JTIT Internationale n°4 – juillet 2013
Special international issue # 4– July 2013
ALAIN BENSOUSSAN
Juristendances Informatique et Télécoms
Le réseau Lexing vous informe – The Lexing Network informs you

L'ACCES DES AUTORITES AUX DONNEES PERSONNELLES – PARTIE 1

GOVERNEMENT ACCESS TO DATA – PART 1

Conjuguer sécurité et liberté

▪ Les récents développements de ce qui a été appelé l'affaire « Prism », où il est apparu que les autorités américaines avaient mis en place un système secret étendu et ultraorganisé d'interception des communications électroniques dans le monde, officiellement pour empêcher les attaques terroristes sur le sol américain, ont fait apparaître qu'un équilibre devait être trouvé entre d'une part la protection de la vie privée et d'autre part la protection de la sécurité nationale.
▪ Il est bien entendu parfaitement compréhensible que les Etats souhaitent procéder à des enquêtes, dont certaines d'entre elles doivent nécessairement porter atteinte à la vie privée ou rester secrètes, et ce à des fins de renseignements ou pour anticiper certaines agressions dont pourraient être victimes les entreprises, les citoyens ou leurs intérêts économiques. Toutefois, il est également généralement admis que les droits civils, parmi lesquels figure notamment le droit absolu à la protection des données à caractère personnel, doivent être garantis de manière prioritaire.
▪ C'est la raison pour laquelle il semble difficile d'assurer un équilibre parfait entre ces deux préoccupations légitimes et qu'il existe des différences notables entre les différentes législations du monde applicables aux interceptions de communication ou à l'accès des autorités judicaires ou publiques aux données.
Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde.

Compte tenu de l'actualité de ce thème, il a été décidé de le traiter dans deux numéros successifs de notre Jtit Internationale. Ce numéro contient les contributions des pays suivants : Afrique du Sud, Angleterre, Belgique, Canada, Chine, Colombie et France. Le numéro suivant sera diffuse en septembre prochain.

Reconcile security with freedom

▪ *The recent developments of what has been called as the "Prism" case, by which it appeared that US governmental authorities have put in place an very large and very well organized secret system to intercept electronic communications around the world officially to avoid any terrorist attack on US soil, has revealed that there is a balance to be found between privacy protection issues, on one hand, and national security protection concerns, on the other hand.*
▪ *It is of course perfectly understandable that governments have to proceed to investigations, some of them being necessarily either invasive or kept secret, either for intelligence purposes or to anticipate some aggressions that companies, citizens or their national economic interest could suffer from. But it is as well generally considered that civil rights, personal data protection being one of their essential parts, should be protected as well and put on top of the priorities.*
▪ *This is why it seems difficult to guarantee a perfect balance between those two legitimate concerns and that certain discrepancy exists in the legislation applicable to communication interceptions or judicial and governmental data access rules across the world.*
The Lexing® network members provide a snapshot of the current state of play worldwide.

As this topical subject is vast and complex, it has been decided to address it in two successive issues of our Jtiti Internationale. This issue incudes the contributions of the following countries: South Africa, England, Belgium, Canada, China, Colombia and France. The next issue will be published in September.

A propos de Lexing®

Lexing® est le premier réseau international d'avocats technologues dédié au droit des technologies avancées.

Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leur pays respectifs..

About Lexing®

Lexing® is the first international network of lawyers dedicated to technology law.

Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

FREDERIC FORSTER

AFRIQUE DU SUD

MICHALSONS

- **Focus sur l'accès des autorités aux données stockées dans le *cloud***

- Les autorités sud-africaines peuvent-elles accéder aux données stockées dans le cloud ? Oui. En Afrique du Sud, conformément à la loi sur l'interception des communications et la fourniture d'informations sur les communications (« RICA ») **(1)**, l'Etat peut intercepter les données stockées dans le *cloud* à condition de disposer d'une autorisation à cette fin. Dans ce cadre, il peut réaliser cette interception sans en informer l'utilisateur au préalable, en se rapprochant directement du prestataire de services *cloud*. Ce dernier, après avoir reçu communication de l'autorisation, décrypte les données contenues dans le *cloud* et les communique aux services de l'Etat.
- Quelles sont les conditions pour l'obtention d'une autorisation d'interception ? La Section 16 du RICA décrit les modalités à respecter afin d'obtenir une autorisation d'interception.
- Par ailleurs, l'administration fiscale sud-africaine, le « SARS » **(2)** peut obtenir des informations relatives aux résidents sud-africains hébergées sur un serveur à l'étranger lorsqu'une convention de double imposition **(3)** a été conclue entre l'Afrique du Sud et le pays où ce serveur est hébergé, dans le cas où le libellé de la clause d'échange d'informations de ladite convention serait assez large. Toutefois, les dispositions d'une telle convention ne peuvent étendre les obligations ou les droits créés par le droit national. Ainsi, le SARS ne pourra se prévaloir de la clause d'échange d'informations d'une convention de double imposition dans le but d'obtenir la communication d'informations qui n'auraient pu être obtenues sur la base de la législation ou dans le cadre de la pratique administrative normale du pays étranger ou de l'Afrique du Sud. En outre, très souvent, la législation sur la protection des données de nombreux pays interdit aux services fiscaux de divulguer des informations au SARS, à moins que les services fiscaux du pays étranger ne soient autorisés à recevoir ces informations dans le cadre de la transmission d'informations fiscales.

REFERENCES

(1) Regulation of Interception of Communications and provision of Communication-related information Act (RICA)

(2) South African Revenue Service ("SARS")

(3) Treaties for the Avoidance of Double Taxation

ANDREW WEEKS

SOUTH AFRICA

MICHALSONS

- ***Focus on Government access to data in the cloud***

- *Can the South African Government access data in the cloud? In terms of the Regulation of Interception of Communications and provision of Communication-related information Act (RICA), Government may intercept your data stored in the cloud only with an interception direction. They can do this without your knowledge by approaching the cloud service provider with the direction. The cloud storage provider then decrypts the data and shares it with Government.*
- *What does Government have to show in order to obtain an interception directive? Section 16 of RICA sets out the requirements for an interception direction to be granted.*
- *The South African Revenue Service ("SARS") **(2)** may be entitled to obtain information that relates to South African residents which is situated on a server abroad if there is a double tax agreement ("DTA") **(3)** in place between South Africa and the relevant country. This is in terms of the information exchange clause which is very wide. However, the provisions of the DTA cannot extend obligations or rights created under domestic law. So SARS may not invoke the information exchange clause in the DTA to impose the obligation to supply information, unless that information were obtainable under the laws or in the normal course of the administration of the law of the overseas country or South African law. Data Protection legislation in several countries will often preclude the Revenue authorities from disclosing information to SARS unless the Revenue authorities in the overseas country are entitled to the information for purposes of tax disclosure in that country.*

REFERENCES

(1) Regulation of Interception of Communications and provision of Communication-related information Act (RICA)

(2) South African Revenue Service ("SARS")

(3) Treaties for the Avoidance of Double Taxation

ANDREW WEEKS

▪ **Focus sur l'accès des autorités aux données stockées dans le *cloud***

▪ Le Cloud computing est en passe de s'imposer comme la solution informatique de prédilection des entreprises et des particuliers.
▪ Or, les systèmes cloud reposant davantage sur des serveurs distants que locaux, il est plus aisé d'accéder aux données qui y sont stockées que de les récupérer sur l'équipement local de l'utilisateur dans le cadre d'une procédure de saisie perquisition classique.

