JTIT Internationale n°5 – octobre 2013
Special international issue # 5– Octobre 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 2

GOVERNEMENT ACCESS TO DATA – PART 2

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 ultra organisé 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 nécessaire porter atteinte à la vie privée ou rester secrètes, que ce soit à des fins de renseignements ou pour anticiper certains 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 la protection des données à caractère personnel, doivent être protégés de manière prioritaire.
▪ C'est la raison pour laquelle il semble difficile de garantir 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 en deux parties. Ce numéro, qui en constitue la deuxième partie, contient les contributions des pays suivants : Etats-Unis, Grèce et Mexique. La première partie, diffusée en juillet, est accessible ici (elle contient les contributions des pays suivants : Afrique du Sud, Angleterre, Belgique, Canada, Chine, Colombie et France).

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 parts. This issue forms its Part 2 and incudes the contributions of the following countries: USA, Greece and Mexico. Part 1 was published in July and can be accessed here (it includes the contributions of the following countries: South Africa, England, Belgium, Canada, China, Colombia and France).

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

▪ La lutte contre les activités criminelles, telles que l'espionnage, le terrorisme, ou le trafic de drogue, pousse les Etats et leurs services de renseignements à chercher à accéder à certaines données et communications. Dans ce contexte, ils peuvent vouloir procéder à la surveillance électronique de communications ou obtenir accès à des documents, équipements ou locaux où les informations désirées sont stockées. Si la plupart des pays dans le monde sont dotés de législations permettant aux services de renseignements d'accéder ou d'obtenir des informations auprès de la personne qui les possède ou les détient, directement ou indirectement, les pouvoirs accordés à ces services par chaque législateur varient significativement d'un pays à l'autre. Les Etats-Unis ont adopté un arsenal législatif complet afin de réglementer l'accès des autorités aux données, mais il serait faux de penser que ces lois sont particulièrement permissives.

▪ **Cadre législatif américain en matière d'accès des autorités aux données et aux communications**

▪ Aux Etats-Unis, de nombreuses lois encadrent les circonstances et modalités dans lesquelles un enquêteur, étatique ou fédéral, est susceptible d'accéder à des données, des communications, des informations, des documents ou des locaux. La plupart de ces lois ont été promulguées à la fin des années 1960, mais ont été par la suite régulièrement amendées afin de prendre en compte les nouveaux types d'infractions ainsi que le développement de nouvelles technologies ou techniques.

▪ Les lois américaines sur la surveillance définissent les règles et exigences spécifiques à respecter par les services de police étatiques ou fédéraux en vue d'obtenir accès à des données ou à des communications ou bien aux locaux ou équipements où se trouvent ces données. Dans la grande majorité des cas, le représentant de l'Etat est tenu d'obtenir en amont une assignation (« subpoena »), une ordonnance d'un tribunal (« court order ») ou un mandat (« warrant »).

▪ Au niveau fédéral, le quatrième amendement de la Constitution américaine **(1)** consacre le droit général pour les citoyens américains d'être protégés contre les perquisitions et saisies abusives. En outre, plusieurs lois fédérales, telles que le Stored Communications Act, le Wiretap Act, le Pen Register Act, le Foreign Intelligence Surveillance Act, le Communications Assistance to Law Enforcement Act, ou le Economic Espionage Act, édictent les règles d'accès applicables dans certains cas spécifiques. Des distinctions sont en effet opérées selon l'objet des données (données de contenu, données hors contenu), la personne visée par l'enquête (citoyen ou résident américain, « agent d'une puissance étrangère ») ou encore la nature des données (données en transit, données stockées).

▪ Des dispositions similaires existent au niveau des Etats. Plusieurs d'Etats américains ont adoptés leurs propres lois sur la surveillance, ainsi que de lois spécifiques destinées à encadrer l'utilisation de certaines technologies à des fins de surveillance, telles que la RFID ou le GPS.

(1) Constitution des Etats-Unis
Version anglaise
Version française

▪ **Le « Stored Communications Act »**

▪ La grande majorité des demandes d'accès à des données ou des communications entre dans le champ du Stored Communications Act (18 USC §§2701-2711) **(2)**. Promulgué en 1986, cette loi s'applique aux communications câblées, orales et électroniques *stockées* (par opposition aux communications *en transit*). Le Stored Communications Act pose le principe d'une interdiction générale pour les personnes physiques et morales d'accéder aux données ou communications de tiers, tout en aménageant de nombreuses exceptions afin, notamment, de permettre aux autorités d'accéder aux données stockées par les prestataires de services de communications et de services informatiques. Les règles régissant ces exceptions sont extrêmement complexes et détaillées.

(2) Stored Communications Act

▪ Preuve de cette complexité, le §2703(a) de la section 18 du USC autorise une autorité à accéder à des contenus stockés depuis moins de 180 jours par un service de communication électronique, sous réserve d'avoir obtenu au préalable un mandat d'un juge. Or, l'obtention d'un mandat suppose le respect de conditions strictes. L'autorité doit démontrer, soit sur la base de l'observation personnelle de ses agents soit d'autres éléments, qu'il existe un « motif raisonnable » de penser que la preuve d'une infraction est susceptible d'être trouvée au cours de la perquisition sollicitée. En revanche, lorsque ces mêmes informations sont détenues depuis plus de 180 jours, d'autres règles s'appliquent. Dans ce cas, il suffit d'obtenir une assignation ou une ordonnance du tribunal. Les modalités d'obtention d'une assignation ou d'une ordonnance sont moins contraignantes que pour un mandat, mais dans ce cas de figure l'autorité est tenue d'informer l'abonné ou le client du service concerné de la demande d'accès qu'elle formule.

▪ Différentes règles s'appliquent également en fonction de la nature de l'information recherchée. En effet, les procédures ci-dessus s'appliquent uniquement aux demandes d'accès aux « contenus » (ce qui a été dit, ce que contenait le message). Les demandes d'accès aux données « hors contenu » (c'est-à-dire, le jour et l'heure d'envoi du message, l'identité de son émetteur et de son destinataire) obéissent à des modalités différentes.

(3) Wiretap Act

(4) Pen Register Act

▪ Enfin, pour rappel, le Stored Communications Act ne s'applique qu'aux données et communications stockées. Les données en transit sont quant à elles régies par le Wiretap Act **(3)** et le Pen Register Act **(4)**.

▪ **Rapports annuels**

▪ Les accès aux données et les interceptions de communications sont étroitement contrôlés. Non seulement les demandes des autorités doivent être dûment justifiées et motivées, mais les juges et le U.S. Attorney General (Procureur général des Etats-Unis, équivalent américain du ministre de la justice) sont également assujettis à des obligations de rendre compte.

▪ Ainsi, un juge ayant délivré ou refusé une ordonnance d'interception (en vertu du Wiretap Act) doit transmettre tous les ans à l'Office administratif des tribunaux des Etats-Unis (service chargé des affaires administratives, juridiques et de gestion du pouvoir judiciaire) un rapport d'information sur ses décisions. Ce rapport doit notamment mentionner le type d'ordonnance sollicitée, la durée de l'interception autorisée, l'infraction concernée et l'identité de l'agent à l'origine de la demande.

▪ Le U.S. Attorney General doit aussi réaliser un rapport à destination l'Office administratif des tribunaux des Etats-Unis. Ce rapport contient des informations détaillées sur chaque enquête conduite, et notamment le nombre de personnes dont les communications ont été interceptées et le nombre d'arrestations ou de condamnations résultant de l'interception.

▪ Une compilation de ces deux rapports est préparée annuellement et une synthèse est transmise au Congrès américain. Ces documents sont rendus publics et publiés sur Internet **(5)**.

