the Swiss National Science Foundation (SNSF) on public acceptance of drones. It is estimated that there are 22,000 such aircrafts in Switzerland, 20,000 of which for private, leisure or commercial use. “These vehicles are indeed becoming exceedingly widespread,” notes Francisco Klauser. “This is a typical case of non-centralised technology, that is to say the contrary of a ‘Big Brother’ situation where a totalitarian State would watch the whole population. We are rather facing ‘Little Sisters’, as anyone can make the technology their own.” But how do things really stand? This is the question explored by the research team led by Francisco Klauser.

Of course, we can hardly speak about digital technology without mentioning computer science. The Complex Systems and Big Data Competence Centre investigates ‘clouds’, i.e. virtual server networks that let you access your data from any point on the globe via the Internet. What can be done to reconcile data accessibility with private information confidentiality? This is the main challenge facing Pascal Felber, professor at the Computer Science Department, and his group. Teams from the University of Neuchâtel are taking part in two European projects aimed at making clouds as secure as possible when it comes to data transfer and storage.

Now the question comes naturally: what is allowed or not allowed when dealing with sensitive personal data likely to reveal our intimate personalities, when it comes to social life, religion or health? Law professor Jean-Philippe Dunand addresses the limits on the surveillance of employees in the workplace, on the eve of a one-day conference he has organised on the protection of personal data in labour law. At the same event, professor Anne-Sylvie Dupont, a specialist in social security law, speaks about the management of personal data by insurance companies, and the intrusive methods they sometimes use with policyholders.

The protection of personal data is also one aspect of journalist and anthropologist Gilles Labarthe’s work. He mentions the growing problems for investigative journalists faced with the proliferation of information channels on the Internet and the rising power of the public relations sector on the media. Journalists are confronted with a world where it is becoming increasingly difficult to guarantee the protection of information sources, an issue at the very centre of journalistic deontology.

The Watchman Above

Now affordable to all, drones are raising the issue of access to the sky more generally. In this respect, an obvious bias appears in the survey carried out by the University of Neuchâtel. Drones are used by quite a limited segment of the population, namely young men fond of new technologies. “The aerial vantage point remains a male prerogative, just as kings in the old days would watch the enemy approaching from a castle tower, or as the royal cartographers would map the kingdom”, explains Francisco Klauser. Society as a whole is therefore far from appropriating this new space, where women remain largely absent.

A three-year research project

This questionnaire survey is part of a wider research programme on civil drones, linked to the Chair of Political Geography headed by Francisco Klauser. The “Power and Space in the Drone Age” project is funded by the Swiss National Science Foundation, reaching more than CHF 440,000 over three years. It will be completed at the end of February 2019. In addition to Francisco Klauser and Silvana Pedrozo, postdoctoral student Dennis Pauschinger joined the programme in March 2017. Two Master’s theses are also being carried out in relation to this FNS project, one by Léa Stuber and the other in anthropology by Raphaële Rasina.
Francisco Klauser, professor at the Chair of Political Geography

What people think about it

The public looks on the use of drones by the police or the army with a much more favourable eye than their use for commercial or leisure purposes. This is one of the outcomes of a survey conducted by professor Francisco Klauser with doctoral student Silvana Pedrozo and a group of Master's students at the Institute of Geography at Neuchâtel. This first-of-its-kind survey concerned the perception of drones by the public, as seen from the point of view of social sciences.

"This is the first time in Europe that a survey has looked into the social acceptability of civil and military drones", highlights Francisco Klauser. The survey is based on a questionnaire sent to 3,000 people in the Canton of Neuchâtel, of whom 600 have responded. Here are the first results.

"The use of these machines for commercial purposes, such as delivery, is still perceived very negatively: nearly two people in three find it upsetting," the researcher goes on. "In other words, people are not ready to see this new part of airspace being used to make money." And this in spite of the fact that 57% of respondents believe that this market is set to grow. The same proportion fears accidents due to these aircrafts, while 72% of respondents would approve a complete ban on their use to observe public spaces.

The study shows that most people are ignorant of what they are – or are not – allowed to do with a drone, as well as of the regulations on the filming of public gatherings. Even though researchers consider the present legal dispositions to be clear enough, the problem lies with the application of the law. What concrete and feasible measures could be taken to enforce the legislation? This question remains open.

