JTIT Internationale n° 7 - juin 2014
Special international issue # 7– June 2014

ALAIN BENSOUSSAN

Juristendances Informatique et Télécoms

Le réseau Lexing vous informe - The Lexing Network informs you

ACCÈS ET MAINTIEN FRAUDULEUX DANS UN STAD

UNAUTHORIZED ACCESS TO IT SYSTEMS

La cybercriminalité au cœur de l'actualité : Focus sur l'affaire « Bluetouff »

▪ La sécurité des réseaux et de l'information est aujourd'hui l'une des préoccupations majeures des entreprises et des particuliers dans tous les pays du monde. Preuve en est de la recrudescence des attaques à grande échelle dont ont été récemment victimes Spotify, eBay, Orange, Barclays, Target, AOL… et du séisme Heartbleed. Les enjeux sont importants : piratage des systèmes de traitement automatisé de données (STAD), usurpation d'identité, perte d'informations confidentielles et stratégiques, pertes de marchés, vol de données personnelles, e-réputation etc. et lourds de conséquences sur le plan financier. En 2013 le coût le moyen d'une cyberattaque pour une grande entreprise s'élevait à 566 000 USD.

▪ Face à ces menaces protéiformes et transnationales, la coopération internationale en matière de lutte contre la cybercriminalité s'est organisée, notamment avec l'adoption de la convention dite de « Budapest » en 2001 ou encore de la Directive européenne 2013/40/EU. La France dispose, quant à elle, d'un arsenal répressif efficient pour sanctionner les actes de piratage informatique (articles 323-1 et suivants du Code pénal) depuis 1988. Dans l'hexagone, ce domaine est d'ailleurs riche en actualité : instauration d'un « préfet cyber », arrestations « Blackshades », et condamnation de « Bluetouff ».

▪ C'est sur cette dernière affaire, qui a agité la blogosphère, que le présent numéro vous propose de s'arrêter : un internaute qui avait consulté et téléchargé, via une simple recherche Google, des documents normalement protégés d'un organisme public mais rendus accessibles en raison d'une défaillance de son système de sécurité informatique, a été relaxé du chef d'accès frauduleux dans un STAD, mais condamné en appel pour maintien frauduleux dans un STAD et vol de fichiers informatiques.

▪ Comment l'affaire Bluetouff aurait-elle été traitée par les juridictions étrangères ? Qu'en est-il de la législation relative au hacking dans les autres pays du monde ?

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde.

Cybercrime: Recent Highlights and Focus on the "Bluetouff" Case

▪ *Network and information security is today one of the major concerns of businesses and consumers of all countries around the world. Amid the growing number of large scale attacks affecting for example Spotify, eBay, Orange, Barclays, Target, AOL…., the Heartbleed bug and its aftermath are a prime example of that. The stakes are high: IT systems intrusion, identity theft, loss of confidential and strategic information, loss of markets, personal data theft, e-reputation.... and the costs are heavy. In 2013, the average damage suffered as a result of a cybersecurity incident for a large company was assessed at USD 566,000.*

▪ *In the face of such these multifaceted, cross border threats, the international community has adopted several instruments in order to develop an integrated approach and tackle cybercrime, including the Budapest Convention in 2001 and EU Directive 2013/40/EU. France has had a comprehensive and efficient body of law to crack down on hacking (articles 323-1 et seq. of Penal Code) since 1988. In France, cybercrime recently hit the headlines: creation of a "cyber prefect", "Blackshades" arrests and "Bluetouff" ruling.*

▪ *This issue will precisely focus on this last case, which created a stir in the blogosphere: an Internet user who consulted and downloaded, via a simple Google search, documents normally protected from a French government agency that were made available due to a security bug of its extranet, was found not guilty of unauthorized access to IT systems but judgment was entered against him for remaining in the IT system and data theft.*

▪ *How the Bluetouff case would have been decided by foreign judges? What about the hacking legislation in the other countries of the world?*

The Lexing® network members provide a snapshot of the current state of play worldwide

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.

VIRGINIE BENSOUSSAN-BRULÉ

▪ Vue d'outre-Rhin, la condamnation du militant français Olivier L., connu sous le pseudonyme Bluetouff, pour « piratage » en raison de l'accès et de la copie de fichiers non protégés stockés sur un serveur Web soulève des questions intéressantes **(1)**.

▪ En effectuant une recherche sur Google, Bluetouff a accédé à des fichiers hébergés sur le site d'une agence publique française, qu'il a ensuite copiés et rendus disponibles en ligne sur un site journalistique auquel il participe. Il s'est avéré qu'une défaillance du système de protection par mot de passe du site extranet de l'agence française avait eu pour effet de rendre ses fichiers librement accessibles sur internet pour tous les internautes, y compris les moteurs de recherche.

▪ S'il semble peu probable que les tribunaux allemands seraient arrivés à la même conclusion pour des faits similaires, les actes de ce type sont également répréhensibles en Allemagne.

▪ Tout comme en droit français, le **Code pénal allemand (2)** sanctionne l'accès non autorisé à des données, mais il y subordonne en revanche la violation d'une mesure de sécurité. En effet, l'Allemagne fait partie des pays qui ont utilisé l'option offerte par les articles 2 de la décision-cadre 2005/222/JAI **(3)** et de la Convention sur la cybercriminalité du Conseil de l'Europe **(4)** consistant à exiger que ce type d'accès ne soit érigé en infraction pénale qu'en cas d'infraction à une mesure de sécurité.

▪ Ainsi, l'incrimination d'espionnage informatique (« **Ausspähen von Daten** ») visée par le Code pénal allemand, modifié en 2007, suppose la réunion de deux éléments : l'existence d'une mesure de sécurité et la violation de ladite mesure. Il convient donc tout d'abord de s'assurer de **l'existence d'une mesure de sécurité**. Par « mesure de sécurité », on entend une mesure mise en place dans le but d'empêcher tout accès par une personne non autorisée. Selon la jurisprudence du Bundesgerichtshof, la Cour fédérale de justice allemande, une mesure de sécurité doit contraindre un « hacker » à accéder aux fichiers de manière différente de la manière normale d'accès **(5)**. Dans cet esprit, le fait d'exiger des identifiants de connexion pour accéder à un extranet constitue bien une mesure de sécurité. Ensuite, il faut **établir que cette mesure de sécurité a été transgressée**. La transgression doit se dérouler sur un certain laps de temps et impliquer des efforts techniques considérables **(6)**. Or, en l'espèce, le contenu était disponible gratuitement sur le Web et était même indexé par Google. Aucune violation de la mesure de sécurité mise en place par l'agence française n'était donc nécessaire afin d'accéder aux fichiers en cause. Le deuxième élément n'est donc pas satisfait. A cet égard, il faut relever qu'en Allemagne sont assimilés à une absence de violation les cas où la mesure de sécurité peut être contournée facilement et sans effort, ou est inefficace pour des non-initiés **(7)**.