(5) Wiretap Report 2012

▪ Les enquêtes ne sont donc pas lancées à la légère. Le poids des formalités à accomplir (préparation de nombreux rapports et déclarations), qui constitue déjà en soi une forme de dissuasion, est associé à un prix prohibitif : le coût d'une « interception » se situe entre 4.000$ et 600.000$ (New York Organized Crime Task Force), le coût moyen étant de 50.000$ par interception.

▪ **Foreign Intelligence Surveillance Act and Amendment**

▪ Le Foreign Intelligence Surveillance Act (FISA) **(6)**, promulgué en 1978, précise les procédures à respecter afin de procéder à des perquisitions de locaux et à la surveillance électronique d'activités de personnes physiques et morales étrangères ayant pour finalité l'obtention d'« informations relatives au renseignement étranger ».

(6) Foreign Intelligence Surveillance Act

▪ L'expression « informations relatives au renseignement étranger » désigne des informations nécessaires à la protection des Etats-Unis contre des attaques, réelles ou potentielles, des actes hostiles graves d'une puissance étrangère ou d'un agent d'une puissance étrangère, des actes touchant au sabotage, au terrorisme international, aux armes de destruction massive, à l'espionnage par ou pour une puissance étrangère ou d'actes autres similaires.

▪ Plus particulièrement, le FISA permet au Président des Etats-Unis, par l'intermédiaire du U.S. Attorney General, d'autoriser des surveillances électroniques destinées à acquérir des informations relatives au renseignement étranger. A cette fin, une autorisation du Tribunal FISA (également dénommé « FISC ») **(7)**, un tribunal spécial chargé de contrôler les activités de surveillance réalisées en vertu du FISA, est nécessaire. La demande de surveillance doit décrire les locaux ou la propriété concernés et démontrer qu'il existe une cause probable de croire que la cible à surveiller est une puissance étrangère.

(7) Présentation et documents

▪ En 2008, le FISA a été amendé par le FISA Amendments Act (FAA) **(8)** afin de permettre au U.S. Attorney General et au directeur du renseignement national d'autoriser conjointement le ciblage de citoyens non américains présumés se trouver hors des Etats-Unis, dans le but d'acquérir des informations relatives au renseignement étranger. Cette autorisation est subordonnée au constat de l'existence d'une situation d'urgence pouvant mener à la perte de renseignements importants pour la sécurité nationale des Etats-Unis. Par la suite, le FAA a lui-même été étendu par le FISA Amendment Acts Reauthorization Act of 2012 **(9)**, signés par le Président Obama début janvier 2013.

(8) FISA Amendments Act of 2008

(9) FISA Amendment Acts Reauthorization Act of 2012 (H.R. 5949)

▪ Il y a lieu de souligner que le gouvernement américain n'a pas compétence sur les entités non américaines situées en dehors du territoire des Etats-Unis et que le FAA n'accorde pas aux autorités américaines le droit d'accéder aux serveurs hébergés en dehors du territoire américain. Le FAA a pour but d'énoncer les règles à suivre par

les agents fédéraux en vue de cibler les communications effectuées par ou à destination de citoyens étrangers, situés à l'étranger, afin d'acquérir des informations relatives au renseignement étranger.

- **Accès aux données détenues dans un pays étranger**

- Que se passe-t-il lorsqu'une enquête nécessite l'accès à des données hébergées dans un pays étranger ? En règle générale, un procureur ou un enquêteur d'un pays n'est pas autorisé à conduire des enquêtes ou auditionner des témoins à l'étranger. Dans la plupart des cas, l'assistance des autorités locales sera donc nécessaire. C'est la raison pour laquelle, depuis plusieurs années, les pays ont conclu des traités bilatéraux ou multilatéraux destinés à organiser leur coopération en la matière.

- Les Etats-Unis sont ainsi partie à de nombreux traités d'assistance judiciaire mutuelle permettant la collecte et l'échange d'informations nécessaires à la mise en œuvre de lois civiles et pénales. Divers traités relatifs à la coopération des services de police sont en place, entre autres en matière d'évasion fiscale.

(10) Convention sur la cybercriminalité

- Les Etats-Unis sont notamment signataires de la Convention sur la cybercriminalité du Conseil de l'Europe **(10)**, ratifiée en 2007. Cette Convention sert de lignes directrices en matière de surveillance électronique, de collecte et de partage de preuve dans le cyberespace. Elle instaure des mécanismes d'entraide entre Etats pour l'investigation et la poursuite de nombreuses infractions telles que le piratage informatique, l'accès non autorisé à des systèmes informatiques, la pornographie enfantine et les atteintes à la propriété intellectuelle.

- En pratique, les procureurs fédéraux américains, qui ne sont pas autorisés à communiquer directement avec les autorités ou les témoins étrangers, ou même à se déplacer dans un pays étranger, auront fréquemment recours aux traités d'entraide judiciaire (TEJ, ou en anglais MLAT) et à d'autres traités et conventions internationaux.

- Enfin, il faut noter que dans certains cas les services de police américains peuvent également obtenir l'accès aux informations d'une entreprise située à l'étranger par le biais de sa filiale américaine. Les tribunaux américains ont en effet jugé qu'une entreprise présente sur le territoire américain était tenue de répondre à une demande valide de communication d'informations émise par l'administration américaine (et formulée en vertu d'une loi américaine applicable) dès lors que ladite entreprise détient la garde ou le contrôle de ces données. La question principale sera bien entendu de déterminer si l'entreprise américaine possède le niveau de « garde » ou de « contrôle » nécessaire l'obligeant à répondre favorablement à cette demande.

- **Pouvoirs importants des services de renseignements dans la plupart des pays**

- Dans la plupart des pays du monde, les services de renseignements disposent de pouvoirs d'enquêtes considérables dans le cadre de la lutte contre une série d'activités criminelles telles que le terrorisme, l'espionnage, le blanchiment d'argent, la pornographie enfantine et le trafic de drogue. Chaque pays reconnaît généralement le besoin de fournir des informations tout en conservant le secret, mais cette reconnaissance peut se traduire différemment dans chaque législation. Les conventions internationales, telles que les traités d'entraide judiciaire, permettent la coopération des services de renseignement ou d'enquête nationaux par-delà les frontières.

▪ Le législateur américain a prévu des règles strictes et détaillées et mis en place des mécanismes de transparence qui astreignent les services de police à des obligations d'information concernant leurs activités. Des mesures de contrôle (rapports annuels), des modalités précises (mandat ou ordonnance), et règles procédurales sont notamment instaurées. Dans d'autres pays, l'accès aux équipements, serveurs ou systèmes de stockage par les services de police ou de renseignement ou les services secrets peuvent être plus ou moins règlementés et laisser davantage de marge de manœuvre aux autorités.

▪ Toujours est-il que lorsqu'un prestataire reçoit une demande émanant des services secrets ou des services de police ou de renseignement, ou de toute autre autorité du pays dans lequel ses serveurs sont hébergés, et que cette demande est conforme aux exigences prescrites par la loi, il n'aura d'autre choix que d'y donner suite et d'accorder l'accès à ses propres données ou équipements, ainsi qu'aux données ou fichiers de ses clients, à moins que la demande soit viciée et ne respecte pas les règles applicables ; dans ce cas, le prestataire peut choisir de contester la demande en arguant, selon le cas, de son illégalité, de sa non-conformité ou de son imprécision.