▪ C'est la raison pour laquelle les services de police s'intéressent très fortement au cloud afin de surveiller les activités illégales et obtenir des données techniques et scientifiques. Cette situation met en jeu des intérêts divergents, d'un côté le respect de la vie privée et de l'autre les besoins de police, et pose juridiquement une série de problèmes épineux :

1) les enquêtes menées en ligne affectent un grand nombre de personnes, dont les droits et les obligations doivent être pris en compte. Les données techniques et scientifiques peuvent en effet être stockées sur des systèmes utilisés non seulement par un suspect, mais également une victime ou encore un tiers innocent. En outre, l'accès aux données suppose la coopération (parfois sous la contrainte) des hébergeurs des serveurs du cloud et des opérateurs des réseaux de télécommunications.

2) De plus, la nature transfrontalière du cloud computing pose des difficultés en terme de compétence, notamment lorsque les dispositions légales d'un pays entrent en conflit avec celles d'un autre pays ou doivent être mises en œuvre dans un autre pays.

3) le stockage morcelé des données techniques et scientifiques sur le cloud peut également rendre difficile la récupération et le réassemblage des données en un tout cohérent. Cet éparpillement peut potentiellement réduire leur valeur probatoire devant le tribunal et leur récupération peut être compliquée si des fragments sont stockés sur des serveurs situés dans différents pays, ou si la localisation d'un serveur hôte est inconnue. Dès lors, identifier les auteurs d'infractions peut s'avérer être un tâche ardue si les liens entre les données et le dispositif dont elles proviennent sont flous ou si les données sont cryptées.

4) Enfin, l'accès des services de police aux données empiète sur le droit à la vie privée, qui est considéré comme un droit fondamental dans de nombreux pays. En Europe, l'article 8 de la Convention européenne des droits de l'homme **(1)** garantit aux personnes le droit au respect de leur « vie privée et familiale ». Toutefois, ce droit n'est pas absolu et peut être limité si nécessaire, notamment pour protéger la sécurité nationale et lutter contre la criminalité et les atteintes à l'ordre public, sous réserve de respecter les dispositions légales, de répondre à un intérêt légitime et de prendre des mesures nécessaire et proportionnées.

REFERENCES

(1) Convention européenne des droits de l'homme

(2) Convention sur la cybercriminalité

(3) Article, "WikiLeaks website pulled by Amazon after US political pressure", The Guardian, 2 December 2010

(4) Amazon message on WikiLeaks

DANNY PREISKEL

▪ Un nombre croissant de pays encadrent la vie privée par une législation spécifique qui protège les personnes physiques et morales contre la collecte et le traitement non autorisés des informations qui pourraient être utilisées pour les identifier personnellement. Toutefois, ces initiatives sont en général contrebalancées par des dispositions légales autorisant les services de police à surveiller et intercepter le contenu des données en ligne, ainsi que des informations entourant leur transmission (détails sur les sites Web consultés, durée des conversations téléphoniques…). Si certains pays subordonnent rigoureusement ces interceptions à une autorisation judiciaire, d'autres – tels que le Royaume-Uni – autorise les services de police à accéder aux données des abonnés par une simple procédure administrative d'auto-autorisation.

▪ Confrontés aux difficultés de satisfaire les demandes d'accès à des données morcelées dans plusieurs pays, plusieurs pays ont rapidement affiché leur volonté d'instaurer une coopération transnationale entre Etats souverains. Le principal traité international encadrant les enquêtes criminelles en ligne est la Convention sur la cybercriminalité du Conseil de l'Europe (2001) **(2)**. Ses signataires incluent des Etats aussi bien européens que non européens, comme les USA. Cette Convention vise à lutter contre la cybercriminalité tant sur le plan national qu'international en instaurant une coopération interétatique pour les affaires transfrontières.

▪ En outre, la coopération extrajudiciaire entre les services de police et les prestataires de service est de plus en plus fréquente. En effet, les services de police n'hésitent pas à solliciter la coopération des prestataires directement afin de contourner les complexités liées aux divergences existant entre les différentes lois nationales, ce fut notamment le cas lorsqu'il a été avancé que la société Amazon aurait pris la décision, par ailleurs controversée, de cesser la fourniture de ses services d'hébergement à WikiLeaks, sous la pression du gouvernement américain **(3) (4)**.

▪ Les prestataires de services cloud, qui sont ainsi amenés à se trouver entre le marteau (leurs clients) et l'enclume (les services de police), devraient au minimum envisager de se protéger en amont en se réservant, dans leurs conditions générales de service, le droit de divulguer les données de leurs clients sur demande des services de police, et ce que les données soient stockées sur le cloud par le client personnellement ou générées du fait de l'utilisation des services cloud.

DANNY PREISKEL

▪ ***Focus on Government access to data in the cloud***

▪ *Cloud computing is rapidly becoming the IT solution of choice for many organisations and individuals. Because cloud systems rely on remote rather than local servers, it is easier to access data that is stored online than to retrieve it from a local end user device under a conventional search and seizure process.*

▪ *For this reason, law enforcement agencies (LEAs) are increasingly turning to the cloud to monitor unlawful activity and to gather forensic data. This raises a number of legal conundrums, which pit the conflicting interests of privacy and law enforcement directly against each other.*

(i) online investigations affect a wide range of people, whose legal rights and obligations all need to be considered. Forensic data may be held on systems used by a suspect, a victim or an innocent third party. Obtaining access to the data invariably involves the co-operation (and often the compulsion) of service providers who host remote servers in the cloud, and telecom networks.

(ii) the transnational nature of cloud computing raises jurisdictional difficulties, especially where laws conflict or need to be enforced in different countries.

(iii) the fragmented storage of forensic data in the cloud can make it tricky to retrieve and re-patch together as a coherent whole. Not only could this potentially degrade its evidential value in court, but its retrieval may be complicated if fragments are stored on servers in different countries, or if the location of a host server is unknown. In this context, identifying perpetrators can be challenging if the links between the data and the device from which it originated are obscure, or if the data is encrypted.

*(iv) giving LEAs access to data intrudes upon the right to privacy, which is regarded as a fundamental right in many countries. In Europe, Article 8 of the European Convention on Human Rights guarantees individuals **(1)** the right to a "private and family life". However, this right is not absolute, and may be limited whether this is necessary to protect national security and prevent disorder and crime (amongst other things). Where the right to privacy is restricted, this must be done in accordance with the law, meet a legitimate interest and any measures taken must be necessary and proportionate.*

(1) European Convention on Human Rights

(2) Convention on Cybercrime

(3) Article, "WikiLeaks website pulled by Amazon after US political pressure", The Guardian, 2 December 2010

(4) Amazon message on WikiLeaks

DANNY PREISKEL

▪ *In a growing number of countries, privacy rights are protected by means of specialised data protection legislation – which safeguards individuals and organisations against the unauthorised collection and processing of information that can be used to identify them personally. These initiatives tend to be matched equally by statutory measures which enable LEAs to monitor and intercept the content of online data, as well as information about the transmission of data (such as details of websites accessed or the length and duration of telephone calls). Some countries severely curtail interception without judicial authorisation, whereas others – like the UK – enable LEAs to access subscriber data through a process of administrative self-authorisation.*