As to the idea of buying a leisure drone, it is swept aside by 81% of respondents, who wouldn't even considering it. This shows a real lack of interest in these machines. One could even call it serious defiance, as one person in three would like to ban them outright, while 68% of respondents fear they might be used to perpetrate terrorist attacks. On top of that, more than half the informants are fearful of the accidents these aircrafts might cause.

Mobile movie cameras

This anxiety can be explained by the fact that 87% of respondents perceive drones as CCTV cameras, which can be running anywhere, any time. As a result, people fear they might appear on pictures of private places, typically through a window; this fear seems to be at the root of their rejection of drones for leisure or commercial purposes.

Having said that, as soon as drones are operated by the police or the army, they enjoy a better image. This is because the authorities' duty is to protect the public, and the use of drones is part of the effort to achieve this objective. For instance, they can be of help in cases of burglary, transport of illicit substances, search and rescue, and security for big events.

To find out more:
Power and Space in the Drone Age:
www.unine.ch/geographie/home/recherche/drones_pouvoir_et_espace_aerien.html

A twenty-year-old technology

Since 2001, Swiss border guards have been using a drone system dating back to 1995 for specific missions around the border zones of the Swiss territory. Geographer Silvana Pedrozo describes this means of operating a wider surveillance of the border, albeit with limitations that justify the air fleet renewal planned for 2019.

In 2014, as a doctoral student at the Institute of Geography, Silvana Pedrozo, had the opportunity to observe a Swiss military drone engaged in a mission across the Swiss Jura region. These aircraft are completely different from the present quadcopters you can carry in one hand. They are real 5.7-metre-wingspan 270-kilo unmanned airplanes, built by the Swiss defence firm RUAG.

The present use of fifteen of such ADS 95 drones is part of an agenda which is both civil and military, designed to improve the security of border zones as well as specific areas within the territory. Thanks to thermal captors and cameras, the drones gather a whole range of data that would be difficult for customs officers to collect otherwise.

Drones are valuable assets for reconnaissance. They are less costly than helicopters; they can be operated at night, thanks to their infrared cameras, and they are well adapted for securing important events. “Our aim is to better know what to look for and where to look. So, we get a better knowledge of certain areas, some of which are difficult to access, and we can then decide whether to send field officers there”, explains one of the border guards interviewed by the researcher.

Drones allow border guards to locate and follow individuals, as well as groups or vehicles. Their missions have contributed to chasing burglars in residential areas and vehicles about to flee across the French-Swiss border, as well as arresting migrants in disused trains.

Risky missions

However, the system suffers rather surprising limitations. While in most countries the military drones deployed can operate above the entire national territory, this is not the case in Switzerland. Surveillance of all the mountainous areas is limited, because it remains riskier for aircraft with such weak high-altitude flying capacity and reduced autonomy (a maximum four hours).

Besides this, for every drone engagement, fifteen to twenty people must be mobilised. Another problem is the machine’s loud noise, which casts doubt on its ability to operate inconspicuously. On top of that, rain and fog affect the performance of the ADS 95, forcing pilots to modify planned routes, or even to ground drones in autumn and winter.

All these weaknesses drove the authorities to order six new military drones. These will be able to operate in all weathers, and will enjoy increased flight autonomy and reduced noise. What’s more, they won’t need a plane to escort them during their use.

A survey carried out by the University of Neuchâtel on the acceptance of drones by the general public showed that half the respondents approved of buying new military drones. However, for 60% of informants, the fact that these drones could carry weaponry causes a problem, and so does the decision to buy them from Israel. This last point elicited 44% of critical opinion, compared to 28% of respondents who did not have any objection to it.

Silvana Pedrozo,
doctoral student at the Institute of Geography

Confidentiality guaranteed

Silvana Pedrozo's interviewees are trying to be reassuring on data protection. First, the use of Swiss military drones is still occasional and does not allow remote interception of communications. The data collected are stored by the Air Force for 30 days before they are deleted, unless they might be valuable for later use. The current sensors reveal shapes and outlines, but facial recognition is impossible. Finally, the army is subject to military safety regulations staving off potential misuse.

A positive image

The presence of CCTV cameras has had a positive impact on the image of the Pâquis neighbourhood, according to 44% of respondents, against 15% who think the opposite. Generally, the recreational aspect of the neighbourhood and its nightlife – including prostitution – are not considered as sources of disturbance.