▪ **Conclusion**

▪ Ainsi donc, les entreprises doivent être bien conscientes que les autorités d'un pays, voire de plusieurs pays, sont en mesure d'obtenir accès à leurs données, notamment pour des raisons de sécurité nationale ou de poursuite ou de prévention d'infractions graves, et ce quel que soit le lieu où ces données sont stockées ou hébergées, par elles ou par un tiers. En outre, bien souvent, cet accès interviendra sans information préalable. Certes, cela a toujours été le cas, même lorsque les données étaient détenues dans des serveurs situés simplement de l'autre côté de la rue du siège de l'entreprise. Toutefois, aujourd'hui, l'utilisation généralisée des services de cloud computing change la donne, car désormais les mêmes données peuvent être détenues dans une kyrielle de serveurs situés en différents points du globe, et peuvent donc faire l'objet de demandes d'accès par davantage d'autorités, dans de nombreux pays, en vertu d'une multitude de lois.

▪ Les prestataires doivent, quant à eux, veiller à assumer la double responsabilité qui leur incombe. Ils sont en effet tenus de répondre aux demandes formulées par les autorités visant à obtenir accès aux données qui leur sont confiés par leurs clients, tout en étant responsables vis-à-vis de ces clients de n'accorder cet accès que de manière responsable et conforme aux dispositions de leurs conditions générales de service. Ils doivent donc s'attacher à bien comprendre et respecter les règles qui s'appliquent à leurs activités. Dès lors, à réception d'une demande d'accès émanant d'une autorité, un prestataire doit avant tout déterminer si cette demande est conforme à la loi applicable. Dans l'affirmative, et si cela lui est légalement et physiquement possible, il prend ensuite les mesures adéquates pour informer son client qu'une enquête des autorités est en cours. La prudence est toutefois de mise car bien souvent, la loi, que ce soit aux Etats-Unis ou ailleurs dans le monde, interdit strictement aux prestataires d'informer leurs clients.

FRANÇOISE GILBERT

▪ *Governments and intelligence services regularly seek access to data and communications as part of their investigation of criminal activities such as espionage, terrorism, or drug trafficking. In these circumstances, they may wish to conduct electronic surveillances of communications, or obtain access to documents, equipment, or premises where the needed information is stored. Most countries have laws that define the extent of the intelligence and secret services' powers to access or obtain this material directly or indirectly, from its owner or its custodian. The scope and provisions of these laws vary significantly from one country to the other. There are also substantial differences in the oversight of the governmental agencies' activities. While undoubtedly the US has adopted a comprehensive set of laws to regulated government access to data, it is wrong to think that these laws are uniquely permissive.*

▪ ***US Laws Regarding Government Access to Data and Communications***

▪ *In the United States, numerous laws govern the circumstances and manner in which a state or federal investigator may have access to data, communications, information, documents, or premises. Most of these laws have been in existence since the late 1960's. They have been periodically amended to take into account new types or forms of crimes, or the development of new technologies or techniques.*

▪ *The U.S. surveillance laws define the specific rules and requirements that must be met for a federal or state law enforcement agent to have access to specific data, communications, premises, or equipment where the data are located. In most cases, the government representative is required to obtain a subpoena, a court order, or a warrant.*

▪ *At the federal level, the basic rule written in the Fourth Amendment to the U.S. Constitution **(1)** grants Americans the right to be secure from unreasonable searches and seizures. In addition, several federal laws, such as the Stored Communications Act, Wiretap Act, Pen Register Act, Foreign Intelligence Surveillance Act, Communications Assistance to Law Enforcement Act, or the Economic Espionage Act, define the rules for access to data or communications in specific circumstances. The Wiretap Act, for instance, pertains to data in transit, whereas the Stored Communications Act pertains to data in storage. There are different provisions for access to content as opposed to access to non-content (i.e., identity of the sender, the recipient, time of the call or communication). The law may distinguish whether the person being investigated is a U.S. citizen or resident, or, instead an "agent of a foreign power" as is the case under the Foreign Intelligence Surveillance Act.*

(1) Constitution of the United States

▪ *A similar regime exists under State law. Most U.S. States have general surveillance laws. They may have specific laws, as well, to govern the use of certain technologies that can be used for surveillance, such as RFID or GPS.*

▪ ***Stored Communications Act***

▪ *The Stored Communication Act **(2)** governs many of the requests for access to data or communications. Enacted in 1986, and codified as 18 USC §§2701-2711, the Stored Communications Act governs access to*

wire, oral, and electronic communications in storage (as opposed to communications in transit). While the law generally prohibits most individuals and companies from accessing a third party's data or communications, it contains numerous exceptions, including provisions that define the conditions under which governmental entities may access data stored by communications and computing service providers. These rules are very complex and very detailed.

(2) Stored Communication Act

▪ *For instance, 18 USC §2703(a) allows a governmental entity to require the disclosure of content that has been held in storage for less than 180 days by an electronic communications service, only after the governmental entity has obtained a warrant from a judge. The standard for obtaining a warrant is very high. In order to obtain the warrant, the government officer must show that "probable cause" exists, based on the officer's personal observation or hearsay information, to show that evidence of a crime would be found in the requested search.*

▪ *There are different rules for obtaining access to the same information that would have been held by the same service provider for more than 180 days. In this case, a subpoena or court order would suffice. The requirements for a subpoena or a court order are less stringent than those that apply to the issuance of a warrant. However, in this later case, if the government opted to use a subpoena or a court order, then it would have to give the subscriber or customer of that service prior notice of the access request. In addition to the dichotomy described above - i.e. more than 180 days v. less than 180 days in storage, there are also different rules that distinguish according to the nature of the information sought. While the rules above would apply to requests for access to "content" (i.e., what was said, what was the message), access to "non-content" (i.e., the time and date when the message was sent, from whom it was sent, who received it) would be regulated differently.*

▪ *While the Stored Communications Act applies only to access to stored data and communications, different rules apply to access to information "in transit." In this, case, the relevant laws are the Wiretap Act* ***(3)*** *or the Pen Register Act* ***(4)****.*

(3) Wiretap Act

(4) Pen Register Act

▪ ***Oversight: Annual Reports***

▪ *The issuance of search warrants or court orders allowing access to, or interception of data or communications is highly controlled. It is not enough that each law enforcement agent must provide substantial information to show why the search is needed, and must identify the grounds to believe that the content is relevant or material. There are also reporting requirements.*

▪ *For example, any judge who has issued an order for an interception (under the Wiretap Act), or has denied the request, must report, annually, to the Administrative Office of the United States Courts information about its approval or denial of requests for warrants or orders. The report must indicate the fact that the order was applied for, and the kind of order or extension request; the fact that the order or extension was granted, and the period of interception authorized; and the offense specified in the order and the identity of the officer making the application.*

▪ *Concurrently, the U.S. Attorney General who has made the request for access must also file a report to the Administrative Office of the United States Courts. This report must also contain detailed information about*

each investigation, including, for example, the number of persons whose communications were intercepted, number of arrests resulting from the interception or number of convictions.