▪ *The difficulties associated with requesting access to fragmented data in multiple jurisdictions has prompted a drive towards trans-national cooperation between sovereign states. The principal international treaty which regulates online criminal investigations is the Council of Europe Convention on Cybercrime (2001)* ***(2)****. Signatories include non-European states such as the US. The Convention is aimed at tackling cybercrime both nationally as well as establishing international cooperation for trans-border cases.*

▪ *Extra-judicial co-operation between LEAs and service providers is also becoming more common. LEAs are progressively seeking the co-operation of service providers directly in order to navigate around the complexities of conflicting national laws – as happened when Amazon controversially took the decision to stop providing hosting services to Wikileaks, allegedly under pressure from the US government* ***(3) (4)****.*

▪ *Service providers who find themselves caught between a rock (their customers) and a hard place (LEAs) may wish to at least consider protecting themselves by reserving the contractual right in their business terms to disclose customer data where required by LEAs, regardless of whether the data is stored by the customer personally or generated by their use of the service on the cloud.*

DANNY PREISKEL

▪ La Belgique encadre strictement l'accès des services publics aux données privées hébergées sur des systèmes informatiques. Le principe est la confidentialité et la protection des données et seules quelques lois permettent, selon une procédure bien définie, l'accès aux systèmes informatiques.

▪ En matière de services de renseignement, les pouvoirs de la sûreté de l'état belge sont listés, de manière exhaustive mais très largement libellés, dans la loi organique des services de renseignement et de sécurité du 30 novembre 1998 **(1)**.

▪ Ces pouvoirs sont organisés en trois catégories de plus en plus attentatoires à la vie privée : les méthodes ordinaires (la communication de données recueillies par l'administration, l'usage de sources humaines,…), les méthodes spécifiques (l'observation à l'aide de moyens techniques de lieux publics ou privés accessibles au public,…) et les méthodes exceptionnelles de recueil des données (entrer secrètement dans des lieux privés et y installer des moyens techniques de surveillance,…).

▪ L'emploi de la plupart de ces méthodes ne nécessite qu'une autorisation du chef de service et une notification, mais les plus intrusives doivent être autorisées par un organe administratif spécifique, la Commission.

▪ Il est à noter que les services secrets belges publient, depuis quelques années, un rapport annuel **(2)**. Ce rapport ne contient évidemment aucune information opérationnelle mais donne quelques informations et statistiques sur les méthodes employées.

▪ Les services de renseignement belges n'ont, sous quelques exceptions (comme l'interception de communications émises à l'étranger lors de missions militaires belges) de compétence et de pouvoirs que sur le territoire national. Ils peuvent par contre accéder à des données situées en Belgique mais ne concernant pas leurs ressortissants. Sauf quelques hypothèses limitativement énumérées dans la loi, comme les crimes contre la sûreté de l'Etat, aucune conséquence ne peut toutefois être tirée à l'encontre de ces étrangers si ceux-ci ne sont pas trouvés en Belgique.

JEAN-FRANÇOIS HENROTTE

REFERENCES

(1) Loi organique des services de renseignement et de sécurité du 30 novembre 2008

(2) Par exemple, cf. Rapport annuel 2011

REFERENCES

▪ *Belgium strictly regulates access to private data hosted on computer systems. The principle is the privacy and data protection. Only a few laws allow, according to a well-defined procedure, access to computer systems for public agencies.*

▪ *When it comes to State Security, Intelligence Services have a very wide range of powers and a great freedom in how to use it. These powers are listed in the Intelligence services Act of 1998. This list is exhaustive but so broad that it probably covers all possibilities.*

▪ *These powers are organized into three categories increasingly intrusive: ordinary methods (communication of data collected by the administration, ...), specific methods (observation by technical means,...) and special methods of data collection (infiltration,…).*

▪ *Most of the measures only need to be authorized by the head of department and notified to a regulatory body called the Commission. The most intrusive measures (wiretapping, hacking, infiltration ...) must be authorized by the Commission.*

▪ *It is noteworthy that Belgian secret service published, for the last few years, an annual report **(2)**. This report obviously contains no operational information but gives some data and statistics on methods used by the service.*

▪ *Belgian intelligence services have, under some exceptions (such as interception of communications issued abroad during Belgian military missions), jurisdiction and powers only on the national territory. But they can access to data located in Belgium which doesn't concern their nationals. However, except for a few cases exhaustively listed in the law, such as crimes against the security of the State, no proceedings may be brought against the foreigners if they are not found in Belgium.*

(1) Loi organique des services de renseignement et de sécurité du 30 novembre 2008

(2) For example, see 2011 Annual Report

JEAN-FRANÇOIS HENROTTE

▪ Dans la foulée des attaques terroristes survenues sur le territoire américain, le parlement canadien a adopté en décembre 2001, la Loi antiterroriste **(1)**, ayant pour effet d'entraîner des modifications à plusieurs lois dont le Code criminel de façon à élargir la portée des pouvoirs accordés aux autorités gouvernementales aux fins de protéger la sécurité nationale.

▪ Différentes lois canadiennes accordent aujourd'hui des droits d'interception et de saisie aux autorités gouvernementales canadiennes :

- Code criminel
- Loi sur le Service canadien du renseignement de sécurité **(2)**
- Loi sur la protection de l'information
- Loi sur la défense nationale
- Loi sur l'entraide juridique en matière criminelle
- Projet de Loi C-30 – Loi édictant la loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le code criminel et d'autres lois **(3)**

▪ La Loi sur le Service canadien du renseignement de sécurité **(4)** et la Loi sur la défense nationale **(5)** contiennent des dispositions qui prévoient la possibilité pour un juge de la Cour fédérale du Canada d'émettre sur demande présentée ex parte et à huis clos, un mandat autorisant l'interception de communications, et l'obtention d'informations. La loi prévoit par ailleurs la possibilité pour le juge d'ajouter au mandat les conditions qu'il estime indiquées dans l'intérêt public, ce qui inclut vraisemblablement de façon générale des ordonnances de non-divulgation destinées aux personnes dont la coopération est requise dans le cadre de l'exécution du mandat, tel qu'un fournisseur de télécommunication.

▪ Par ailleurs, la Loi sur la défense nationale (art 273.65) prévoit que le ministre de la Défense nationale peut autoriser le Centre de la sécurité des télécommunications à intercepter des communications privées (impliquant des entités étrangères) liées à une activité ou une catégorie d'activités qu'il mentionne expressément. Le ministre peut également autoriser l'interception de communications privées au sens du Code criminel afin de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada.

▪ Le Code criminel **(6)** dont les dispositions ont été modifiées par la Loi antiterroriste en 2001 (art. 83.01 et suiv.) prévoit la possibilité pour le procureur général de présenter ex parte et à huis clos à un

(1), Loi modifiant le Code criminel, la Loi sur les secrets officiels, la Loi sur la preuve au Canada, la Loi sur le recyclage des produits de la criminalité et d'autres lois, et édictant des mesures à l'égard de l'enregistrement des organismes de bienfaisance, en vue de combattre le terrorisme L.C. 2001, ch. 41 (la « Loi antiterroriste »).