▪ Si le chef d'accès frauduleux ne peut être retenu, un autre angle d'attaque reste cependant possible : punir la copie et la distribution des fichiers auxquels il a été accédé frauduleusement en recourant aux **dispositions pénales en matière de droit d'auteur**. Les fichiers concernés doivent bien évidemment pouvoir être considérés comme une œuvre protégeable par le droit d'auteur. Toutefois, dans le cas présent, une telle action aurait peu de chances de prospérer, car d'autres aspects rentrent en ligne de compte, notamment la liberté d'expression et les droits de la presse.

▪ En somme, l'affaire Bluetouff rappelle aux entreprises et aux organismes publics que, quel que soit le pays, ils doivent redoubler de précautions et veiller à **mettre en œuvre des mesures de sécurité fonctionnelles et efficaces**. Si l'accès frauduleux cause une perte de données, une action en justice, même si elle se conclut par l'allocation de dommages et intérêts substantiels, constituera rarement une réparation adéquate aux **préjudices financiers ou d'image** subis. Il ne fait pas oublier qu'en cas de **faille de sécurité** concernant des données personnelles de clients, de salariés ou de tiers, les législations en matière de protection de données trouvent également à s'appliquer, et que celles-ci imposent notamment des **obligations de notification** aux personnes concernées et au public.

REFERENCES

(1) Cf. « French journalist "hacks" govt by inputting correct URL, later fined $4,000 for publishing public documents » Megan Geuss, 9-2-2014, arstechnica.com

(2) *« Celui qui, sans autorisation, obtient accès pour lui ou une autre personne, à des données qui ne lui sont pas destinées et qui sont protégées spécialement contre les accès non autorisés, en contournant cette protection, est puni d'une peine d'emprisonnement allant jusqu'à trois ans ou d'une peine d'amende ».* Article. 202a 1° du Code pénal allemand („Ausspähen von Daten"), en allemand et en anglais

(3) Décision-cadre 2005/222/JAI : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:FR:PDF

(4) Convention sur la cybercriminalité : http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm

(5) Bundesgerichtshof, 6-7-2010 – affaire n°4 StR 555/09 disponible (en allemand) à l'adresse http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=52875&pos=2&anz=634

(6) Cf. historique législatif : BT-Drs 16/3656 p. 10 (http://dip21.bundestag.de/dip21/btd/16/036/1603656.pdf)

(7) Cf. historique législatif : BT-Drs 16/3656 p. 10 (http://dip21.bundestag.de/dip21/btd/16/036/1603656.pdf)

TIM CAESAR
&
FRANK FALKER

▪ *The conviction of French activist Olivier L., known as "Bluetouff", on "Hacking" charges for accessing and copying unprotected files stored on a web server raises interesting questions* ***(1)***.

▪ *The files were hosted by a French government agency, when Bluetouff stumbled upon them via a Google search. He subsequently made some of the agency's files available as part of a journalistic venture he participated in. As a security measure to prevent access to these files, the aggrieved party had improperly implemented a password protection on its extranet which made the files available for everyone on the web, including search engines.*

▪ *Whereas it seems unlikely that German courts would ultimately convict a "Hacker" for similar actions in the way the French court did, it is not a far-fetched assumption that this might happen in Germany as well.*

▪ *The* ***relevant German statute*** *as amended in 2007* ***(2)*** *is based on Article 2 of the Framework Decision 2005/222/JHA* ***(3)*** *and Article 2 of the Cybercrime Convention of the Council of Europe* ***(4)***. *Germany has used the option provided by the Framework Decision and the Cybercrime Convention to require that a security measure must be infringed in order for the crime to be committed.*

▪ *It would be debatable whether a security measure in the meaning of the law was even in place. A* ***security measure*** *must be able to prevent unauthorized access and be put in place with this intent. According to the German Federal Supreme Court, this means that the "Hacker" has to choose a different way to access the files because of the security measure* ***(5)***. *With this in mind, the required – or merely, intended – login per se appears to fit the definition of a security measure. However, as a further requirement, a security measure must be infringed. Such* ***infringing of a security measure*** *must take some time and involve considerable technical effort* ***(6)***. *In the case at hand, the content was freely available from the web and even indexed by Google. It was not necessary to infringe the (intended) security measure in order to access the files. Cases in which the bypassing of a security measure is possible without effort or in which the measure is ineffective even to hold off non-experts are not within the scope of the statute* ***(7)***.

▪ *Besides the hacking charges, it could be possible to harness* ***criminal statutes of copyright law*** *to punish the copying and distribution of such files. The files would have to be a work in the meaning of copyright law. A conviction is unlikely in the case against Bluetouff, as there are further aspects involved, especially freedom of speech and press privileges. In other cases, this might be an option.*

▪ *As a result, unsurprisingly, companies just like agencies will have to take utmost care to* ***implement functional and effective security measures***. *Criminal charges in case of data loss will pretty much never be an adequate "tool" to remedy* ***economic and reputation loss***. *Where personal data of customers, employees, or other individuals is concerned,* ***data protection regulations*** *come into play – including, for example, notification duties to individuals respectively to the public.*

REFERENCES

(1) See: "French journalist "hacks" govt by inputting correct URL, later fined $4,000 for publishing public documents", Megan Geuss, 9 Feb. 2014, arstechnica.com

(2) *"Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine".* Sec. 202a(1) of the German Criminal Code: ("*Ausspähen von Daten*": in German and in English

(3) Framework Decision 2005/222/JHA: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF

(4) Cybercrime Convention: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

(5) Federal Supreme Court, 6 July 2010 – case no. 4 StR 555/09 at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=52875&pos=2&anz=634

(6) See the legislative history: BT-Drs 16/3656 p. 10 at http://dip21.bundestag.de/dip21/btd/16/036/1603656.pdf

(7) Compare the legislative history: BT-Drs 16/3656 p. 10 at http://dip21.bundestag.de/dip21/btd/16/036/1603656.pdf

TIM CAESAR
&
FRANK FALKER

▪ L'affaire dite « Bluetouff », du nom de ce blogueur français condamné pour avoir récupéré des informations confidentielles d'un serveur de l'ANSES rendues librement accessibles par le biais du moteur de recherche de Google suite à une erreur de paramétrage, a fait grand bruit parmi les afficionados du web et les partisans des « **white hat** » **(1)**. Ceux-ci se sont insurgés contre la condamnation d'un des leurs, dont les actions n'avaient finalement eu comme conséquence qu'une mise en évidence d'une faille grossière de sécurité.