- *Based on the judge reports and the U.S. Attorney General reports, a compilation is prepared annually, and a summary report is provided to Congress. These reports are publicly available for anyone to review, and are posted on the Internet **(5)**.*
- *Thus, these investigations are not started lightly. The perspective of having to prepare so many reports and statements would already be a deterrent. In addition, each such investigation is very costly. For example, according to the report on wiretaps installed in 2011, the average cost of an "interception" ranges from $4,000 to close to $600,000 (New York Organized Crime Task Force), with a median around $50,000 per interception.*
- **Foreign Intelligence Surveillance Act and Amendment**
- *The Foreign Intelligence Surveillance Act (FISA) **(6)**, enacted in 1978, prescribes procedures for physical searches and electronic surveillance of activities of foreign entities and individuals where a significant purpose of the search or surveillance (and the collection of information) is to obtain "foreign intelligence information."*
- *The term "foreign intelligence information" is defined to include information that relates to actual or potential attacks or grave hostile acts of a foreign power or an agent of a foreign power, sabotage, international terrorism, weapons of mass destruction, clandestine intelligence activity by or on behalf of a foreign power, or similar issues.*
- *FISA allows the President of the United States, through the U.S. Attorney General, to authorize electronic surveillances in order to acquire foreign intelligence. To conduct such electronic surveillance, the government agent must seek an order from the FISA Court (or "FISC") **(7)**, a special court that oversees surveillance activities under FISA. The application to conduct the surveillance must set out the facts to support a finding by the FISC judge reviewing the application that there is probable cause to believe that the proposed target is a foreign power. The application must also describe the premises or property that is the proposed subject of the search or surveillance.*
- *FISA was amended in 2008 through the FISA Amendment Act (FAA) **(8)** to permit the U.S. Attorney General and the Director of National intelligence to jointly authorize the targeting of non-U.S. persons reasonably believed to be located outside the United States, in order to acquire foreign intelligence information. The FAA was extended though the FISA Amendment Acts Reauthorization Act of 2012, H.R. 5949 **(9)**, signed into law by President Obama in early January 2013. Targeting under the FAA requires a determination by the U.S. Attorney General and the Director of National Intelligence that exigent circumstances exist because intelligence important to the national security of the United States may be lost.*
- *The U.S. government does not have jurisdiction over non-U.S. entities located outside the U.S. territory. The FAA does not grant U.S. governmental entities the right to access servers held outside the United States. It only defines the rules that federal agents must follow to target communications made by or to non-U.S. persons believed to be located abroad, in order to acquire foreign intelligence information.*

(5) Wiretap Report 2012

(6) Foreign Intelligence Surveillance Act

(7) Presentation and public filings

(8) FISA Amendments Act of 2008

(9) FISA Amendment Acts Reauthorization Act of 2012

▪ **Access to Data Held in a Foreign Country**

▪ *What happens when an investigation would require access to data held in a foreign country? Generally, a U.S. prosecutor or investigator will not be permitted to conduct an investigation, or interview witnesses abroad. In most cases, the assistance of the local government will be necessary. To this end, over the years, countries have entered into bilateral or multilateral treaties that define how they will cooperate in these matters.*

▪ *The United States is a party to several Mutual Legal Assistance Treaties (MLAT) for gathering and exchanging information necessary to enforce public laws or criminal laws. There are numerous MLATs related to police and law enforcement cooperation, including MLATs with respect to tax evasion.*

▪ *The United States is also a member of the Council of Europe Convention on Cybercrime **(10)**, which it ratified in 2007. The Convention governs electronic surveillance, sharing of evidence, and computer crime. It allows governments to request and provide mutual assistance in the investigation and prosecution of a number of crimes, such as hacking, unauthorized access to computer systems, child pornography, or copyright infringements.*

(10) Convention on Cybercrime

▪ *Thus, in practice, federal prosecutors who need access to data will frequently take advantage of the methods provided in the applicable MLATs, treaties, or conventions, since they are not allowed to communicate directly with foreign authorities, or witnesses, or to undertake travel to a foreign country.*

▪ *In some cases, law enforcement seeking information that might be stored abroad with an entity may attempt to obtain access to this information by approaching the U.S. affiliate of that entity located abroad who may have custody or control over the documents or information at stake. United States courts have held that a company with a presence in the United States is obligated to respond to a valid demand by the U.S. government for information (made under one of the applicable U.S. laws) so long as the company retains custody or control over the data. In this case, of course, the key question is whether and the extent to which the U.S. company does have the required level of "custody or control" to be forced to respond to the government request.*

▪ **Expect Intelligence Services to Have Significant Powers in Most Countries**

▪ *Intelligence services, in their fight against terrorism, espionage, money laundering, child pornography, drug trafficking, and the like, have significant investigatory powers in most countries. The concerns and the need for information on one end, and the need for some secrecy on the other, are generally similar in most countries, even though they might be translated differently in each local law. Further, MLATs and other multinational treaties allow many countries' intelligence or investigative services to cooperate with each other across borders.*

▪ *U.S. laws contain strict and detailed rules, provide a lot of transparency, and require law enforcement to make numerous disclosures of their activities. There are many control measures (e.g., annual reports) or detailed procedures (e.g., warrant or a court order), and procedural rules. In other countries, access to equipment, servers or storage systems by law enforcement, or intelligence or secret services may be much less*

regulated, and provide more freedom to governmental entities.

▪ *If a service provider receives a request from the secret services, intelligence services, or other law enforcement authority of the country in which its servers are located, in the manner prescribed by applicable law, it will not have much choice other than providing access to its data or equipment, and to its customers' data or files, unless the request is defective and does not follow the applicable rules; in this case, the service provider may opt to fight the request and argue that it is illegal, does not conform to the legal requirements or is too broad, as applicable.*

▪ **Conclusion**

▪ *Organizations should remain aware that wherever their data are stored or hosted by a third party, it may be possible to a government - or several governments concurrently - to obtain access to these data, especially when there are overarching reasons for such access, such as national security or the prosecution or prevention of serious crimes. In addition, in many cases, this access will be provided without the customer being informed that the service provider is responding to a government request, and providing access to the customer's data or communication. This has always been the case, even when data were held in server farms across the street from one's corporate headquarters. Today, with the ubiquitous use of cloud computing services, the dynamic changes because, now, these same data may be held in several servers located anywhere in the world, and consequently may be subject to requests for access by many more entities, in many more countries, and under many more laws.*

▪ *Service providers have a dual responsibility. They must understand and abide by the rules that apply to their business, and they have an obligation to their customers to respond to government or other request for access to data in their custody in a responsible manner and in accordance with their Terms of Service. When a service provider receives a government request for access, it has the responsibility to evaluate this request and determine whether the request is conform to applicable law. If it is, and if this is legally and physically possible to do, the service provider might be able to take the necessary steps to inform the customer, in a manner that is consistent with the provisions of its Terms of Service, that a government investigation is being conducted. However, companies should remain aware that the service provider might not necessarily be able to contact the customer to alert the customer on the governmental entity's request because many laws in the United States and elsewhere strictly prohibit the service providers from doing so.*

FRANÇOISE GILBERT

▪ L'accès des autorités aux données a toujours été une question controversée en Grèce, qui se pose avec encore plus d'acuité depuis ces deux dernières décennies compte tenu de l'utilisation croissante des nouvelles technologies de communication et, plus récemment, des services et produits *cloud*.

▪ Le débat qui fait actuellement rage, aussi bien sur les plans juridique que politique, autour de la nécessité d'assouplir le cadre législatif existant est révélateur des contraintes que celui-ci représente pour les services de police et de renseignement. En Grèce, les communications bénéficient d'une protection constitutionnelle de confidentialité, à laquelle il ne peut être dérogé que par une procédure spéciale dite de « levée du secret ». La question essentielle consiste à déterminer si cette protection, et par conséquent la procédure de levée du secret y associée, couvre uniquement les données relatives au contenu des communications ou bien également les données connexes à ce contenu (c'est-à-dire les données de trafic). La procédure de levée du secret est en effet assez contraignante (une ordonnance du procureur de la cour d'appel grecque ou du conseil judiciaire compétent est requise) tandis que l'accès aux données non soumises à cette procédure est plus simple (ordonnance du procureur du tribunal de grande instance).