(2) Security of information Act

(2) Le Projet de loi C-30 visait à introduire des dispositions relatives à « l'accès légal », soit l'interception de communications privées et la saisie d'information par les organismes chargés de la sécurité nationale ou du contrôle d'application des lois et ce, sans nécessité d'autorisation judiciaire. Il appert que le ministre de la Justice ait décidé de ne pas en poursuivre l'étude et de le laisser mourir au feuilleton de la Chambre des communes

(4) Loi sur le Service canadien du renseignement de sécurité

(5) Loi sur la défense nationale

(6) Code criminel

juge de la Cour fédérale une demande en vue de l'émission d'un mandat de confiscation dans le cadre d'enquête anti-terroristes. Des articles du Code criminel accordent des par ailleurs des droits d'interception de communications (184.4/185), de fouille et de saisie de données (487(2.1)), d'émission d'ordonnance de communication de documents (487.012) et d'assistance (487.02).

▪ De façon générale, l'exercice des pouvoirs d'accès est assujetti à l'obtention d'une autorisation et nécessite une preuve par affidavit de motifs raisonnables indicatifs de la commission, ou d'un risque de commission d'une infraction, une description des démarches d'enquête effectuées et la portée de l'interception ou de la perquisition pour laquelle une autorisation est recherchée.

▪ Le Canada a également adopté une Loi sur l'entraide juridique en matière criminelle **(7)** afin de mettre en œuvre les engagements souscrits aux termes de traités. Le ministre de la Justice peut autoriser un état étranger et, le cas échéant, l'assister aux fins de présenter une requête de mandat pour fouille, saisie, perquisition, ou obtention d'éléments de preuve. Dans une affaire récente, le procureur général du Canada a demandé et obtenu, pour et au nom du gouvernement des États-Unis, un mandat de saisie visant des serveurs informatiques appartenant à un fournisseur canadien de services d'infonuagique (Equinix) qui auraient été utilisés dans le cadre des activités de Megaupload Ltd. **(8)**, laquelle fait l'objet de poursuites aux États-Unis.

▪ Les seules données publiques relatives à l'exercice des pouvoirs d'accès extraordinaires accordés aux gouvernements canadien et américain aux termes des lois relatives à la sécurité nationale sont de nature quantitative. Les données publiées ne fournissent aucun éclairage sur les personnes et documents visés, ni sur la nature des enquêtes dans le cadre desquelles des communications et des documents sont interceptés, fouillés ou perquisitionnés. Il n'est donc pas possible d'apprécier le type d'usage qui en est effectivement fait.

(7) Loi sur l'entraide juridique en matière criminelle L.R.C. (1985), ch. 30 (4e suppl.)

(4) Megaupload Inc. v. Attorney General of Canada, 2012 ONSC 6331; Canada (United States of America) v. Equinix Inc., 2013 ONSC 193 (CanLII). La saisie a été effectuée en janvier 2012 et la plus récente décision fait état du débat qui a cours sur l'étendue des données qui devront être communiquées.

JEAN-FRANÇOIS DE RICO

REFERENCES

▪ *In the wake of the terrorist attacks on the US soil, the Canadian Parliament adopted in December 2001 the Anti-terrorism Act* ***(1)*** *(amending several laws, including the Criminal Code so as to extend the scope granted to governmental authorities in order to protect national security.*

▪ *A number of Canadian laws now grant interception and seizure powers to Canadian governmental authorities:*

- *Criminal Code*
- *Canadian Security Intelligence Service Act*
- *Security of information Act* ***(2)***
- *National Defense Act*
- *Mutual Legal Assistance in Criminal Matters Act*
- *Bill C-30 - An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts* ***(3)***

▪ *The Canadian Security Intelligence Service Act* ***(4)*** *and the National Defense Act* ***(5)*** *include provisions for a judge of the of the Federal Court, on ex parte application heard in private, to issue a warrant authorizing the interception of communications and the obtaining of information. It is also provided that a judge may, if the judge thinks fit, add to the warrant such terms and conditions as the judge considers advisable in the public interest, which will typically generally include non-disclosure orders for individuals whose cooperation is required for the enforcement of the warrant, such as a telecommunications provider.*

▪ *The National Defense Act (Art 273.65) further provides that the Minister of National Defence may authorize the Communications Security Establishment to intercept private communications (involving foreign entities) in relation to an activity or class of activities specified in the authorization. The Minister may also authorize the interception of private communications within the meaning of the Criminal Code for the purpose of protecting the computer systems or networks of the Government of Canada.*

▪ *The Criminal Code* ***(6)****, which has been amended by the Anti-terrorism Act in 2001, (Art. 83.01 et seq.) provides the possibility for the Attorney General to make an ex parte application examined in private by the Federal Court for the issuance of an order of forfeiture in the course of an anti-terrorism investigation. Articles from the Criminal Code further grant powers to intercept communications (184.4/185), search and seize data (482(2.1)), issue an order to produce documents and an assistance order.*

(1), An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism L.C. 2001, ch. 41 (Anti-terrorism Act)

(2) Security of information Act

(3) Bill C-30 . The Bill C-30 aimed at introducing provisions on "lawful access", i.e. the interception of private communications and the seizure of information by national security and law enforcement agencies without requiring a judicial authorization. It appears that the Minister of Justice decided not to continue the review of such Bill and let it die on the order paper of the House of Commons of Canada.

(4) Canadian Security Intelligence Service Act

(5) National Defense Act

(6) Criminal Code

▪ *Generally, the exercise of powers of access is subject to the grant of an authorization and requires proof by affidavit that there are reasonable grounds to believe that an offence has been committed or risked to be committed. A description of the investigative steps taken and the scope of the interception or search for which an authorization is requested.*

▪ *Canada has also adopted a Mutual Legal Assistance in Criminal Matters Act* ***(7)*** *to enforce the commitments made under various treaties. The Minister of Dense may authorize a foreign state and, where applicable, assist it to apply for a warrant to search, seize, or obtain elements of proof. In a recent case, the attorney general of Canada requested and obtained, for and on behalf of the US government, a seizure warrant for the computer servers belonging to a Canadian provider of cloud services (Equinix) that would have been used for the activities of Megaupload Ltd* ***(8)*** *which was sue din the US.*

▪ *The only public data relating to the exercise of the extraordinary powers to access granted to the Canadian and US governments under laws related to national security are quantitative. The data published provides no information on the individuals and documents concerned or on the nature of the investigations in the course of which communications and documents are intercepted, seized or searched. It is therefore impossible to assess the type of use actually made of the same.*

(7) Mutual Legal Assistance in Criminal Matters Act L.R.C. (1985), ch. 30 (4e suppl.)

(8) Megaupload Inc. v. Attorney General of Canada, 2012 ONSC 6331; Canada (United States of America) v. Equinix Inc., 2013 ONSC 193 (CanLII). The seizure was made in January 2012 and the most recent decision deals with the ongoing debate on the scope of the data to be communicated.

JEAN-FRANÇOIS DE RICO

JADE & FOUNTAIN PRC LAWYERS

▪ La Constitution de la République populaire de Chine **(1)** pose le principe selon lequel la liberté et le secret des correspondances d'une personne sont protégées par la loi contre toute violation illégale. Il peut toutefois être dérogé à ce principe pour des raisons de sécurité de l'Etat ou d'enquêtes criminelles nécessitant un contrôle des correspondances par les services de la sécurité publique ou le ministère public, dans le respect des procédures établies à cette fin.