▪ Pourtant, même si certains sociologues s'interrogent sur l'application du terme « crime » en matière de hacking **(2)**, singulièrement de hacking éthique **(3)**, dura lex, sed lex.

▪ L'arrêt (le jugement d'instance ordonnant la relaxe) de condamnation de la Cour d'Appel de Paris **(4)** aurait sans doute été identique s'il avait été prononcé par la Cour d'Appel de Bruxelles.

▪ En effet, en Belgique, les infractions d'accès non autorisé à et de maintien non-autorisé dans un système informatique ont été introduites à l'**article 550 bis du Code pénal (5)** par la **loi du 28 novembre 2000 relative à la criminalité informatique (6)**.

▪ Aux termes de cet article, celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient est puni d'une peine d'emprisonnement ou d'amende, majorée en cas d'intention frauduleuse.

▪ Vu l'examen des faits, ni l'intention frauduleuse, ni l'accès non-autorisé n'auraient été retenus par la Cour dès lors qu'il était établi que l'**accès** avait été réalisé **par erreur**, les données étant librement accessibles par le biais du moteur de recherche Google, une **faille de sécurité** ayant permis l'indexation.

▪ Par contre, l'infraction **maintien non-autorisé** dans le système aurait également été retenue en Belgique puisqu'une fois l'accès accidentel réalisé, le « pirate » ne pouvait plus ignorer qu'il se trouvait dans un espace non-autorisé. Le fait de rester connecté au système, de le parcourir et de télécharger des fichiers constituent dès lors l'infraction de maintien non-autorisé dans un système informatique au sens de l'article 550 bis du Code pénal belge.

REFERENCES

(1) Hackers éthiques

(2) V. à ce sujet notamment, L. DUFF, S., GARDINIER, "Computer crime in the global village – strategies for control and regulation – in defence of the hacker", International Journal of the sociology of Law, 24, 1996, p. 213. Et par analogie avec la "criminalité en col blanc": J., MUNCIE, E., McLAUHLIN (eds), "The problem of crime", 2nd ed, London: Sage Publication, 2001, p.10, M., GOTTFREDSON, T., HIRSCHI, "A general theory of crime", Stanford University Press, 1990, p.183

(3) P. HIMANEM, The Hacker Ethic and the Spirit of the Information Age, London: Vintage, 2001

(4) Paris, Pole 4, 10ème Ch., 5 février 2014, accessible sur http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4011 (visité le 28 avril 2014).

(5) Art. 550bis §1er : « Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement. Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans. »

(6) Loi du 28 novembre 2000 relative à la criminalité informatique
Cf. commentaire M.B. 3 février 2001. Pour une analyse plus détaillée de la loi, V. O. LEROUX, Les infractions contre les biens, Bruxelles Larcier, 2008 p. 365-453

JEAN-FRANÇOIS HENROTTE

▪ *The so-called "*Bluetouff*" case, from the name of a French blogger convicted for having retrieved from the server of ANSES confidential information freely accessible through the Google search engine as a result of incorrect settings has caused quite a stir among the Web community and* ***"white hat"*** *supporters* ***(1)****. They have rebelled against the conviction of one of them, whose actions had ultimately resulted in the disclosure of a gross security breach.*

▪ *However, even if some sociologists question the application of the term "crime" to hacking* ***(2)****, particularly ethical hacking* ***(3)****, it nonetheless remains that* dura lex, sed lex.

▪ *The appeal judgment (the first instance judgment had ordered the release) of the Court of Appeals of Paris* ***(4)*** *would probably have been the same if it had been issued by the Court of Appeals of Brussels.*

▪ *Indeed, in Belgium, the unauthorized access to and maintenance in an IT system are offenses, which have been introduced in* ***Article 550 bis of the Penal Code (5)*** *by the* ***Computer Crime Act of 28 November 2000 (6)****.*

▪ *Under this Article, anyone who, knowingly and without authorization, gains access to or remains in a computer system shall be punished by imprisonment and/or a fine, which shall be increased in case of fraudulent intent.*

▪ *Having regard to the facts of the Bluetouff, neither the fraudulent intent nor the unauthorized access would have been accepted by a Belgian Court to the extent that it was established that* ***access*** *was made* ***in error****, as the data was freely accessible through the Google search engine, due to a* ***security flaw*** *that allowed its indexation.*

▪ *On the other hand, the offense for* ***unauthorized maintenance in the system*** *would have also been retained in Belgium since once accidentally accessing a system, the "pirate" could no longer ignore that he was in an unauthorized area. Staying connected to the system, browsing and downloading files constitute the offense of unauthorized maintenance in a computer system within the meaning of Article 550 bis of the Belgian Penal Code.*

REFERENCES

(1) Ethical computer hackers

(2) See in particular L. DUFF, S. GARDINIER, "Computer crime in the global village – strategies for control and regulation – in defence of the hacker", International Journal of the sociology of Law, 24, 1996, p. 213. And, by analogy with white collar crime: J., MUNCIE, E., McLAUHLIN (eds), "The problem of crime", 2nd ed, London: Sage Publication, 2001, p.10, M., GOTTFREDSON, T., HIRSCHI, "A general theory of crime", Stanford University Press, 1990, p.183

(3) P. HIMANEM, The Hacker Ethic and the Spirit of the Information Age, London: Vintage, 2001

(4) Paris, Pole 4, 10th Ch., 5 Feb. 2014, accessible on http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4011 (last visited: 28 April 2014).