▪ **Cadre juridique grec**

▪ Le cadre législatif grec en matière de protection de confidentialité et d'accès par les autorités aux données est principalement constitué des textes suivants :

- Loi 2472/1997 sur la protection des données, à caractère personnel, transposant la législation communautaire ;
- Loi 3471/2006 sur la protection des données et de la vie privée dans le secteur des télécommunications électroniques (transposant la directive communautaire « vie privée »), et en particulier son article 4 relatif à la confidentialité des communications électroniques (« loi sur la protection de la vie privée ») ;
- Constitution grecque, article 19 relatif au secret des communications ;
- Loi 2225/1994 stipulant les conditions et la procédure judicaire applicables à l'interception légale du contenu des communications et à l'accès aux données de communications ;
- Décret présidentiel 47/2005, portant les mesures techniques et organisationnelles pour l'interception et l'accès aux données ;
- Articles 248-250 du code pénal, spécifiant les sanctions applicables en cas de violation du secret par les agents postaux et les employés des entreprises de télécommunications ;
- Articles 370 et 370A du code pénal, spécifiant les sanctions applicables en cas de violation du secret des correspondances, des appels téléphoniques et des communications privées ;
- Avis 9/2009, 12/2009 et 9/2011 du Procureur de la Cour suprême de Grèce ;
- Avis 1/2005 de l'Autorité hellénique pour la sécurité et la confidentialité des communications (ADAE).

▪ **Accès aux données aux termes de la loi de protection des données à caractère personnel et la loi sur la protection de la vie privée**

▪ Aux termes de la loi informatique et libertés grecque **(1)**, le traitement de données à caractère personnel (et l'accès à ces données) n'est autorisé que lorsque la personne concernée a expressément donné son consentement (article 5). Par exception, les données personnelles peuvent faire l'objet d'un traitement sans le consentement de la personne concernée lorsque (notamment) le traitement est nécessaire « à l'exécution d'une mission d'intérêt public ou

(1) ΝΟΜΟΣ 2472/1997, «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
Version grecque
Version française

relevant de l'exercice de l'autorité publique ». S'agissant des « données sensibles », l'article 7 interdit par principe la collecte et le traitement de ces données, sauf autorisation accordée par l'Autorité grecque de protection des données, notamment lorsque « le traitement est réalisé par une autorité publique et est nécessaire pour (i) la sûreté de l'Etat ; (ii) la détection et la poursuite d'infractions, les condamnations pénales ou les mesures de sûreté ; (iii) la protection de la santé publique ; ou (iv) l'exercice du contrôle public des services fiscaux et sociaux ». Toutefois, aucune autorisation n'est requise « lorsque le traitement est effectué par les autorités judiciaires » (article 7A). En outre, les dispositions de la loi sur la protection des données à caractère personnel ne s'appliquent pas aux traitements de données effectués par les autorités judiciaires, le ministère public et les autorités agissant sous leur supervision aux fins d'enquête portant sur des crimes ou des délits (article 3, par. 2b). Dans ce cas, seule la législation concernant la levée du secret des communications (cf. ci-dessous) est applicable.

▪ La loi sur la protection de la vie privée **(2)** inclut des dispositions sur la sécurité et la confidentialité des communications. Selon son article 4, les données *de trafic* sont couvertes par le principe constitutionnel de confidentialité des communications (tout comme le *contenu* des communications). Plus particulièrement, toute utilisation des services de communications électroniques fournis par des réseaux de communications électroniques ouverts au public, ainsi que les données de trafic correspondantes sont protégées par le principe de secret des télécommunications consacré la Constitution grecque et la levée de ce secret ne peut être autorisée que selon les procédures et les modalités énoncées à l'article 19 de la Constitution. Par conséquent, tout type d'interception ou de surveillance de contenus de communications et des données de trafic correspondantes est interdit, sauf autorisation légale contraire (cf. ci-dessous).

▪ La levée du secret des communications aux termes de la Constitution grecque et de la législation applicable

▪ La Constitution grecque (article 19) **(3)** pose le principe de l' « inviolabilité absolue » du secret des communications, auquel il ne peut être dérogé que dans des cas très limités (pour la sûreté de l'Etat et pour une liste limitative d'infractions telles que la contrefaçon, la corruption, le meurtre, le vol ou l'extorsion) et exclusivement sous les garanties et la supervision du pouvoir judiciaire et d'une autorité indépendante établie par la Constitution (l'ADAE, dont la mission est de protéger la confidentialité et le secret des communications).

▪ La loi 2225/1994 **(4)** et le décret présidentiel 47/2005 **(5)** précisent la liste des infractions pour lesquelles le secret des communications peut être levé et décrivent les modalités, les délais et les garanties techniques et organisationnelles à respecter à cette fin. Seul le procureur compétent ou une autorité judiciaire ou une autorité publique politique, miliaire ou de police compétente pour traiter les questions touchant à la sûreté de l'Etat et impliquant la levée du secret, sont habilités à déposer une demande de levée du secret, sur laquelle statuera ensuite le procureur de la cour d'appel grecque ou le conseil judiciaire compétent (ou exceptionnellement le procureur du tribunal de grande instance).

▪ La procédure de levée du secret à suivre pour accéder aux données, s'applique aux communications effectuées via les réseaux de communication ou les prestataires de services de communication. Sont concernés les communications effectuées par téléphone (fixe et mobile), les communications effectuées via les réseaux de données, les communications internet, les communications sans fil, les communications par satellite, ainsi que les services fournis dans le cadre des différents types de communication susmentionnés (répondeurs automatiques, SMS/MMS, accès aux sites Web, accès aux bases de données, messages électroniques, transactions électroniques, services d'annuaires, services d'urgence…). Les données stockées dans le cloud sont tombent naturellement dans le champ d'application des dispositions de levée du secret.

(2) ΝΟΜΟΣ 3471/2006, «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/1997»
Version grecque
Version anglaise

(3) ΣΥΝΤΑΓΜΑ
Version grecque
Version française

(4) ΝΟΜΟΣ 2225/1994, «Για την προστασία της Ελευθερίας και ανταπόκρισης και επικοινωνίας και άλλες διατάξεις»
Version grecque

(5) ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ 47/2005, «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του»
Version grecque

- **Accès aux données de trafic**

- Les données de trafic englobent les données de communication hors contenu, c'est-à-dire l'identité des parties participant à la communication, le service de communication utilisé, les informations de facturation, la localisation, l'heure, la durée et la langue de la communication.

- Depuis la fin des années 90, un débat agite le monde judiciaire grec concernant le champ d'application de la protection constitutionnelle de secret accordée aux communications : couvre-t-elle les données de trafic ? La réponse à cette question est importante car, comme exposé ci-dessus, elle détermine la procédure à suivre par les autorités en vue d'accéder aux données de trafic. Si l'on y répond par l'affirmative, la procédure de levée du secret est applicable (et impose l'obtention d'une ordonnance du procureur de la cour d'appel grecque ou du conseil judiciaire compétent). En revanche, dans la négative, une simple ordonnance du procureur du tribunal de grande instance grec est suffisante. La question est épineuse, et aucune réponse catégorique n'y est apportée.

- En effet, d'un côté, la loi sur la protection de la vie privée inclut spécifiquement les données de trafic dans le giron de la protection constitutionnelle. La même position a été adoptée par l'Autorité hellénique pour la sécurité et la confidentialité des communications (ADAE) dans son avis 1/2005 **(6)**. En outre, l'article 4 du décret présidentiel 47/2005, qui dresse la liste des données de communication soumises à la procédure de levée du secret, y inclut expressément certaines données de trafic.

(6) www.adae.gr/en/

- D'un autre côté, le procureur de la Cour suprême grecque soutient, dans ses avis 9/2009, 12/2009 et 9/2011, que les données de trafic ne sont pas couvertes par le principe de secret et, par conséquent, que la procédure de levée de secret ne s'applique pas à ces données.