▪ En ce qui concerne l'Internet, des prérogatives importantes ont été accordées à l'Etat au nom de la protection de la sécurité de l'information afin de censurer les contenus « illégaux et illicites » et d'enquêter sur les activités criminelles. Ainsi, aux termes de l'article 14 du règlement sur les services d'information Internet de la RPC (2000) **(2)** « *Un prestataire de services d'information Internet fournissant des services d'actualités, de publication, ou de bulletin d'information électronique est tenu de conserver les données fournies, l'heure de publication et l'adresse du nom de domaine. Un fournisseur de services de connexion Internet est tenu de conserver les données suivantes relatives aux utilisateurs en ligne : l'heure de connexion, les comptes, l'adresse Internet ou le nom de domaine ainsi que le numéro de téléphone de l'appelant. Le prestataire de services d'information Internet et le fournisseur d'accès Internet conservent ces données pendant une période de 60 jours et les communiquent aux autorités compétentes si nécessaire pour des besoins d'enquête* ». Ce texte impose donc l'enregistrement et la conservation de données relatives à plusieurs secteurs de l'Internet et accorde à différents services de l'Etat des droits d'accès aux données stockées.

▪ De manière générale, l'accès de l'Etat aux données est consacré par le « Bouclier doré » **(3)**, également connu sous l'expression « Grande muraille pare-feu de Chine » ou « Grand Firewall de Chine ». Il s'agit d'un programme de censure et de surveillance érigé et piloté par le Ministère de la sécurité publique (« MPS ») du gouvernement chinois. Ce projet, lancé en 1998, est opérationnel depuis novembre 2003. Le Bouclier d'or est se présente comme un système ayant davantage vocation à veiller au maintien de l'ordre de la police qu'au maintien de l'ordre d'Internet, dans divers domaines tels que la sécurité sociale, les impôts, les finances, l'agriculture, les douanes, le contrôle des finances publiques…. Ce projet a en effet permis d'établir des normes et des pratiques informatiques communes dans l'ensemble des ministères, ainsi qu'un réseau public de système de surveillance de sécurité.

▪ Le projet Bouclier doré s'inscrit dans le cadre de la construction d'un e-gouvernement reposant sur les bases établies en 2002 par les lignes directrices sur la construction d'un e-gouvernement par le groupe d'information de l'Etat **(3)**. Ce e-gouvernement comprend 4 bases de données, dont la Base de données Internet de référence coordonnée par le MPS. Cette base de données rassemble et compile des données des FAI, des fournisseurs de contenus, des prestataires de bases de données et des services de messageries électroniques tous les mois depuis 2006. Les données collectées incluent toutes les informations sur tous les comptes et les abonnements des utilisateurs, personnes physiques et morales.

REFERENCES

(1) Constitution de la République populaire de Chine

(2) Regulation on Internet Information Service of the People's Republic of China (2000)

(3) Page Wikipedia, "Grand Firewall de Chine"

(4) Guiding Opinion on Construction of E-Government by the State Information Leading Group" (2002)

JUN YANG

▪ *Although the Chinese Constitution Law* ***(1)*** *prescribes that the freedom and secrecy of correspondences of a person are protected by law from "unlawful" infringements, the exceptions are made to meet the needs of state security or of criminal investigation when public security or prosecutorial organs are permitted to censor correspondence in accordance with the certain procedures.*

▪ *As to internet related laws, extensive rights have been given in the name of information security protection to censor "illegal and harmful" content and to investigate criminal activities. For instance, according to Article 14 of the Regulation on Internet Information Service of the People's Republic of China (2000)* ***(2)****, "*An Internet information service provider engaged in news, publication, or electronic bulletin board services shall keep records of the information provided, time of publishing and the Internet address or domain name. An Internet connection service provider shall keep records of the online users' connection time, accounts, Internet address or domain name, and the calling party's telephone number. The backup records of the Internet information service provider and the Internet access service provider shall be kept for 60 days, and shall be provided to the relevant authorities for inquiry purposes if so required*". This law requires data record relating to many internet related businesses and grants right of access to the data retained to many government departments.*

▪ *The government's access to data has been collectively embodied in the Golden Shield Project, which is also known as the "Great Firewall of China"* ***(3)****, it is a censorship and surveillance project operated by the Ministry of Public Security (MPS) of the Chinese government. The project was initiated in 1998 and began operations in November 2003. Golden Shield is better described as an effort to network the police, rather than police the network, covering the social security, tax collection, financial industry, agriculture, customs, government auditing, and so on. By this project, ministry-wide IT standards and practices, as well as public network security monitoring system has been established.*

▪ *The Golden Shield Project is part of construction of e-government based on a framework set up as per the "Guiding Opinion on Construction of E-Government by the State Information Leading Group" (2002)* ***(4)****. E-government includes 4 databases, one of them is Basic Internet Database coordinated by the MPS. The Basic Internet Database collected data from ISPs, ICPs, and IDCs and email services monthly since 2006. The data collected include all users' account and registration information, both individual and corporate.*

REFERENCES

(1) Constitution de la République populaire de Chine

(2) Regulation on Internet Information Service of the People's Republic of China (2000)

(3) Wikipedia Page, "Golden Shield Project"

(4) Guiding Opinion on Construction of E-Government by the State Information Leading Group" (2002)

JUN YANG

▪ Dans le monde moderne, l'interception des communications à des fins de défense se traduit avant tout par la possibilité pour l'Etat d'anticiper et, bien souvent, de contrecarrer la cybercriminalité. L'accès par les autorités aux données est une pratique ancienne et le présent article limitera ici son analyse aux accès destinés : (i) aux services de renseignement et (ii) aux autorités judiciaires.

▪ La croissance et la sophistication permanentes des infractions transfrontières ont justifié la naissance de nouveaux types d'outils de contrôle permettant de les endiguer. Ces cinq dernières années ont ainsi conduit à l'adoption par de nombreux pays d'une série de mesures destinées à répondre au phénomène de la cybercriminalité. La Colombie a elle aussi développé des stratégies dans ce domaine. En outre, au niveau judiciaire, ces mesures sont accompagnées de programmes destinés à harmoniser les pratiques au niveau mondial.

▪ Dans le document CONPES 3701 / 2011 **(1)**, la Colombie a définie une stratégie de cybersécurité et introduit une réglementation pour encadrer les enquêtes de cybercriminalité. Dans le même esprit, depuis 2000 et la réforme du code pénal et du code de procédure pénale colombien, des travaux ont été entrepris afin de doter le pouvoir judiciaire de nouveaux mécanismes afin de faciliter l'obtention de preuves et le déroulement des enquêtes criminelles. En 2005, la Colombie avait ainsi adopté un nouveau système de poursuites pénales de type accusatoire, qui instaure davantage d'agences spécialisées (police judiciaire), un système basé sur l'oralité et l'intervention de juges permet de garantir une fonction de contrôle.

▪ Ce dispositif a récemment été complété par la nouvelle loi sur les services de renseignements nationaux : la Statutory Act 1621 de 2013 **(2)**, dont la mouture précédente, la loi 1288 de 2009 **(3)** a été déclarée inconstitutionnelle par la Cour constitutionnelle. A cette occasion, la Cour constitutionnelle avait procédé à une analyse approfondie du texte et constaté la violation de certains droits, tels que le droit à la vie privée, par différentes autorités.