24/7 corner shops ("rescuers") are the places that are viewed most unfavourably. These shops sell alcoholic beverages at any hour of day or night, and their prices are lower than those in licensed drinking venues. Once the purchase is made, clients usually end up drinking in the public space, causing various disturbances such as noise and conspicuous alcohol abuse.

Raoul Kaenzig,
research fellow at the Institute of Geography

A Geneva neighbourhood studied at Neuchâtel

For the first time in Switzerland, the effect of CCTV cameras on the life of a neighbourhood was the subject of a long-term detailed study. Following the installation in 2014 of 29 CCTV cameras in the Pâquis, an area well known for its animated nightlife, Raoul Kaenzig and Francisco Klauser interviewed various population groups (residents, police officers, local business owners, and people involved in prostitution). On behalf of the Geneva State authorities, researchers from the University of Neuchâtel published the results of their surveys in November 2016, at the end of their two-year study.

"The most striking result of our study is the overall positive reception of this surveillance project by the public," notes Raoul Kaenzig, research fellow at the Chair of Political Geography. While it is true that there were fears at the beginning of the scheme, they rapidly disappeared, as 59% of respondents do not think that the system harms privacy. Only 15% of informants would like the CCTV cameras to be removed from the neighbourhood.

The public's sense of safety has undeniably increased in the Pâquis, especially at night; one in three people report feeling safer since the CCTV cameras were installed. Among pilot zone residents, this proportion even reaches 36%.

While the video surveillance system is well accepted, the public is certainly not enthusiastic, the researchers add by way of qualification. The public's preference clearly goes to measures involving human presence or streetscaping, such as local police, enhancing social ties via neighbourhood life and associations, and better public lighting.

A complementary tool

When it comes to solving crimes, CCTV cameras can by no means replace police fieldwork; but they are used as a complementary tool. Proof of this is the relatively modest use of image retrieval. Retrieval of CCTV images was carried out on 89 occasions in the pilot zone, which corresponds to an average of only 3.1 occasions per camera over the two years of the evaluation. A slight rise in solving crimes was observed over the period, but the part played by CCTV cameras in this increase cannot be quantified.

With respect to the operational aspect of the scheme, the study emphasises the importance of the training of the operators viewing the images collected. "Their sense of observation and their analytical skills, their knowledge of the field and their ability to cooperate with the other actors in the safety chain are decisive for the system's efficiency. Without this human element, cameras are useless", highlights Raoul Kaenzig.

The dissuasive effect of the use of CCTV cameras remains minimal. Police statistics have shown no reduction in crime: in fact, while there was a slight drop in theft and assault records, infractions taking place within the cameras' scope paradoxically increased (+15%) over the period studied. In general, the presence of the cameras has not resulted in a displacement of crime to adjacent streets outside the monitored area, except for drug dealing.

"Drug dealing has not disappeared from the area covered with cameras, but the transactions performed in nearby streets have been increasing", Raoul Kaenzig points out. Deals are done in an area that is both harder to control and bigger than in 2014. There is also a change in the places where deals are done within the monitored area: in off-screen zones, in vehicles, in courtyards or in apartment block lobbies.

To find out more:
Raoul Kaenzig and Francisco Klauser, *Evaluation de la 'vidéoprotection' dans le quartier des Pâquis à Genève*, summary for the press, 2016 www.unine.ch/geographie/home/recherche/paquis.html

When your smartphone mediates where you go

How does the *Foursquare* software influence your movements? For her PhD thesis at the Institute of Geography, Sarah Widmer investigated the use of this smartphone application in New York in 2013 and carried out detailed analysis of about 30 users' feedback. Doing so, the geographer brought to light the pros and cons of this navigation aid.

What is *Foursquare*?
Basically, *Foursquare* started as a location-based social networking app with a gamification aspect, and then evolved into a local search engine recommending leisure venues such as bars, cafes and restaurants. It provides personalised aid to urban navigation based on the history of the places the user has been to before, or those visited by members of their social network, or users with similar habits. This results in "tailor-made" movements that encourage exclusive forms of togetherness.