- Ces avis divergents ont provoqué une insécurité juridique et un imbroglio administratif plaçant les prestataires dans une situation paradoxale délicate : des fournisseurs d'accès internet (FAI) qui avaient refusé de fournir à la police des données de trafic, aux motifs qu'une telle divulgation, non conforme à la procédure de levée du secret, serait contraire à la loi sur la protection de la vie privée et à la loi 2225/1994, se sont ainsi vu poursuivis pénalement pour « désobéissance » et « accueil de criminels », au sens des articles 169 et 231 du code pénal grec.

- **Accès aux données par les autorités de police étrangères**

- En principe, les autorités de police étrangères peuvent accéder à certaines données en formulant une demande s'appuyant sur les dispositions d'un traité d'assistance juridique mutuelle. Ce type de traité permet généralement l'échange d'informations et de preuves en matière pénale.

(7) Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire, 19-7-2003

- Concernant plus particulièrement les demandes faites par les autorités américaines, il convient de noter l'existence d'un accord entre les Etats-Unis et l'Union européenne en matière d'entraide judiciaire, en vigueur depuis 2003 **(7)**. Cet accord s'applique en parallèle d'autres conventions d'entraide judiciaire conclues séparément par les différents États membres de l'UE avec les États-Unis. La Grèce et les Etats-Unis ont ainsi signé un traité d'entraide judiciaire, en vigueur depuis le 20 novembre 2001 **(8)**, et dont le champ d'application couvre l'assistance dans le contexte d'enquêtes, de poursuites et de prévention d'infractions et de procédures criminelles (criminalité organisée, meurtres, etc.). Dans ce cadre, il est prêté assistance pour (a) la fourniture de documents et de dossiers, (b) la localisation ou l'identification des personnes ou d'objets et (c) la réalisation de perquisitions et de saisies.

(8) Treaty with the Hellenic Republic on mutual legal assistance in criminal matters, Treaty Doc. 106-18

GEORGE A. BALLAS

- *Government access to data has always been a controversial issue in Greece, especially during the last two decades, given the introduction and wide use of new communication technologies and - most recently – due to the use and implementation of cloud services and products.*
- *The current legal and political debate in Greece on the necessity of lowering the requirements set by the current legislation regarding the 'lifting of secrecy of communications' is indicative of the hurdles that such framework poses to law enforcement and intelligence agencies. Such debate includes a discussion on whether the protection of confidentiality covers only the content of the communication or traffic data as well and, in this scope, if the procedure for the 'lifting of secrecy' applies to traffic data, in which case an Order by the Public Prosecutor of the Greek Court of Appeals or the competent Judicial Council is required, or simply an Order by the Public Prosecutor of the Greek First Instance Court is sufficient for the disclosure of such data.*
- ***The main Greek Legal Framework***
- *The main legislative framework regulating protection of confidentiality and government access to data includes the following legal texts and Opinions:*
  - *Data Protection Law, 2472/1997, implementing relevant EU data protection legislation ("DPL");*
  - *Law 3471/2006, on the protection of personal data and privacy in the electronic telecommunications sector (implementing E-Privacy Directive), and in particular Article 4, on the confidentiality of electronic communications ("PECL");*
  - *Greek Constitution, Article 19, regarding the secrecy of communications;*
  - *Law 2225/1994, stipulating the conditions and the judicial procedure, under which the lawful interception of the content of communications and the access to communications data is legitimate;*
  - *Presidential Decree 47/2005, including the technical and organizational measures for lawful interception and access to data;*
  - *Articles 248-250 of the Penal Code, laying down sanctions for the violation of secrecy by post officials and employees of telecommunication companies;*
  - *Articles 370 and 370A of the Penal Code, laying down sanctions for the violation of secrecy of letters and telephone calls and private communications;*
  - *9/2009 Opinion of Public Prosecutor of the Greek Supreme Court; 12/2009 Opinion of Public Prosecutor of the Greek Supreme Court; 9/2011 Opinion of Public Prosecutor of the Greek Supreme Court;*
  - *1/2005 Opinion of the Hellenic Authority for Communication Security and Privacy (ADAE).*
- ***Access to Data According to DPL and PECL***
- *According to DPL **(1)**, processing of personal data (including access to such data) is permitted only when the Data Subject has provided his/her consent (Article 5). Exceptionally, personal data can be processed without the Data Subject's consent, when (inter alia) processing is necessary "for the performance of a task of public interest or of a task carried out by a Public Authority in the framework of the exercise of its authority". In particular with regard to 'sensitive data', according to Article 7, collection and processing of such data is prohibited. Exceptionally, collection and processing of 'sensitive data' can take place pursuant to a Permit issued by the Hellenic Data Protection Authority (DPA), when (inter alia) "processing is carried out by a Public Authority and is necessary for the purposes of (i) national security; (ii) criminal or punishment policy and*

(1) ΝΟΜΟΣ 2472/1997, «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
Greek version
English version

pertains to the detection of offences, criminal convictions or security measures; (iii) protection of public health; or (iv) the exercise of public control on tax or social services". However, no Permit will be required "when processing is carried out by Judicial Authorities" (Article 7A). We note that the DPL provisions do not apply to the processing of personal data, which is carried out by Judicial - Public Prosecution Authorities and by the Authorities acting under their supervision, in the framework of providing justice or for operational purposes, in order to investigate crimes, which are punished as felonies or misdemeanors (with intent) (Article 3, par. 2b). In such case, applicable will be only the legislation regarding the 'lifting of secrecy of communications' (as analyzed herein below).

▪ *PECL **(2)** includes provisions for the security and confidentiality of communications. It is important the fact that, according to PECL Article 4, traffic data are covered by the constitutional principle of confidentiality (as it is clearly the case with the* content *of communication). More specifically, any use of electronic communications services offered through a publicly available electronic communications networks, as well as the relevant traffic data are protected by the principle of confidentiality of telecommunications (as established by the Greek Constitution) and the 'lifting of secrecy of communications' can be allowed only under the procedures and conditions provided for in Article 19 of the Greek Constitution. Therefore, all kinds of interception or surveillance of content of communications and of the relevant traffic data is prohibited, except when legally authorized (as explained herein below).*

(2) ΝΟΜΟΣ 3471/2006, «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/1997»
Greek version
English version

▪ ***'Lifting of Secrecy of Communications' according to Greek Constitution and Relevant Legislation***

▪ *The Greek Constitution (Article 19) **(3)** establishes the 'absolute inviolability' of secrecy of communications, which can be side-stepped only for very specific cases (national security and very limited number of felonies, including inter alia forgery, bribery, murder, robbery, and extortion) and only under the guarantees and supervision of the judiciary and the involvement of a constitutionally established independent authority (with the sole purpose of safeguarding the confidentiality and secrecy of communications).*

(3) ΣΥΝΤΑΓΜΑ
Greek version
English version

▪ *A list of the felonies for which 'lifting of secrecy of communications' can be allowed and the procedures, time limits and technical and organizational safeguards that need to be followed are included in Law 2225/1994 **(4)** and Presidential Decree 47/2005 **(5)**. Only the competent Public Prosecutor or a Judicial Authority or other political, military or police public authority, competent for an issue of national security requiring the 'lifting of secrecy', may submit a request for 'lifting of secrecy', which then can be ordered by the Public Prosecutor of the Greek Court of Appeals or the competent Judicial Council (exceptionally by the Public Prosecutor of the Greek First Instance Court).*

(4) ΝΟΜΟΣ 2225/1994, «Για την προστασία της Ελευθερίας και ανταπόκρισης και επικοινωνίας και άλλες διατάξεις»
Greek version

(5) ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ 47/2005, «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του»
Greek version

▪ *The 'lifting of secrecy' applies to communication conducted via communication networks or via communication service providers. The types and forms of communication which are subject to the 'lifting of secrecy' are (inter alia) telephone (fixed and mobile), data communication via data networks, internet communication, wireless communication, satellite communication, and services provided in the framework of the above types/forms (e.g. automatic answering machine, SMS/MMS, access to websites, access to databases, e-mail, electronic transactions, directory information, emergency services). Data stored in the cloud are certainly within the scope of the 'lifting of secrecy' provisions.*

▪ ***Access to Trafic Data***

▪ *Traffic data refer to the non-content data of the communication, including the identity of the communicating parties, the communication service used, billing information, location, time, duration, and language.*

▪ *Special reference must be made to the legal debate, which has been taking place since the late 90s in Greece, on whether the protection of confidentiality covers only the content of the communication or traffic data as well and, in this scope, if the procedure for the 'lifting of secrecy' applies also to traffic data, in which case an Order by the Public Prosecutor of the Greek Court of Appeals or*

the competent Judicial Council is required, or simply an Order by the Public Prosecutor of the Greek First Instance Court is sufficient for the disclosure of such data.