▪ Il convient de noter que la Colombie a adopté des règles imposant aux fournisseurs de services de communications d'autoriser le ministère public à traiter (c'est-à-dire analyser, capturer et détenir) des informations sur les réseaux de communications. En particulier, le décret 1704 de 2012 **(4)** impose aux opérateurs et prestataires de services de communication de coopérer avec les autorités afin de leur permettre d'accéder au flux de données de communication réalisés sur leurs réseaux.

▪ Par ailleurs, dans le cadre de la coopération judiciaire internationale, la Colombie est signataire de traités d'assistance mutuelle permettant de coopérer sur des questions de cybercriminalité transnationale et d'enquêtes criminelles mondiales.

▪ Enfin, tout récemment a été lancé le programme « PUMA »(« Plataforma Única de Análisis y Monitoreo » ou « Single Platform Monitoring and Analysis »), analogue au programme PRISM des Etats-Unis. Il s'agit d'un système informatique robuste capable de surveiller 20 000 moyens de télécommunications, sur la base d'autorisations légales émises par les autorités compétentes. Plusieurs voix se sont élevées contre cet outil des récentes affaires de violations de la vie privée qui ont ébranlées la Colombie, impliquant l'interception par les services de renseignements colombiens des communications de nombreuses personnalités (appartenant presque toutes à des groupes d'opposition politique et au secteur judiciaire), créant un énorme scandale non encore apaisé aujourd'hui. C'est la raison pour laquelle, le programme PUMA créé un large débat.

REFERENCES

(1) Document CONPES 3701/2011

(2) Ley 1621 de 2013

(3) Ley 1288 de 2009

(4) Decreto 1704 de 2012

IVAN DARIO MARRUGO JIMENEZ

▪ *The interception of communications for defense has been understood under the winds that move the modern world, as the ability of the state to anticipate and often counter the effects of cybercrime. While this is a much older practice, for the purpose of our discussion we will assume that the access data hosted online by the authorities may in principle have two purposes: 1. Intelligence Work. Two. Connotations in a judicial proceeding.*

▪ *Clearly, the continued growth and modernization of transnational crimes have justified the birth of a new type of tools by the states to cope. The last five years has led to the adoption of a series of measures aimed at establishing patterns of response to the phenomenon of computer crime. Colombia has not been immune to this reality. Thus, the country is developing strategies in this area. Also at the judicial level these measures are accompanied with plans to put the country in line with current conditions in the globalized world.*

▪ *In particular from the document CONPES 3701 / 2011* ***(1)*** *the country defined a Cyber and Cyber security strategy and introduced the need for articulating program efforts in the investigation of cybercrimes. Likewise, and since 2000 on the occasion of the Colombian penal code reform and criminal procedure began work to provide the judicial branch of new mechanisms at both the level of evidence as criminal investigation. So it was that in 2005 Colombia adopted a new system of criminal prosecution called accusatorial system. This work introduced a new system with more specialized technical agencies (Judicial Police), a system based on orality and the intervention of judges guarantees control function.*

▪ *To complement the work undertaken by the authorities in criminal investigations and intelligence work recently issued a new law on national intelligence: Statutory Act 1621 of 2013* ***(2)****, whose closest antecedent Law 1288 of 2009* ***(3)*** *had been declared unconstitutional by the Constitutional Court in its formation defects. Also the constitutional court then made a detailed analysis of the violation of rights such as privacy in certain authorities granted mechanisms.*

▪ *It is also important to note that Colombia has adopted rules requiring providers of communications services by prosecutors to allow processing (analyze, capture and hold) of information in communication networks by organizations. In particular, the Decree 1704 of 2012* ***(4)*** *makes it mandatory for operators and communications service providers provide cooperation with the authorities to gain access to the capture of communications traffic that course through their networks.*

▪ *Moreover, in international judicial cooperation Colombia is part of the mutual assistance treaties in order to participate cooperatively on issues of transnational crime and global criminal investigations.*

▪ *Finally has drawn attention in recent weeks the launch of a program called Single Platform Monitoring and Analysis - PUMA,* ***(5)*** *which saves quite closely with U.S. government PRISM. It is a robust computer system capable of monitoring 20,000 telecommunications means, according to legal orders issued by the competent authorities. Different voices of rejection have been raised against such tools as the country has a serious precedent regarding violation of individual privacy when in a dark episode intelligence agencies intercepted communications for a significant number of personalities (almost all belonging to opposition political groups and magistrates) generating a large-scale scandal that even today has failed to be resolved. Due to the above the platform to develop as indicated will not be free to generate a series of discussions that have serious reasons for doubt not only because of impunity in the cases mentioned, it because they seem to be part of a state policy.*

REFERENCES

(1) Document CONPES 3701/2011

(2) Ley 1621 de 2013

(3) Ley 1288 de 2009

(4) Decreto 1704 de 2012

IVAN DARIO MARRUGO JIMENEZ

▪ En France, en matière criminelle, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques.

▪ Pour réaliser sa mission, le juge d'instruction dispose de pouvoirs étendus, et notamment du pouvoir de décider de procéder à des opérations de perquisition et de saisie de preuves **(1)**, et d'ordonner des interceptions **(2)**.

▪ Immédiatement après les attentats du 11 Septembre 2001, la France a en effet adopté la loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne **(3)**, qui a considérablement renforcé les pouvoirs des services de police français **(4)**. En sus des prérogatives des autorités judiciaires, l'article 6 de la loi 2006-64 a inséré un article L34-1-1 dans le code des postes et des communications électroniques, et modifié l'article 6 II de la loi 2004-575 autorisant les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions à exiger des opérateurs de télécommunications et des prestataires internet la communication des données conservées et traitées par ces derniers afin de prévenir les actes de terrorisme.

▪ Les autorités sont donc dotées de pouvoirs accrus en matière de surveillance électronique dans le cadre des enquêtes intéressant le terrorisme, la sécurité nationale et d'autres infractions graves.

▪ Un tribunal peut ainsi autoriser l'interception et l'enregistrement de communications électroniques, même au stade de l'enquête préliminaire, si les besoins de l'enquête le justifient. En revanche, pour les « interceptions de sécurité », aucune ordonnance du tribunal n'est requise. Les fournisseurs de prestations de cryptologie sont également tenus, sous certaines conditions, de remettre aux agents autorisés les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'ils fournissent.

▪ En outre, l'article L450-4 du code de commerce autorise l'Autorité de la concurrence à visiter les locaux d'une entreprise suspectée de pratiques anticoncurrentielles et de saisir tous les documents et supports d'information utiles aux besoins de l'enquête. Le 30 novembre 2011, la cour de cassation **(5)** a confirmé une arrêt qui avait décidé que les opérations de visite et de saisie réalisées dans le cadre d'enquêtes conduites par l'Autorité de la concurrence échappaient aux dispositions de la loi informatique et libertés aux motifs que ces opérations avaient été dûment autorisées par le juge des libertés et de la détention. En l'espèce, la cour a constaté que les agents avaient été autorisés par la loi à saisir des correspondances privées dans le cadre de leur enquête et que par conséquent l'examen par eux de courriers électroniques ne constituait pas une violation du secret des correspondances.