How do *Foursquare* users feel? Do they get the feeling they are being manipulated?
Rather interestingly, several informants were not aware that the results were actually personalised via an algorithm. Other users were perfectly aware of the way the application works, and used it precisely in order to receive this personalised advice. Quite often, the recommendations were not adopted blindly, but rather compared with results from other apps (e.g. Yelp or Google Maps), or refined using new search criteria, or criticised for their lack of relevance. Decision making can therefore not be considered as entirely determined by this technology.

Of course, some people are more enthusiastic about technology than others, and use the app in a more strategic way. In this case, they use it with the conscious goal of accessing personalised content, and avoiding being directed to certain places they see as ill-suited to them. Obviously, this raises issues as to our present ways of living together in cities.

What feelings did the use of personal data arouse?
Users were aware of the privacy risks involved (most of my interviews took place a few months after Edward Snowden's revelations), but they tended to think that giving their personal data was the price to pay to receive the personalised service offered by the app. On the whole, this type of risk has become commonplace, and is perceived as inevitable, and part of daily life.

In your view, what part do these apps play in the management of our movements?
Immediate Internet access on our mobiles certainly impacts the way we experience mobility. It can be very simple things, like that Paris app called "Parisci la sortie du métro" ("This way to the subway exit"), which tells you which carriage to get on to be positioned just in front of the subway exit as the train stops at your destination, or these public transport apps that show bus arrivals in real time. Accessing this type of information allows us to manage our activities better within our time/space budget. Smartphones offer great flexibility and allow us to adapt to an ever-moving reality made of changes and unexpected events. The feeling of self-confidence provided by this technology (my interviewees often told me they never felt lost) has a deep impact on the way we manage and experience our relationship with space and movement.

And the other side of the argument?
Obviously, in my PhD thesis, I take a rather critical look at these technologies and point out two major issues, namely data surveillance (and therefore privacy risks) and the social segregation automatically carried out by these algorithms that continuously prioritise, sort and classify their users.

To find out more:
Sarah Widmer, *Smartphone* et *big data*, GeoAgenda 2016/4, p. 10-12

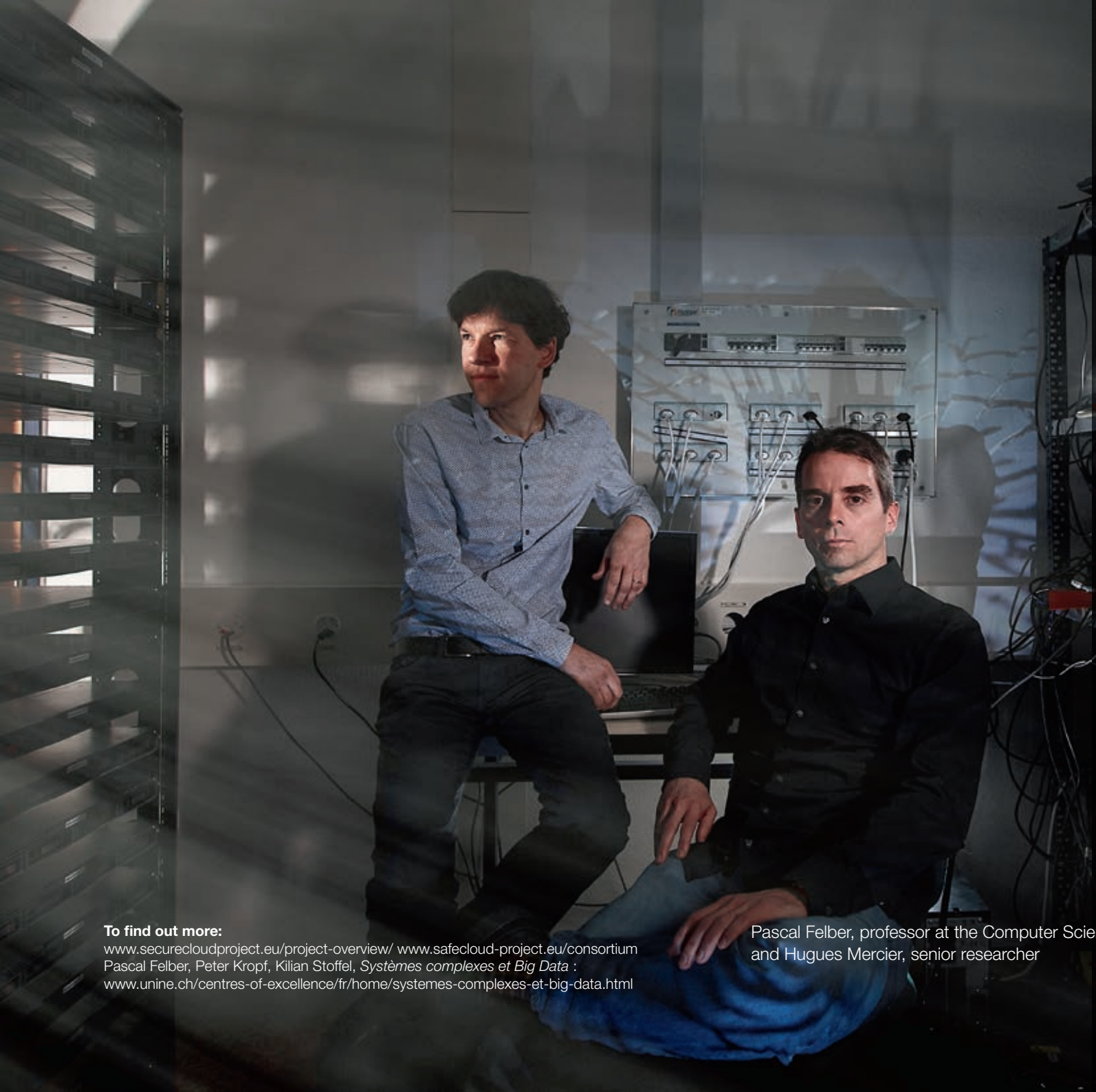
Sarah Widmer,
author of a PhD thesis on urban uses of smartphones