- *PECL specifically included traffic data under the protection of confidentiality. The same position was also adopted by the 1/2005 Opinion of the Hellenic Authority for Communication Security and Privacy (ADAE)* ***(6)****. Moreover, Article 4 of Presidential Decree 47/2005, specifically refers to some traffic data when listing the communication data for which 'lifting of secrecy' can be ordered.*
- *Contrary to the above, the 9/2009, 12/2009 and 9/2011 Opinions of Public Prosecutor of the Greek Supreme Court supported the view that traffic data are not covered by the principle of confidentiality and therefore the procedure for the 'lifting of secrecy' does not apply to such data.*
- *The above have caused legal uncertainty and created a legal paradox, when e.g. Internet Service Providers (ISPs) who had received disclosure requests by the Police (without the procedure for the 'lifting of secrecy' having been followed) faced penal charges ('Disobedience' and 'Harbouring a Felon', Articles 169 and 231 of the Penal Code) when they refused to provide the Police with such traffic data, arguing that such disclosure would be in breach of PECL and Law 2225/1994 (which also included sanctions for offenders).*

(6) www.adae.gr/en/

- ***Access to Data by Foreign Enforcement Authorities***
- *Access to data can in principle be granted to foreign enforcement authorities further to relevant disclosure requests made on the basis of a Mutual Legal Assistance Treaty (MLAT), which allow generally for the exchange of admissible evidence and information in criminal matters.*
- *In particular with regard to requests made by US Authorities, we note that a MLAT is in force between the U.S. and the E.U. since 2003* ***(7)****. The MLAT between the U.S. and the E.U. applies in conjunction with MLATs concluded between various E.U. Member States and the U.S. and currently in force. Greece and the U.S. have signed a MLAT* ***(8)****, which is in force since November 20th, 2001 and its scope covers the assistance in connection with the investigation, prosecution and prevention of offenses and in proceedings related to criminal matters (including organized crime, murder, etc.). Such assistance includes (a) providing documents and records; (b) locating or identifying persons or items; (c) executing searches and seizures.*

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

(8) Treaty with the Hellenic Republic on mutual legal assistance in criminal matters, Treaty Doc. 106-18

GEORGE A. BALLAS

REFERENCES

▪ Le Mexique est un Etat fédéral constitué de 32 entités (un District fédéral siège des autorités fédérales et 31 Etats).

▪ Chaque Etat est doté de sa propre constitution, auquel s'ajoute la Constitution fédérale **(1)** qui organise le pays en différents niveaux (fédéral, étatique et municipal). La répartition des compétences entre ces différents niveaux est fixée par l'article 73 de la Constitution fédérale.

(1) Constitución Política de los Estados Unidos Mexicanos
Version espagnole
Version française (2005)

▪ La loi sur les archives fédérales, promulguée le 23 janvier 2012 **(2)**, encadre l'organisation et la conservation des archives détenues par les entités fédérales et instaure des mécanismes permettant de coordonner la conservation des archives détenues par les autorités étatiques et municipales ainsi que par celles du District fédéral de Mexico.

(2) Ley Federal De Archivos
Version espagnole

▪ En outre, le ministère de la Fonction publique (Secretaría de la Función Pública) a adopté en 2011 un cadre juridique pour l'interopérabilité et l'open data de l'administration publique fédérale **(3)**. Il renferme les règles à suivre par les entités fédérales pour l'intégration de processus en matière de services numériques, ainsi que des mécanismes de partage d'informations destinés à améliorer la fonction publique fédérale. Ces règles font notamment référence aux notions de « cloud computing », de « cybersécurité » et de « gouvernance numérique ».

(3) Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal
Version espagnole

▪ En outre, différents textes organisent l'accès par les autorités aux données à caractère personnel, qu'elles soient stockées dans le cloud ou dans des fichiers su support papier ou électronique.

▪ **Code pénal fédéral**

▪ En matière pénale, l'article 180 du code pénal fédéral **(4)** confère aux procureurs et aux juges de larges pouvoirs d'accès aux informations détenues par des personnes publiques ou privées.

(4) Código Penal Federal
Version espagnole

▪ **Loi fédérale sur la transparence et l'accès à l'information publique gouvernementale**

▪ Cette loi **(5)** permet aux personnes privées d'accéder à des informations de nature publique. Le droit d'accès aux informations publiques doit être interprété conformément à plusieurs textes (Constitution fédérale mexicaine, Déclaration universelle des droits de l'homme, Pacte international relatif aux droits civils et politiques, Convention américaine relative aux droits de l'homme, Convention sur l'élimination de toutes les formes de discrimination à l'égard femmes, et autres instruments internationaux souscrits et ratifiés par le Mexique) et l'interprétation de ceux-ci par les organismes internationaux spécialisés.

(5) Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
Version espagnole (2012)
Version anglaise (2002)

▪ La loi fédérale sur la transparence et l'accès à l'information publique gouvernementale garantit la protection des secrets commerciaux, des données à caractère personnel et d'autres types d'informations sensibles en son article 22 : « Le consentement d'entités privées n'est pas requis pour l'obtention de données personnelles dans les cas suivants : I. ... II. Si nécessaire pour des raisons statistiques, scientifiques ou d'intérêt général tel que prévu par la loi, après mise en œuvre d'un procédure permettant d'empêcher que les données à caractère personnel soient associées à l'entité privée à laquelle elles se réfèrent ; III. Si elles sont échangées entre les parties ou entre des départements et des agences, à condition que ces données soient utilisés dans l'exercice de leur autorité respective ; IV. Si exigé par une ordonnance du tribunal ; V. Si elles ont été fournies à

des tiers dans le cas où un service régi par un contrat nécessite des données personnelles. Lesdits tiers ne peuvent utiliser les données personnelles pour d'autres finalités que celles pour lesquelles elles ont été transmises ; et VI. Dans tous les autres cas prévus par la loi. »

- **Loi sur la propriété industrielle**

- Associé au Code pénal fédéral, l'article 86 bis de la loi sur la propriété industrielle **(6)** réglemente les « secrets commerciaux » : « Lorsque l'une des parties impliquées dans une procédure judiciaire ou administrative est tenue de révéler un secret commercial, l'autorité saisie de l'affaire prend les mesures nécessaires afin d'empêcher sa divulgation à des tiers n'ayant aucun lien avec le litige. Aucune partie intéressée ne peut, en aucun cas, révéler ou utiliser le secret commercial visé au paragraphe précédent ».