(5) Art. 550bis §1er: Any person who accesses or maintains access to a computer system, while knowing that he is not authorized to do so, shall be punished by a term of imprisonment between 3 months to 1 year and to a fine between €26 to €25,000 or one of these sanctions. Where the offence stated in §1 above is committed with fraudulent intent, the term of imprisonment shall be between 6 months to 2 years."

(6) Loi du 28 novembre 2000 relative à la criminalité informatique
See comment M.B. 3 février 2001. For a deeper analysis, see O. LEROUX, Les infractions contre les biens, Bruxelles Larcier, 2008 p. 365-453

JEAN-FRANÇOIS HENROTTE

▪ La **Constitution brésilienne**, promulguée en 1988 **(1)**, consacre le droit à la vie privée et au secret des communications privées, qu'elle considère comme des droits fondamentaux. A ce titre, elle garantit l'inviolabilité de l'intimité, de la vie privée, de l'honneur et de l'image des personnes et, par là même, l'inviolabilité de la correspondance et des communications télégraphiques, de données et téléphoniques. Il ne peut être dérogé à cette protection constitutionnelle que sur décision d'un tribunal dans le cadre d'une enquête criminelle **(2)**.

▪ Par conséquent, depuis 1988 au Brésil, personne, ni même l'Etat, ne peut violer le secret des données et des communications, et en cas de violation de cette interdiction, la personne physique ou morale lésée a le droit de réclamer une indemnisation civile si cette violation provoque un dommage matériel ou moral, tel qu'une atteinte à l'honneur ou à l'image **(3)**. Cependant, il a fallu attendre 2012 pour que le législateur brésilien se penche spécifiquement sur ces infractions dans le cyberespace. Tout est parti d'une affaire qui a suscité une vive émotion au Brésil, impliquant une célébrité locale qui a vu des photos intimes copiées et publiées sur Internet sans son consentement **(4)**. En réaction, la **loi n°12.737/2012** a été adoptée pour punir, notamment, les accès frauduleux à un système informatique d'une peine d'emprisonnement de trois mois à un an et d'une amende **(5)**.

▪ La loi n°12.737/2012 concerne tous types d'appareils électroniques, des ordinateurs aux téléphones portables, en passant par les smartphones, les tablettes, etc. En outre, il n'est pas nécessaire que l'appareil soit connecté à Internet. L'accès frauduleux peut également intervenir par n'importe quel procédé, par exemple à distance ou manuellement. Toutefois, aux termes de la loi **l'accès n'est frauduleux**, et donc constitutif d'une infraction, **que si les mesures de sécurité mises en œuvre pour protéger l'appareil n'ont pas été respectées**. A contrario, l'accès n'est pas considéré frauduleux s'il peut être facilement accédé à l'appareil sans avoir à enfreindre aucune sorte de restriction – à savoir, au sens large, tout système de sécurité mis en place par le propriétaire pour protéger ses données, tel que mot de passe, clé d'accès, antivirus... En d'autres termes, si le propriétaire n'a pas pris la peine de protéger l'accès à ses données, il est logique de présumer que le contenu de ces données est public, ou du moins que le propriétaire assume le risque d'un accès non autorisé.

▪ Quid de l'**élément moral de l'infraction** ? Là encore, le droit brésilien pose une limite quant à la nature frauduleuse de l'accès : l'auteur doit avoir spécifiquement pour intention d'obtenir, d'altérer ou de détruire les données ou les informations du système informatique accédé sans l'autorisation expresse ou tacite du propriétaire, ou d'y installer des vulnérabilités lui permettant d'en retirer un avantage indu. Autrement dit, si le contrevenant accède frauduleusement à un système informatique (par exemple en déchiffrant un mot de passe) sans avoir aucune des intentions prévues par la loi (par exemple si l'accès n'est motivé que par la curiosité), l'infraction n'est pas caractérisée et il ne pourra voir sa responsabilité pénale engagée. Bien entendu, ce dernier reste toutefois civilement responsable des actes commis et s'expose au paiement de dommages et intérêts. En effet, quiconque cause un dommage à autrui, même non intentionnellement, est tenu de le réparer.

▪ En outre, la même loi punit quiconque produit, distribue, vend ou diffuse un dispositif ou un programme informatique dans le but de permettre un accès frauduleux à un système informatique.

▪ Par ailleurs, **certains types d'accès sont plus sévèrement réprimés** en raison de la gravité de leurs conséquences, de la nature des informations concernées ou de la qualité des victimes. Il en est ainsi lorsque (a) l'accès entraîne des pertes économiques, (b) l'accès concerne des informations confidentielles, telles que des communications privées, des secrets commerciaux ou industriels, ou des informations qualifiées de confidentielles par la loi, ou est réalisé au moyen d'un contrôle à distance de l'appareil, (c) l'auteur divulgue ou commercialise les informations auxquelles il a accédé, (d) l'accès est commis à l'encontre d'agents de l'Etat, (président, gouverneurs, maires, président de la Cour suprême, président du Parlement, etc.).

▪ **En conclusion**, le Brésil réprime pénalement les accès frauduleux à des systèmes informatiques, mais ce type d'infraction est très encadré par la loi, le contrevenant ne pouvant être puni que dans certains cas spécifiques, mentionnés ci-dessus. Pour tous les autres cas n'entrant pas dans le champ de la législation pénale, il convient de rappeler que la Constitution brésilienne garantit le secret des données et des communications et donne droit à réparation en cas de dommage matériel ou moral. Ainsi donc, si l'action est fermée sur le terrain du droit pénal, la victime peut toujours agir devant les juridictions civiles.

REFERENCES

(1) Constitution fédérale du Brésil (Constituição da República Federativa do Brasil de 1988).

(2) Article 5 XII de la Constitution fédérale du Brésil : « le secret de la correspondance, des communications télégraphiques, de données et téléphoniques est inviolable sauf, en ce qui concerne ces dernières, par mandat judiciaire, dans les hypothèses et selon les formes que la loi établit aux fins d'enquête criminelle ou d'instruction de la procédure pénale. »

(3) Article 5 X de la Constitution fédérale du Brésil: « l'intimité, la vie privée, l'honneur et l'image des personnes sont inviolables ; le droit à l'indemnisation des dommages matériels ou moraux est assuré en cas de violation ».