International collaborations

SecureCloud brings together 14 research partners from Germany, England, Brazil, Denmark, Italy, Israel and Switzerland. Marcelo Pasin, researcher at the University of Neuchâtel and professor at the HE-Arc is in charge of the local coordination of the research project, which started at the beginning of 2016, scheduled to take three years. *SecureCloud* has provided the University of Neuchâtel's Complex system and Big Data Competence Centre, with funding of CHF 600,000.

SafeCloud involves seven academic and industrial partners in an international consortium including Germany, Estonia, Portugal and Switzerland. The project started at the beginning of September 2015. It is funded for a three-year period, and there is a share of about one million Swiss francs for the University of Neuchâtel. Hugues Mercier, senior researcher at the Computer Science Department and at the Institute of Mathematics, is in charge of the scientific coordination of the project.

To find out more:
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



Pascal Felber, professor at the Computer Science Department and Hugues Mercier, senior researcher

Private data and public interest

When it comes to health, banking or Internet voting, cloud computing is an attractive solution for companies, governments and citizens. But how can we benefit from these services without revealing our personal data? Technological answers are developed at the Computer Science Institute of the University of Neuchâtel, as part of international research projects.

The growth of clouds, these virtual data storage networks, allows anyone to access data reliably from any connected spot in the world, 24/7. But how can data confidentiality be guaranteed? This is the challenge at the heart of the research done by the team around Pascal Felber, professor at the Computer Science Institute of the University of Neuchâtel. “We are dealing mainly with two aspects of cloud technologies, namely data transfer security and data storage security”, points out Prof Felber, a specialist in complex systems.

In the medical field, information from patient records is frequently communicated for statistical purposes or to monitor epidemics. At the same time, patient records from which this information originates must be unidentifiable. It is almost like asking external partners — partners you do not trust — to read a text without accessing it. The challenge may seem paradoxical, but it is the very objective of the *SecureCloud* research project. The idea is to mimic what happens when bank customers want to access their safety deposit boxes: a bank employee accompanies them, and withdraws while the customer examines the boxes’ content.

“The data owner, for instance a hospital, stores data on its own computers. When it must share some of the data with external partners, the hospital does this via a secured enclave in the cloud, a virtual shield protecting it from any possible intrusion from the recipient computer. So we are certain that these data will not be read nor altered without the owner being informed,” explains Marcelo Pasin, who is in charge of the local coordination of the *SecureCloud* research project.

As for storage, the strategy is one of file partition. Imagine we want to store a picture in a cloud: the operation entails encrypting, then dividing up the photo into smaller pieces, each stored in a different location with different providers (such as Dropbox, Google Drive or Amazon).