(6) Ley de la Propiedad Industrial
Version espagnole

- **Loi fédérale sur la protection des données personnelles détenues par des personnes privées**

- Cette loi **(7)** a été promulguée afin d'encadrer la collecte, le traitement et la communication légitimes des données à caractère personnel détenues par des parties privées.

(7) Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Version espagnole
Version anglaise

- Aux termes de son article 10 : « Le consentement au traitement de données personnelles n'est pas requis lorsque : I. Une loi le prévoit ; II. Les données sont contenues dans des sources accessibles au public ; III. Les données personnelles sont soumises à une procédure de dissociation préalable ; IV. Le traitement a pour finalité le respect d'obligations dans le cadre d'une relation juridique entre le propriétaire des données et le responsable du traitement ; V. Il s'agit d'une situation d'urgence qui pourrait potentiellement nuire à une personne dans sa personne ou ses biens ; VI. Il est nécessaire pour les soins médicaux, la prévention, le diagnostic, la prestation de soins de santé, le traitement médical ou la gestion des services de santé, dans le cas où le propriétaire des données se trouve dans l'incapacité de donner son consentement dans les conditions établies par la loi générale sur la santé ou d'autres lois applicables, et ledit traitement de données est effectué par une personne soumise à une obligation de secret professionnel ou à une obligation équivalente ; ou VII. Une autorisation est délivrée par une autorité compétente ».

- **Loi fédérale sur le droit d'auteur**

- La loi fédérale sur le droit d'auteur **(8)** faisait déjà référence aux informations et données privées contenues dans les bases de données dès sa promulgation en 1996. Elle dispose en son article 109 : « L'accès aux informations de caractère privé concernant les personnes qui sont contenues dans les bases de données visées à l'article précédent, ainsi que la publication, la reproduction, la divulgation, la communication au public et la transmission de ces informations, nécessitent l'autorisation préalable des personnes concernées. Les dispositions qui précèdent ne s'appliquent ni aux enquêtes menées par les autorités responsables de l'administration et de l'application de la justice conformément à la législation applicable, ni à l'accès aux archives publiques par des personnes autorisées par la loi, à condition que l'accès ait lieu dans le respect des procédures adéquates ».

(8) Ley Federal del Derecho de Autor
Version espagnole

- Les textes ci-dessus s'appliquent au niveau fédéral. Au niveau étatique, chaque Etat possède sa propre loi sur la transparence et l'accès à l'information publique et ses propres autorités chargées de veiller à son application au sein de son territoire.

ENRIQUE OCHOA DE GONZÄLEZ ARGÜELLES

- *Mexico is organized and structured into 32 different legal entities. It has a Federal District in which the Federal offices reside and 31 States.*
- *Each State has its own Constitution, and a Federal Constitution **(1)** by which the country is organized in different levels (Federal, State and Municipal). In line with the above, article 73 of the Federal Constitution sets forth the topics which will be regulated by a Federal Law, a State Law and a Municipal Law.*
- *On January 23, 2012, the Federal Archive Law **(2)** was enacted and same refers to the organization and conservation of archives hold by Federal entities, and the mechanism to coordinate the conservation of archives hold by the State and Municipal authorities and of the Federal District of Mexico.*
- *Previously, on 2011, the Ministry of Public Office (Secretaría de la Función Pública) enacted the Legal Framework for Interoperability and Open Data of the Federal Public Administration **(3)**. This is the principles and policies by which Federal entities will integrate processes regarding digital services, as well as share information in order to improve federal public service. These rules include concepts such as "cloud computing", "cybersecurity" and "digital governance".*
- *There are different scenarios in which governmental entities may access to personal data, being same stored in the "cloud" or in any other file, physical or electronic.*
- ***Federal Criminal Code (4)***
- *Article 180 grants the prosecutors and the judges wide and ample capacities to request information either form other governmental authorities or to private parties for the purposes of criminal proceedings*
- ***Federal Transparency and Access to Governmental Public Information Law (5)***
- *These legal provisions allow private parties to access information of public nature. The right to access public information shall be interpreted in terms of the Federal Constitution; the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights; the American Convention on Human Rights; the Convention on the Elimination of All Forms of Discrimination against Women, as well as any other international instruments subscribed and ratified by the Mexico and the interpretation thereof by specialized international entities.*
- *This Law provides protection for trade secrets, personal data and other type of sensitive information, and in articles 22, provides: "No consent of private entities shall be required to provide personal data in the following cases: I. ... II. If required for statistical, scientific or reasons of a general interest as provided by the law, after a procedure whereby the personal data may not be associated to the private entity they refer to; III. If they*

REFERENCES

(1) Constitución Política de los Estados Unidos Mexicanos
Spanish version
English version

(2) Ley Federal De Archivos
Spanish version

(3) Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal
Version espagnole

(4) Código Penal Federal
Spanish version

(5) Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
Spanish version (2012)
English version (2002)

are exchanged between disclosing parties or between departments and agencies, provided that the same are used in the exercise of their respective authority; IV. If required by court order. V. If provided to third parties in case a service is contracted that requires personal data. Said third parties may not use the personal data for purposes other than those for which they were transmitted, and VI. In the other cases provided by the law."

- ***Industrial Property Law (6)***

- *Article 86 BIS regulates, along with the Federal Criminal Code "trade secrets", and states: "Where one of the parties involved in any judicial or administrative proceeding is required to reveal a trade secret, the authority hearing the proceeding shall take the necessary measures to prevent its disclosure to third parties having no connection with the dispute. No interested party may, in any event, reveal or make use of the trade secret referred to in the previous paragraph."*

(6) Ley De La Propiedad Industrial
Spanish version

- ***Federal Law on Protection of Personal Data Held by Private Parties***

- *This Law **(7)** was enacted to regulate the legitimate collection, processing and disclosure of personal data held by the private parties.*

- *Furthermore, article 10 establishes that: "Consent for processing of personal data will not be necessary where: I. Any Law so provides; II. The data is contained in publicly available sources; III. The personal data is subject to a prior dissociation procedure; IV. It has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller; V. There is an emergency situation that could potentially harm an individual in his person or property; VI. It is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data owner is unable to give consent in the terms established by the General Health Law and other applicable laws, and said processing of data is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or VII. A resolution is issued by a competent authority.*

(7) Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Spanish version
English version

- ***Federal Copyright Law***

- *Federal Copyright Law **(8)** enacted in 1996 already makes reference to private information and data contained in databases: "Art. 109. Access to information of private character concerning persons that is contained in the databases referred to in the foregoing article, and also the publication, reproduction, disclosure, communication to the public and transmission of such information, shall require prior authorization by the persons concerned. The foregoing shall not apply to investigations by the authorities responsible for the administration and enforcement of justice according to the relevant legislation, or to access to public archives on the part of persons authorized by the law, provided that the access is had according to the relevant procedures".*

(8) Ley Federal del Derecho de Autor
Spanish version

- *The States of the country have their own Transparency and Access to Public Information Laws, as well as Agencies for the enforcement of same within their territories.*

ENRIQUE OCHOA DE GONZÁLEZ ARGÜELLES

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*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	marc.gallardo@lexing.es
Etats-Unis *USA*	IT Law Group	Françoise Gilbert	+ 1 (650) 804 1235	fgilbert@itlawgroup.com
France *France*	Alain Bensoussan-Avocats	Alain Bensoussan	+33 1 82 73 05 05	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 & Associés Zineb Laraqui	Bassamat Fassi-Fihri Zineb Laraqui	+ 212 522 26 68 03 + 212 66 144 8284	contact@cabinetbassanat.com zlaraqui@zineblaraqui.com
Mexique *Mexico*	Langlet, Carpio y Asociados, S.C.	Enrique Ochoa De Gonzälez 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, 58 boulevard Gouvion-Saint-Cyr, 75017 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