(4) Carolina Dieckmann, une actrice populaire de telenovelas, s'était fait dérober, sur son ordinateur, des photos d'elle dénudée et avait subi un chantage avant de voir ses photos finalement diffusées sur plusieurs sites Web.
(cf. article de rfi.fr du 17-7-2012)

(5) Lei Nº 12.737, de 30 de Novembro de 2012 (également nommé « loi Dieckmann »), qui a introduit l'article 154-A dans le Code pénal brésilien sur les intrusions dans un système informatique (« *Invasão de dispositivo informático* ») (version anglaise non officielle)

SILVIA REGINA BARBUY MELCHIOR
&
LILIAN MALATEAUX

▪ *The **Brazilian Constitution** **(1)** considers privacy and private communications as fundamental rights and guarantees the inviolability of intimacy, private life, honor and image of the persons, ensuring to those who suffered any kind of violation the right to claim for indemnification for material and moral damages **(2)**. Also –and as a consequence-, the Brazilian Constitution guarantees the inviolability of correspondence, telegraphic, data and telephone communications. The only exception to this constitutional commandment is when the violation is determined by a court order to ensure a criminal investigation, as defined by law **(3)**.*

▪ *Therefore, since 1988, Brazil established that neither the government nor individuals could breach the secrecy of data and communications; also, it guaranteed the right to claim for civil indemnification if any eventual violation causes any material or moral harm including to the honor or image of an individual or a legal entity. However, it was only in 2012 that Brazil specifically criminalized the cybercrimes, and among them, the fraudulent access to an IT system. The law was created after an incident occurred with a local celebrity **(4)** that supposedly had her photos copied and published on the internet without her permission. As a response, the **law number 12.737/2012** criminalized the conduct of fraudulent access to an IT system, establishing the penalty of detention of 3 months to one year and a fine **(5)**.*

▪ *The crime is applied to any kind of electronic devices, including computers, cellphones, smartphones, tablets etc. In addition, the device does not necessarily have to be connected to the internet. By this statement the law establishes that the fraudulent access can be done by any method, for example, remotely or even manually. **The law considers crime and fraudulent the access only if the agent breaches any security mechanism**. If the agent can easily access the IT system without breaching any kind of barrier – that must be broadly interpreted as any security system that the owner has to protect the data such as password keys, antivirus, etc. – it cannot be considered a fraudulent access. The idea behind those boundaries is that if the owner did not worry about protecting the data, it is presumable that this content is public or at least he is assuming such risk.*

▪ *Another limit to criminalize the fraudulent access in Brazil is that t**he agent has to have specific intentions** when accessing the IT system. He must want to obtain, tamper or destroy the data or information of the system without any expressed or tacit permission of the owner, or, yet, the intention to install vulnerabilities to gain undue advantage. So, even if the agent makes a fraudulent access to anyone's IT system – by breaking a keyword password, for example -, but has none of those intentions required by the law – for example, he is just invading for curiosity -, he cannot be considered a criminal either. It doesn't mean on the other side that in terms of civil law he is not responsible for damages. Even without intention someone who causes damages to other, will be liable for indemnification.*

▪ *The same law also criminalizes those who produces, distributes, sells or disseminates device or computer program in order to enable the practice of fraudulent access to an IT system.*

▪ *In addition, there are **some situations** concerning the fraudulent access to IT systems classified in the law as more severe, which had the **penalty increased**, This is because they are considered more harmful to the Brazilian criminal system (implications for the economy or for the victim, type of information accessed, occupation of the victim that makes presumable that their IT system stores strategic information for the country). In short, there are four cases. The first one is when the access results in economic losses. The second one is when the access enables the agent to get the content of some specific confidential information – such as private communications, commercial or industrial secrets, information defined as confidential by law and also if the agent remotely controls the device. The third one is if the agent publicizes or commercializes the information he accessed. Moreover, the last one is if the crime is against the government's agents – such as the President, governors, mayors, president of the Supreme Court, president of the parliament etc.*

▪ ***In conclusion**, here in Brazil, we do have a criminal treatment for the theme of fraudulent access to IT systems, but it is very restricted to the situations defined by law. So the agent can only be punished by the state in some specific cases, as above mentioned. In all the other cases, even though we cannot criminalize the conduct, our Constitution guarantees the right to claim for indemnification if proved any material or moral damages, which can be discussed on the civil court.*

REFERENCES

(1) Federal Constitution of Brazil (Constituição da República Federativa do Brasil de 1988)

(2) Article 5(10) of the Federal Constitution of Brazil: "the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured".

(3) Article 5(12) of the Federal Constitution of Brazil: "the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts."

(4) Carolina Dieckmann, is a popular telenovela actress whose naked pictures were stolen on her computer and who was blackmailed before her pictures were released on various websites. (see Reuters article of 26-2-2013)

(5) Lei Nº 12.737, de 30 de Novembro de 2012 (also known as Dieckmann Act), which introduced Article 154-A into the Brazilian Penal Code about intrusion in IT systems (« *Invasão de dispositivo informático* ») (unofficial English translation)

SILVIA REGINA BARBUY MELCHIOR
&
LILIAN MALATEAUX

▪ Il n'existe pas de jurisprudence spécifique en Espagne en matière d'accès « frauduleux » à un système informatique contenant des données publiques non protégées, dont les faits seraient similaires à l'affaire récemment intervenue en France qui a fait l'objet de la décision rendue par la cour d'appel de Paris le 5 février 2014 (Olivier L. c/ Ministère de public).

▪ S'agissant de la découverte et de la révélation de secrets, **l'article 197 du Code pénal espagnol** punit d'une peine d'emprisonnement de un à quatre ans et d'une amende quiconque qui, pour découvrir les secrets ou violer l'intimité d'autrui, sans son consentement, s'empare de ses papiers, lettres, messages de courrier électronique ou tous autres documents ou effets personnels ou intercepte ses télécommunications ou utilise des dispositifs techniques d'écoute, de transmission, d'enregistrement ou de reproduction du son ou de l'image, ou tout autre signal de communication.