“This makes it impossible for one or the other of the providers to learn anything about the content of the stored data,” concludes Hugues Mercier, senior researcher at the University of Neuchâtel and scientific coordinator of the *SafeCloud* project.

As a result, the information remains unusable not only to hackers, but also to any authority (e.g. network administrator, government agency) that might have privileged access to the servers where the data are stored. Only the legitimate beneficiaries, who have access to all the pieces, can group them back together and so reveal their initial meaning: in this case, the original photo.

The right to be forgotten

Alongside the technical aspect of confidentiality, the *SafeCloud* project has a legal component covered by the Intellectual Property and Innovation Research Centre of the Law Faculty, where Yves Bauer and Prof Nathalie Tissot investigate, among other things, the right to be forgotten.

The aim is to make sure the technical solutions implemented respect this fundamental right that allows anybody, after a certain length of time, to demand the erasure of all traces of acts which might damage their reputation. However, the way the data are handled to make them confidential somewhat implies that they are set in stone, with their erasure nearly impossible. “There should be a way to write certain information ‘in chalk’ to make it erasable, but only by authorized persons”, Hugues Mercier suggests. Therefore, this legal research aims to find a balance between what can be erased and what cannot.

Gilles Labarthe,
journalist and anthropologist

Exponential growth

In the last twenty years, the information available on the Internet has grown exponentially, through the proliferation of both sources (administrations, NGOs, associations, blogs, etc.) and channels (online news media and social media). New processing and presentation capabilities (such as cartography) have also opened a path for new journalistic production possibilities based on cooperation and participation.

What comes to mind here is the collective enquiries originating with transnational investigative journalist networks. These enquiries rely on leaks and confidential information released by whistle blowers. One topical example of these is the “Panama Papers”: millions of pieces of data transmitted in spring 2016 by the *International Consortium of Investigative Journalists* (ICIJ), revealing tax evasion practices. There are also the “Football Leaks”: 18.6 million documents exposing money-laundering cases, prostitution and organised crime networks in the football industry. (GL)

Investigating under influence

In his PhD research project carried out at the Journalism and Media Academy of the University of Neuchâtel, journalist and anthropologist Gilles Labarthe is looking into the impacts of the New Information and Communication Technologies (NICT) on the methods used by investigative journalists in French-speaking Switzerland. These new tools offer advantages but also raise a number of issues: misinformation, Internet surveillance, risks related to digital fingerprints, and so on.

In Western Europe, investigative journalists have never seemed so well connected, able to access information, to investigate and to publish. Drones have even been used in some countries to reveal the luxury homes of corrupt civil servants or contested leaders, to expose their lavish lifestyles (in stark contrast to their official wages), or to show the real number of demonstrators at protests.

Perhaps less sensational than drones is the hidden (and, on a smartphone, inconspicuous) camera, another of those seemingly "perfect tools", swiftly and cheaply producing dramatic, entertaining or emotional effects, essential to catch television viewers' attention. The use of such cameras has become extremely widespread in investigative programmes in France. To justify this use, producers and journalists say that it is harder and harder to "get past the communication professionals' gatekeeping" — that is to say, the growing hold of the PR sector over the media.

The "fifth estate"

Researchers have suggested the concept of a "fifth estate" to describe this hold. Civil servants, politicians, lobbyists, etc. all communicate via the Internet and the social media to influence journalistic reports and to develop gatekeeping strategies, thereby imposing their control over information.

In French-speaking Switzerland too, the journalists interviewed for this study highlight the obvious increase, since the 2000s, of the effects of this "fifth estate". A majority believe that NICTs have now more detriments than advantages in the exercise of their profession. More than half of them have given up publishing investigative reports in the French-speaking Swiss media.

Among the reasons mentioned are the risks of being manipulated by external actors circulating false documents or exerting pressure and, in particular, the difficulties in guaranteeing the protection of sources. Indeed, what can be done about digital fingerprints? Some people recommend encryption, others going back to "analog" (pen, note-taking, informal one-to-one meetings with informers) in order to reduce the risks related to Internet surveillance and the possible hacking of their digital tools.

The reorganisation of regional and national professional organisations would be yet another way to respond to the inversion of the relationship between journalists and communication professionals. Today, there are between ten and twenty times as many PR professionals as the 4600 members of the Swiss Federation of Journalists.