▪ S'agissant de la surveillance électronique, la loi de 1991 requiert l'autorisation du juge d'instruction avant toute installation d'un dispositif d'écoute. La durée de l'écoute est limitée à une période quatre mois, qui peut être renouvelée **(6)**. Cette même loi a également institué une commission nationale de contrôle des interceptions de sécurité (CNCIS), dont la mission est de veiller au respect des dispositions relatives aux interceptions et de formuler des avis **(7)**. Elle publie chaque année un rapport public **(8)**.

▪ Par ailleurs, à l'automne 2007, le parlement français a adopté une loi établissant une délégation parlementaire au renseignement (DPR) **(9)** qui a pour mission de « suivre l'activité générale et les moyens des services

REFERENCES

(1) Code de procédure pénale, articles 92 à 99-411

(2) Code de procédure pénale, art. 100 à 100-7,

(3) Loi 2001-1062 du 15-11-2001 relative à la sécurité quotidienne

(4) Par exemple un procureur, un officier de police judiciaire ou un juge d'instruction

(5) Cass. crim. 30-11-2011

(6) Loi 91-646 du 10-7-1991 relative au secret des correspondances émises par la voie des communications électroniques

(7) Aux termes de l'article 6 de Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, the CNCIS exerce un contrôle sur les demandes de communication de données prévues par l'article L 34-1-1 du code des postes et des communications électroniques

(8) Par exemple, en 2011, les services de police ont réalisé 6 396 interceptions: dont 4 156 nouvelles interceptions et .2 240 renouvellements, représentant une augmentation de 6 % en 2019. Le nombre d'interceptions demandées en urgence absolue ont augmenté de près de 5 % en 2011,. Cf. Commission nationale de contrôle des interceptions de sécurité, 20e rapport d'activité 2011.

spécialisés », donnant ainsi aux services de renseignement français une nouvelle légitimité tout en préservant la confidentialité de leurs actions. En dépit des nouveautés introduites par la loi, le texte n'en reste pas moins une première étape modeste : la DPR n'aura aucun moyen d'exercer un réel contrôle sur les services et son rôle sera davantage symbolique **(10)**. Aucun publication de rapport incluant des statistiques détaillées sur les interceptions ou des écoutes réalisées n'est prévu.

▪ Lorsqu'il existe une suspicion d'actes illicites commis au niveau international, il convient de noter que l'application de la loi française s'étend à l'étranger car le droit française permet expressément aux autorités françaises d'obtenir toutes les informations utiles à une enquête, comme par exemple les données stockées au sein d'un système informatique, pour autant que ces données soient accessibles à partir de ce système informatique. Aussi, l'Etat français peut demander à un opérateur de télécommunications ou un prestataire de services cloud de lui fournir les données de réseaux ou de serveurs nationaux ou internationaux en appliquant la procédure judiciaire décrite précédemment.

▪ La situation inverse peut également se présenter, lorsque les services de police situés à l'étranger demandent aux autorités françaises de leur communiquer des données relatives à des sociétés basées en France.

▪ De manière générale, un procureur ou enquêteur étranger n'est pas autorisé à mener une enquête ou à auditionner des témoins sur le territoire français. Dans la plupart des cas, l'assistance des autorités françaises sera par conséquent nécessaire. A cette fin, au fil des ans, la France a signé plusieurs traités internationaux qui autorisent les autorités étrangères des Etats parties auxdits traités à demander l'accès aux données stockées sur les serveurs d'un prestataire de services cloud physiquement situés sur le territoire des Etats concernés ou sont assujettis aux lois de ces Etats.

▪ Par exemple, en vertu de l'accord d'entraide judiciaire conclu entre les Etats-Unis et les Etats Membres de l'UE, dont la France, une demande d'entraide portant sur la communication de données ne peut être refusée pour des motifs liés à la protection des données que dans des « cas exceptionnels ». **(11)**

▪ Autrement dit, la grande majorité des demandes de données effectuées dans le cadre d'un traité d'entraide judiciaire seront honorées par l'Etat requis.

▪ De plus, aux termes de l'article 13(3) de la décision cadre 2008/977/JAI du Conseil de l'UE **(12)** les données à caractère personnel peuvent être transférées lorsque cela est nécessaire à des fins d'enquête, même dans des pays qui n'assurent pas un niveau de protection adéquat pour le traitement de données envisagé lorsque sont prévues des « garanties appropriées ». L'expression « garanties appropriées » est interprétée de manière large afin d'inclure les conventions internationales telles que traités d'entraide judiciaire (TEJ, ou en anglais MLAT).

▪ Enfin, la France a ratifié la convention sur la cybercriminalité du Conseil de l'Europe **(13)**. Cette convention, qui traite de la criminalité informatique, instaure également un système d'entraide entre services de police étrangers afin de recueillir et partager les preuves sous forme électronique de différents types d'infractions, y compris par l'assistance des banques, FAI et autres prestataires détenant des informations pouvant être utiles aux services de police.

(9) Loi 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement

(10) Cf. M. le Sénateur Jean-Louis Carrère, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2011, Assemblée nationale et Sénat, 17-7-2012

(11) Article 9(2)(b) de l'Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire 19-7-2003

(12) Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

(13) Convention sur la cybercriminalité

FREDERIC FORSTER

▪ *In France to proceed to criminal investigations, a judge may order the interception, recording, and transcription of electronic communications where the requirements of the investigation call for it.*

▪ *To perform his mission, the investigating judge is given extensive powers that include the right to order a search for and seizure of evidence* ***(1)****, and the right to order a wiretap* ***(2)****.*

▪ *In the immediate aftermath of the 9/11 terrorist attacks, France adopted the Act No 2001-1062 of 15 November 2001 on day-to-day security* ***(3)****, significantly strengthening the powers of French law enforcement agencies* ***(4)****. In addition to the prerogatives of the judicial authorities, Article 6 of the French Act No 2006-64 inserted Article L 34-1-1 in the French Code of Post and Electronic Communications and modified Article 6 II of the Act No 2004-575 in order to authorize, for the purpose of preventing acts of terrorism, agents individually designated and duly empowered from the police services to request communication of any of the aforementioned data retained by telecom operators or internet providers.*

▪ *Thus, for investigations into terrorism, national security, and other serious crimes, governmental authorities are provided with expanded electronic surveillance capabilities.*

▪ *A court may authorize the interception and recording of electronic communications during even the preliminary stage of an investigation if justified by the needs of the investigation. For so-called "security interceptions," no court order is required. Providers of encryption services are also required to hand over encryption keys to government officials under certain conditions.*

▪ *Moreover, Article L 450-4 of the French Code of Commerce grants the French Competition Authority ("Autorité de la concurrence") the power to inspect the premises of a company suspected of anti-competitive practices and to search and seize all company documents and information that may be relevant to an investigation. On November 30, 2011, the French Court of Cassation* ***(5)*** *upheld a decision that excluded the application of the French Data Protection Act ("loi relative à l'informatique, aux fichiers et aux libertés") to an investigation conducted by the Competition Authority on the grounds that the search and seizure was authorized by a "freedoms and custody judge" ("juge des libertés et de la detention"). In this case, the Court ruled that the agents were authorized by law to include private correspondence if it was relevant to the investigation, and thus their review of the emails did not constitute a violation of correspondence secrecy rights.*