▪ Les mêmes peines sont prononcées à l'encontre de :

> (a) toute personne qui, sans y être autorisée, s'empare, utilise ou modifie, au préjudice d'un tiers, des données privées d'autrui de nature personnelle ou familiale qui sont conservées dans des fichiers ou des supports informatiques, électroniques ou télématiques, ou dans tout autre type de fichier ou registre public ou privé ; et
>
> (b) toute personne qui, sans y être autorisée, accède à ces données par tout moyen et les altère ou les utilise au préjudice du titulaire des données ou d'un tiers.

▪ En outre, une peine d'emprisonnement de deux à cinq ans s'applique si les données ou les faits découverts ou les images captées sont divulgués, révélés ou cédés à des tiers.

▪ Enfin, une personne qui commet les actes décrits dans le paragraphe précédent sans avoir participé à leur découverte, mais en connaissant l'origine illicite de ces faits ou données, est passible d'une peine d'emprisonnement de un à trois ans et d'une amende.

▪ Par conséquent, il semblerait que si les magistrats espagnols avaient à connaître d'une affaire semblable au cas Bluetouff, ceux-ci ne prononceraient pas le même verdict que leurs homologues français. En effet, au regard du droit espagnol, il est peu probable que ce comportement soit qualifié d'infraction pénale, en raison du fait que les informations en cause étaient mises à la disposition du public sur Internet.

REFERENCES

Código Penal
en espagnol et en français

Artículo 197:
1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
(...)

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. (…)".

MARC GALLARDO

▪ *There is no specific case law on "fraudulent" access to an IT system containing unprotected public data, as it exists in France after the decision issued by the Paris Court of Appeals on February 5 2014 (Olivier L. / Ministère public).*

▪ *On the discovering and revealing of secrets,* ***Article 197 of the Spanish Criminal Code*** *states that any individual who, for the purpose of discovering the secrets or violating the privacy of another and without the consent of the latter, takes possession of that individual's papers, letters, electronic mail messages or any other personal documents or belongings or intercepts his or her telecommunications or uses technical devices for listening, transmitting, recording or reproducing sound or images or any other communications signal, will be punished by imprisonment from between one and four years and a fine.*

▪ *The same punishment will be applicable to:*

> *a) any individual who, without authorization, seizes, uses or modifies, to the detriment of a third party, such private personal or family data of another individual as may be recorded on computer, electronic or telematic files or media, or in any other type of file or record, whether public or private; and*
>
> *b) any individual who, without authority, accesses such data by any means or alters or uses such data to the detriment of the owner of the data or of a third party.*

▪ *Punishment consisting of imprisonment from between two and five years will be imposed if the data or facts discovered or the images captured, are divulged, revealed or transferred to third parties.*

▪ *Lastly, punishment consisting of imprisonment from between one and three years and a fine will be imposed on any individual who, with prior knowledge of the illicit origin of such facts or data but without having taken part in their discovery, commits the acts described in the preceding paragraph.*

▪ *Therefore, in our opinion, in the case at hand it would be less likely that this conduct be punished, as a criminal offence according to Spanish Law, due to the fact the information is made publicly available on the Internet.*

REFERENCES

Código Penal
(in Spanish and in English)

Artículo 197:
1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
(…)

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. (…)".

MARC GALLARDO

▪ En France, les atteintes à un système de traitement automatisé de données (STAD) **(1)** sont réprimées par le Code pénal **(2)**. La récente affaire Bluetouff, ci-après analysée, permet de faire le point sur l'état du droit en la matière **(3)**.

▪ **Cadre juridique.** Le délit d'accès frauduleux dans un système de traitement automatisé de données est prévu et réprimé par l'article 323-1 du Code pénal aux termes duquel « le fait d'accéder (…), frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende ». L'auteur doit avoir eu conscience d'accéder anormalement dans le système de traitement automatisée de données. Il n'est en revanche pas nécessaire qu'il ait eu l'intention de nuire.

▪ Le délit de maintien frauduleux dans un système de traitement automatisé de données est prévu et réprimé par l'article 323-1 du Code pénal aux termes duquel « le fait (…) de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende ». Comme pour le délit d'accès frauduleux, le maintien doit être volontaire et l'auteur doit avoir eu conscience qu'il se maintenait anormalement dans le système.

▪ **Mesures de sécurité.** La protection du système par un dispositif de sécurité n'est pas une condition des incriminations d'accès et de maintien frauduleux dans un système de traitement automatisé de données : il suffit que le maître du système ait manifesté son intention d'en restreindre l'accès aux seules personnes autorisées **(4) (5)**.

▪ **Application dans l'affaire Bluetouff.**

▪ **Contexte.** Ayant constaté un accès frauduleux sur son serveur extranet, et la diffusion sur internet d'information confidentielles provenant de fichiers disponibles sur ce seul extranet, l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses), opérateur d'importance vitale (OIV) **(6)**, a déposé plainte devant le procureur de la République de Créteil.

Les services enquêteurs ont constaté que certains des contenus avaient été publiés sous le pseudonyme « Bluetouff », identifié comme étant Monsieur Olivier L.. Monsieur Olivier L était renvoyé devant le tribunal correctionnel des chefs d'accès et de maintien frauduleux dans un système de traitement automatisé de données et de vol de fichiers informatiques.

▪ **Relaxe en première instance.** Dans son jugement du 23 avril 2013 **(7)**, la 11e chambre correctionnelle du Tribunal de grande instance de Créteil a jugé qu'aucune des trois infractions poursuivies n'étaient constituées en l'espèce et a, en conséquence, relaxé le prévenu des fins de la poursuite. Le tribunal a en effet considéré que dès lors que l'Anses n'avait pas pris de mesure pour sécuriser son système informatique et n'avait pas « manifesté clairement l'intention de restreindre l'accès aux données (…) aux seules personnes autorisées », l'accès et le maintien frauduleux dans un système de traitement automatisé de données ne pouvaient être caractérisés.

En ce qui concerne le vol de fichiers informatiques, le tribunal a considéré qu'« en l'absence de toute soustraction matérielle de documents appartenant à l'Anses, le simple fait d'avoir téléchargé et enregistré sur plusieurs supports des fichiers informatiques de l'Anses qui n'en a jamais été dépossédée, puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose ».

Le parquet a fait appel du jugement.