The objective would be to compensate to a certain extent for the gradual loss of investigative teams in the main daily and weekly newspapers in French-speaking Switzerland – with the exception of the "investigative unit" of the *Matin Dimanche* and *SonntagsZeitung*, set up in 2012. This is also one of the reasons for the launch, about 10 years ago, of the Swiss Investigative Journalists' Network, which offers, among other things, access to transnational investigative networks. (GL)

To find out more:
http://www.investigativ.ch, Swiss Investigative Journalists' Network

The limits of surveillance in the workplace

In the age of the pervasive use of computers in all professions, what does the law say about staff surveillance? Specialist in labour law Prof Jean-Philippe Dunand wrote a commentary on the law as it applies to the protection of employees' personal data. On the same topic, he and his colleague Pascal Mahon also co-edited a 380-page book that has just come out.

While staff surveillance is not a new issue, in the digital era it can take on some insidious characteristics: for example, a CCTV camera that, under the guise of monitoring an automatic machine, pointed right at an employee's workstation. While this case seems clearly illegal, the general question of whether or not to ban staff surveillance must be afforded more nuance. "The first reason for this is that it's in the very nature of work relations that the employer can supervise their employee's work in some way, in order to check that their guidelines have been applied," says Jean-Philippe Dunand.

This is precisely the argument justifying the surveillance of emails or Internet use: not only a desire to check that a task is correctly executed, but to make sure that instructions about confidentiality, security and company reputation are duly followed. Employers, however, are required to inform their staff about the surveillance. They must also stick to certain principles, such as good faith and proportionality, in processing the worker's personal data. "However, when private use of email is allowed or tolerated, the employer should not have access to the employees' private emails", explains the law professor.

This is coupled with other types of electronic surveillance generally accepted in the workplace. For example, CCTV cameras may cover some strategic or sensitive places in company premises, such as parking lots, safety deposit room, entrances, counters or shop shelves. For accident prevention purposes, it is also possible to monitor places with machines or dangerous substances.

Vehicles, too, can be followed using a GPS device. This is the case, for instance, in private security, road transport or taxi companies. "The Federal Supreme Court has admitted that a system making it possible to locate all the vehicles in service at any time could be justified under certain conditions", indicates Jean-Philippe Dunand.

More specifically, implementing a geolocation system is allowed if the employer can prove that employees are not monitored in real time: that is to say, that the check only takes place after the event, at the end of the work day. Indeed, according to the Federal Supreme Court, "the possibility of following the vehicles' journeys during the day in real time involves the risk that the employer may repeatedly and unexpectedly ask their employees about their position or their route choice, which would add to the stress caused by the feeling of being constantly watched."

However, the Federal Supreme Court considers that installing spyware on an employee's computer is in principle illegal; it is an excessively intrusive and disproportionate measure that goes against the rules for the protection of workers, and against the applicable law regarding personal data protection.

To find out more:
Jean-Philippe Dunand et Pascal Mahon (eds), *La protection des données dans les relations de travail*, Genève/Zurich/Bâle, éditions Schulthess, 2017

Protecting the personality

All individuals have a right to the protection of their personality. This notion includes physical integrity, physical and psychological health, moral integrity and social consideration, individual liberties and privacy. Personal data are all the information that might make a person identifiable. “From a mere AVS (i.e. social security) number, it is conceivable to identify a person in a company”, explains Philippe Dunand. In work relations, personal data include all the information about workers, regarding both their private and professional lives. The law distinguishes, among personal data, sensitive data comprising “opinions and religious, philosophical, political or trade union activities, health, the realm of intimacy, membership of a race, social assistance measures, legal proceedings and penal and administrative sanctions.”

Jean-Philippe Dunand,
professor in Labour Law

Anne-Sylvie Dupont,
professor in Social Security Law

Policyholders held hostage

In the health sector, insurance companies usually impose the lifting of medical confidentiality on their policyholders' medical records. In case of refusal, it is not possible to receive cover. Holder of the Chair of Social Security Law, Prof Anne-Sylvie Dupont, highlights the imbalance between insurance companies, who hold the purse strings, and policyholders, on whom excessively intrusive rules are imposed.

The processing of patients' or social benefit seekers' personal data is a sensitive area for private insurance companies and social security agencies. In theory, applicable law demands that insurers only ask for the relevant data allowing them to make a decision on the insured party's right to benefits. "In practice, the insurer usually asks the insured party to release doctors from their duty of confidentiality, so that they can enquire directly from them," explains Anne-Sylvie Dupont.