▪ *As far as electronic surveillance is concerned, the French 1991 Act requires permission of an investigating judge before a wiretap is installed. The duration of the tap is limited to four months and can be renewed.****(6)*** *This Act created a national commission controlling security wiretaps ("Commission nationale de contrôle des interceptions de sécurité", or CNCIS), which sets rules and reviews wiretaps* ***(7)****, and publishes public reports each year* ***(8)****.*

REFERENCES

(1) Code of criminal procedure, arts 92 to 99-411

(2) Code of criminal procedure, arts. 100 to 100-7,

(3) Loi 2001-1062 du 15-11-2001 relative à la sécurité quotidienne

(4) E.g., a public prosecutor, a judicial police officer or an investigating judge

(5) Cass. crim. 30-11-2011

(6) Loi 91-646 du 10-7-1991 relative au secret des correspondances émises par la voie des communications électroniques

(7) Under Article 6 of the Act No. 2006-64 of 23 January 2006 on the fight against terrorism, the CNCIS is responsible for checking the data transmission requests set out in Article L 34-1-1 of the French Code of Post and Electronic Communications

(8) For instance, in 2011, law enforcement conducted 6 396 interceptions: 4.156 new interceptions and 2 240 renewals. This represents a 6 percent increase over 2019. There was a 5 percent increase in 2011 in emergency interception requests ("interceptions demandées en urgence absolue"):. Cf. Commission nationale de contrôle des interceptions de sécurité, 20e rapport d'activité 2011.

▪ *Moreover, in fall 2007, the French Parliament passed a law establishing a parliamentary intelligence committee ("Délégation parlementaire au renseignement", DPR), **(9)** whose purpose is to allow members of the National Assembly and senators to "follow the general activity and the means of the specialized services", thus helping the French intelligence services to gain greater recognition while preserving the confidentiality of their actions. Despite what this new law introduced, this text is a modest first step: the DPR will not have the means to exercise real control over the services and its role will be rather symbolic. **(10)** and there isn't any publication of any report detailing the statistics of authorized interceptions or wiretaps realized.*

▪ *When international suspicion of illegal acts is concerned, it has to be taken in consideration that the application of French regulation extends abroad as French law expressly permits governmental authorities to obtain all information relevant to an investigation, for instance from a computer system so long as the data are accessible from that computer system. Therefore, the French government can require a telecom operator or a Cloud service provider to obtain data from both domestic and foreign networks or servers through the preceding described legal mechanisms.*

▪ *The opposite situation could be also encountered, as in France based companies should also raise the question of the possibility of a transmission to investigation agencies located abroad.*

▪ *Generally, a foreign prosecutor or investigator will not be permitted to conduct an investigation or to interview witnesses in France. In most cases, the help of the French government will be necessary. To this end, over the years, France has agreed on a variety of international treaties that allow foreign governmental authorities to request access to data stored on the servers of a Cloud service provider physically located in or subject to the jurisdiction of the foreign nation.*

▪ *For example, pursuant to the agreement governing mutual legal assistance between the U.S. and EU member states, including France, a request for data shall only be denied on data protection grounds in "exceptional cases".**(11)***

▪ *That is, most mutual legal assistance treaty (MLAT) requests for data will be honored by the recipient party.*

▪ *Moreover, Article 13(3) of Framework Decision 2008/977/JHA of the Council of the European Union **(12)** allows transfers of personal data for law enforcement purposes even to countries whose privacy regimes have not been found "adequate" by the EU where there are "appropriate safeguards." The phrase "appropriate safeguards" is widely interpreted to include international agreements such as MLATs.*

▪ *In addition, France ratified the Council of Europe Convention on Cybercrime **(13)**, which not only deals with computer-related crime, but also provides for mutual assistance to foreign police agencies in gathering and sharing electronic evidence of any kind of crime, including mutual assistance to be provided by banks, Internet service providers, and other businesses holding information of interest to law enforcement*.

9) Loi 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement

(10) Cf. M. le Sénateur Jean-Louis Carrère, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2011, Assemblée nationale et Sénat, 17-7-2012

(11) Article 9(2)(b) of the Agreement on mutual legal assistance between the European Union and the United States of America 19-7-2003

(12) Council Framework Decision 2008/977/JHA of 2711-2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

(13) Convention on Cybercrime

FREDERIC FORSTER

PAYS / COUNTRY	CABINET/ FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons Attorneys	Lance Michalson John Giles	+27 (0) 21 300 1070	lance@michalsons.co.za john@michalsons.co.za
Allemagne *Germany*	Buse Heberer Fromm	Bernd Reinmüller Tim Caesar	+ 49 69 971097100	reinmueller@buse.de caesar@buse.de
Angleterre *UK*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	dpreiskel@preiskel.com
Argentine *Argentina*	Estudio Millé	Antonio Millé Rosario Millé	+ 54 11 5297 7000	antonio@mille.com.ar rosario@mille.com.ar
Belgique *Belgium*	Philippe & Partners	Jean-François Henrotte	+ 32 4 229 20 10	jfhenrotte@philippelaw.eu
Brésil *Brazil*	Melchior, Micheletti e Amendoeira Advogados	Silvia Regina Barbuy Melchior	+ 55 113 8451511	melchior@mmalaw.com.br
Canada *Canada*	Langlois Kronström Desjardins	Jean-François De Rico	+1 418 650 7923	jean-francois.derico@lk
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	jun.yang@jadefountain.com
Colombie *Colombia*	Marrugo Rivera & Asociados	Ivan Dario Marrugo Jimenez	+57 1 4760798	imarrugo@marrugorivera.com
Espagne *Spain*	Alliant Abogados	Marc Gallardo	+ 34093 265 58 42	marc.gallardo@alliantabogados.com
Etats-Unis *USA*	IT Law Group	Françoise Gilbert	+ 1 (650) 804 1235	fgilbert@itlawgroup.com
France *France*	Alain Bensoussan-Avocats	Alain Bensoussan	+33 1 41 33 35 35	paris@alain-bensoussan.com
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	central@balpel.gr
Israël *Israel*	Livnat, Mayer & Co.	Russell D. Mayer	+972 2 679 9533	mayer@lmf.co.il
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	r.zallone@studiozallone.it
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	info@kouatlylaw.com
Luxembourg *Luxembourg*	Philippe & Partners	Jean-François Henrotte	+ 32 4 229 20 10	jfhenrotte@philippelaw.eu
Maroc *Morocco*	Bassamat & associée	Bassamat Fassi-Fihri Zineb Laraqui	+ 212 522 26 68 03	contact@cabinetbassamat.com
Mexique *Mexico*	Langlet, Carpio y Asociados, S.C.	Enrique Ochoa De González Argüelles	+ 52 55 25 91 1070	eochoa@lclaw.com.mx
Norvège *Norway*	Føyen Advøkatfirma DA	Arve Føyen	+ 47 21 93 10 00	arve.foyen@foyen.no
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	sebastien.fanti@sebastienfanti.ch
Tunisie *Tunisia*	Younsi & Younsi International Law Firm	Yassine Younsi	+216 71 34 65 64	cabinetyounsi_younsi@yahoo.fr

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 29, rue du colonel Pierre Avia 75015 Paris, président : Alain Bensoussan
Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier
Diffusée uniquement par voie électronique – gratuit –

Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-juristendance
ISSN 1634-0701