REFERENCES

(1) Au sens large, un « système de traitement automatisé de données » s'entend de l'ensemble des éléments physiques et des programmes employés pour le traitement de données, ainsi que des réseaux assurant la communication entre les différents éléments du système informatique (ordinateurs, périphériques d'entrée/sortie, terminaux d'accès à distance, réseaux de communications électroniques etc.) Cf. Alain Bensoussan, Informatique, Télécoms, Internet, 5e édition (2012), n°2512 et suivants.

(2) Articles 323-1 à 323-7 du Code pénal, introduits par la loi sur la fraude informatique du 5 janvier 1988, dite « loi Godfrain ».

(3) Le niveau de la menace informatique est assez difficile à évaluer (cf. « Cybersécurité, l'urgence d'agir », Note d'analyse 324 - Mars 2013, Centre d'analyse stratégique). En 2012 en France, plus de 10 millions de personnes ont été victimes de la cybercriminalité (Etude Norton 2012). Plus spécifiquement, concernant les atteintes aux STAD, 1427 atteintes aux STAD ont été enregistrées en 2012 par les services de police et unités de la gendarmerie nationales (contre 419 en 2009) "(« Ondrp, Rapport annuel 2013 », dossier 2, section 6). En France, la cybersécurité représenterait plus de 50.000 emplois pour un chiffre d'affaires de 10 milliards d'euros (« L'explosion de la cybercriminalité » ww.lejdd.fr, 28-1-2013).

(4) Cf. notamment CA Paris, 5-4-1994. En outre, il a été jugé que l'existence d'une faille de sécurité ne constitue en aucun cas une excuse ou un prétexte pour l'auteur des faits d'accéder de manière consciente et délibérée à des données dont la non-protection pouvait être constitutive d'une infraction pénale (CA Paris, 12e ch. sect. A 30-10-2002 n°02/04867)

(5) Cela devient néanmoins une obligation dans le cadre du respect des dispositions de la loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés modifiée par la loi du 6 août 2004 pour respecter l'interdiction de diffusion d'informations à caractère personnel à des tiers non autorisés

▪ **Infirmation par la Cour d'appel.** Si, dans son arrêt du 5 février 2014 **(8)**, la Cour d'appel de Paris a confirmé le jugement du Tribunal de grande instance de Créteil du 23 avril 2013 en ce qu'il a jugé que le délit d'accès frauduleux dans un système de traitement automatisé de données n'était pas constitué en l'espèce, aux motifs que « l'accès (…) a en fait été permis en raison d'une défaillance technique concernant l'identification existant dans le système, défaillance que reconnaît l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail », elle a, en revanche, infirmé le jugement en ce qu'il a jugé que les délits de maintien frauduleux dans un système de traitement automatisé de données et de vol de fichiers informatiques n'étaient pas constitués en l'espèce.

La Cour a en effet considéré que « pour ce qui concerne les faits commis de maintien frauduleux dans un système de traitement automatisé de données et de vol,(…) il est constant que le système extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail n'est normalement accessible qu'avec un mot de passe dans le cadre d'une connexion sécurisée, que le prévenu a parfaitement reconnu qu'après être arrivé "par erreur" au cœur de l'extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail, avoir parcouru l'arborescence des répertoires et être remonté jusqu'à la page d'accueil, il avait constaté la présence de contrôles d'accès et la nécessité d'une authentification par identifiant et mot de passe ; qu'il est ainsi démontré qu'il avait conscience de son maintien irrégulier dans le système de traitement automatisé de données visité où il a réalisé des opérations de téléchargement de données à l'évidence protégées ; que les investigations ont démontré que ces données avaient été téléchargées avant d'être fixées sur différents supports et diffusées ensuite à des tiers ; qu'il est, en tout état de cause, établi qu'Olivier L. a fait des copies de fichiers informatiques inaccessibles au public à des fins personnelles à l'insu et contre le gré de leur propriétaire ; que la culpabilité d'Olivier L. sera donc retenue des chefs de maintien frauduleux dans un système de traitement automatisé de données et de vol de fichiers informatiques au préjudice de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail ».

L'incrimination de vol de fichiers informatiques a donc été reconnue par la Cour d'appel de Paris même en l'absence de « dépossession » du propriétaire des fichiers **(9)**.

▪ **Pourvoi en Cassation.** Le prévenu s'est pourvu en cassation.

▪ **En résumé.** En droit français:

- Les atteintes à un système de traitement automatisé de données, par quelque moyen que ce soit, sont sanctionnées par les articles 323-1 et suivants du Code pénal ;

- Le vol de fichiers informatiques, longtemps rejeté par les juridictions françaises, est une infraction aujourd'hui reconnue sur le fondement de l'article 311-1 du Code pénal disposant que le vol constitue la soustraction frauduleuse de la chose d'autrui.

(Loi du 6-1-1978 art. 34). Cf. Alain Bensoussan, Informatique et Libertés, 2e édition (2010)

(6) Les opérateurs d'importance vitale sont des opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, ou les établissements dont la destruction ou l'avarie peut présenter un danger grave pour la population. (Code de la défense, articles L.1332-1 et suiv. et R1332-1 et suiv.).
Ils sont soumis à des obligations particulières : formation des responsables, analyse de risque, identification de points d'importance vitale qui feront l'objet d'un plan particulier de protection (PPP) et d'un plan de protection externe (PPE), etc.

(7) TGI Créteil 23-4-2013 11e ch.

(8) CA Paris 5-2-2014 n°13/04833 Ministère public c. Olivier L.

(9) La doctrine et la jurisprudence ont toujours été très partagées sur cette question, le vol impliquant une atteinte à la propriété alors que l'information n'est pas un bien susceptible d'appropriation, hormis le cas des protections spécifiques du secret de certaines informations (défense nationale et secret de fabrique). A ce sujet cf. notamment CA Grenoble ch. corr., 15-2-1995, Cass. crim. 3-3-1992 pourvoi 90-82.964 et TGI Clermont-Ferrand 26-9-2011 ; *comp.*. CA Paris 13e ch. B 25-3-1993, CA Aix-en-Provence 29-2-2000 et CA Paris 13e ch. A 25-11-1992.

VIRGINIE
BENSOUSSAN-BRULÉ

▪ Under French law, unauthorized access and remaining in an IT system **(1)** are actionable under criminal law. This has been recently illustrated in a case known as the *Bluetouff* case, analyzed below.