The main drawback of this situation is that it gives insurers a carte blanche, as it were, as they often have the insured party sign statements phrased in very general terms. "These release not just doctors, hospitals and other health professionals who know about the case from their duty of confidentiality, but also other private insurance companies, social security agencies, social workers, employers, etc."

This results in information on a benefit seeker circulating far too widely and not always in the right way. This blatantly happens in companies offering several types of insurance, both private and social, where sensitive data often flows to and fro.

Sometimes, it can turn against the insurer. This happened in a case where a company wanted to invalidate a contract falling within the framework of private insurance, on the grounds that the policyholder had omitted to mention certain facts when signing the contract.

The Federal Supreme Court ruled against the insurer, judging that the company must have known about these facts, since the insured party also had mandatory health insurance (LAMal) policies with the same insurers.

"In other sectors of insurance, such as disability insurance and accident insurance, it's a problem that the insured party's sensitive personal data are stored in a 'global' record, to which nearly everyone can have access," adds Anne-Sylvie Dupont. In their defence, insurance companies claim they want to fight harder against fraud, and base their argument on a balancing of interests. So, in their view, efforts to avoid paying undue benefits should systematically outweigh policyholders' interest in keeping some private aspects of their lives to themselves.

In this context, it seems very difficult to compel insurance companies to restrict access to a patient's data to those deciding whether or not to allocate benefits. There is a single exception to this: namely, mandatory health insurance, where companies rely on a medical adviser whose role is to filter sensitive data, so that only the information needed to decide on providing cover is transmitted to the insurer. "Today, this system doesn't work fully, because it's not always watertight," surmises Anne-Sylvie Dupont. "But at least it exists, contrary to what happens with other social insurances, like disability insurance (AI)."

"In order to better defend the patient's medical confidentiality, political action would be necessary," recommends the law professor. "Or at least activist work, reporting cases to the Federal Data Protection and Information Commissioner (FDPIC). Insurance companies' practices are regularly criticised in the FDPIC's reports."

To find out more:
Anne-Sylvie Dupont, «La protection des données confiées aux assureurs», in Jean-Philippe Dunand et Pascal Mahon (eds),
La protection des données dans les relations de travail, Geneva/Zurich/Basle, éditions Schulthess, 2017

University of Neuchâtel degree programmes related to Big Data:

Master of Arts in Social Sciences, major in Human Geography

Majoring in the “Geography of major contemporary issues”, students are taught to analyse the crucial issues facing society today: global urbanization and its challenges in the North and the South, international migration and the issue of refugees, the role of new technologies in political change, and the social dimensions of climate change. This curriculum gives students the skills to analyse and critique the geographical aspects of these issues, as well as the means to develop relevant and innovative solutions.

Swiss Joint Master in Computer Science at the Universities of Bern, Neuchâtel and Fribourg

This unique programme provides students with a wide range of courses at the cutting edge of computer science research and development. It is an ideal program for computer scientists who want to expand their knowledge, enriching their career perspectives or preparing themselves for doctoral studies.

Research *Complex Systems and Big Data* Competence Centre

The Complex Systems Group’s expertise lies in large-scale systems, with a focus on cloud computing, distributed storage, concurrent programming, and complex data processing. In particular, its researchers have been developing novel techniques to acquire, transmit, store, and process massive amounts of data.

The Data Mining Group’s research activities primarily focus on two questions: firstly, how data mining algorithms can benefit from knowledge representation systems; and secondly, how the efficiency of existing systems can be improved.

UniNEws is a publication of the University of Neuchâtel. Av. du 1er-Mars 26, 2000 Neuchâtel. Tel.: + 41 32 718 10 40, bureau.presse@unine.ch, www.unine.ch.
Notice: Bureau presse et promotion, University of Neuchâtel. Text: Igor Chlebny; except p. 14-15: Gilles Labarthe; English translation: Language Centre, University of Neuchâtel
Photos: Guillaume Perret; except p. 1 & 2: Bernard Léchot and p. 11: Anna Montemayor Layout: Leitmotiv; Printed by IJC on recycled paper (FSC)
March 2017 issue. Appears at least four times per year.