▪ **Criminal code.** Article 323-1 of the French Penal Code states that "*Fraudulently accessing (…) within all or part of an automated data processing system is punished by two year's imprisonment and a fine of €30,000.*" The author must have been aware that he accessed abnormally in the IT system. A malicious intent is however not required.

▪ The same Article further states "*Fraudulently (…) remaining within all or part of an automated data processing system is punished by two year's imprisonment and a fine of €30,000.*" As for the offense of fraudulent access, remaining must be voluntary and the author must have been aware that his remaining in the system was abnormal.

▪ **Security measures.** Protecting the IT system by a security device is not a prerequisite: it is enough that the holder of the IT system expressed his intention to restrict access to authorized persons only.

▪ ***Bluetouff* case.**

- **Background.** It came to the attention of the French National Agency for Food Safety, Environment and Labor (ANSES), an operator of vital importance (OIV), that its extranet server had been fraudulently accessed and that confidential information only available in files on the extranet had subsequently been posted online. ANSES therefore filed a complaint with the public prosecutor of Créteil.

  The investigators found that some of these contents were published by someone using the alias "Bluetouff", later identified as Mr. Olivier L.

  Olivier L was prosecuted for (i) fraudulent access and (ii) fraudulent remaining in an automated data processing system as well as (iii) theft of computer files.

- **Trial court.** In its judgment of 23 April 2013, the 11th criminal chamber of the court of first instance of Créteil found none of the three offenses prosecuted existed in the case at hand and therefore acquitted the accused. For the court, since ANSES had not taken steps to secure its computer system and had not "*clearly expressed its intention to restrict access to data (...) to authorized persons only*" it could not claim any fraudulent access and remaining.

  Regarding the theft of computer files, the court held that "*in the absence of any physical removal of documents belonging to ANSES, the mere fact of having downloaded and saved on multiple IT media the computer files of ANSES — which has never been dispossessed thereof since this data, as it is an intangible element, remains available and accessible to all on the server — cannot constitute the material element of theft, namely the fraudulent appropriation of a thing belonging to another person, as this is an offense that requires the taking of a thing.*"

  The public prosecutor decided appealed the judgment.

REFERENCES

(1) French Penal Code refers to the concept of "automated data processing system". In a broad sense, it means all hardware and software used for data processing, as well as networks for communication between the different components of the computer system (computers, input/output devices, remote access terminals, electronic communications networks etc.) See Alain Bensoussan, Informatique, Télécoms, Internet, 5e édition (2012), n°2512 et seq.

(2) Articles 323-1 to 323-7 of French Penal Code, introduced by IT Fraud Act of 5 January 1988, known as Godfrain Act.

(3) The level of security threat is quite difficult to assess (see « Cybersécurité, l'urgence d'agir », Note d'analyse 324 - Mars 2013, Centre d'analyse stratégique). In 2012 in France, more than 10 million people were victims of cybercrime (Norton Study 2012). More specifically, 1,427 "STAD" attacks were recorded in 2012 by the French police and gendarmerie units (against 419 in 2009) ("Ondrp, Rapport annuel 2013", dossier 2, section 6). In France, cybersecurity would represent more than 50,000 jobs for a turnover of 10 billion euros ("L'explosion de la cybercriminalité" ww.lejdd.fr, 28-1-2013).

(4) See inter alia decision of court of appeals of Paris dated 5-4-1994. It was further considered that the existence of a security flaw did not constitute an excuse or pretext for the perpetrator to knowingly and deliberately access to data whose non-protection could constitute a criminal offense (CA Paris, 12e ch. sect. A 30-10-2002 n°02/04867)

(5) However this is an obligation under the provisions of the Data Protection Act of 6 January 1978, amended by the Act of 6 August 2004, to enforce the prohibition to disclose personal data to unauthorized parties (French Data Protection Act dated 6-1-1978 Art. 34). See Alain Bensoussan, Informatique et Libertés, 2e édition (2010)

(6) "Operators of Vital Importance" are public or private operators operating facilities or using installations and structures, whose unavailability could

- **Appeal Court.** By judgment of 5 February 2014, the Paris Court of Appeals upheld the decision of the trial court dated 23 April 2013 and confirmed there was no offense of fraudulent access to an IT system on the grounds that "*access (...) was actually allowed due to a technical failure in the login feature existing in the system, a failure that had been recognized by ANSES*".

  On the other hand, the appeal judges reversed the first instance ruling regarding the absence of fraudulent remaining and theft of IT files in an automated data processing system.

  According to the Court of Appeals "*with regard to the fraudulent maintaining in an automated data processing system and the theft of data, (...) it is clear that the extranet system of the National Agency for Food Safety, Environment and Labor is normally accessible only with a password through a secure connection, that the defendant fully recognized after he arrived "by mistake" at the heart of extranet of the National Agency for Food safety, Environment and Labor, that he browsed the directory tree and returned back to the home page, where he noted the presence of control access and the need for authentication by username and password; it is thus demonstrated that he was aware that he was remaining in an unauthorized manner in the automated data processing system he browsed and where he downloaded data that were obviously protected; investigations have shown that these data had been downloaded before being affixed to different media and then disseminated to other persons; it is, in any event, established that Oliver L. made copies of computer files inaccessible to the public for personal use without the knowledge and against the will of their owner; Olivier L. leaders should therefore be found guilty of fraudulently remaining in an automated data processing system and theft of computer files to the detriment of the National Agency for Food safety, Environment and Labor*."

  Note that the theft of computer files has been acknowledged by the Court of Appeals of Paris even in the absence of "deprivation" caused to the owner of the files.

- **What's next.** The story is to be continued as the accused lodged an appeal with the Cour de cassation.

- **In a nutshell.** Under French law:

  - Unauthorized access to automated data processing, by any means whatsoever, is sanctioned by Articles 323-1 et seq. of the Penal Code;

  - The theft of computer files, long rejected by the French courts, is an offense now recognized on the basis of Article 311-1 of the Penal Code, defining theft as the fraudulent appropriation of a thing belonging to another person.

VIRGINIE BENSOUSSAN-BRULÉ

significantly reduce the war or economic potential, the security or survivability of the nation, or facilities whose destruction or damage can be a serious danger to the population. (Defense Code, L.1332-1 et seq. and R1332-1 et seq.).
They are subject to specific obligations: training of managers, risk analysis, identification of points of vital importance that will be subject to a special protection plan ("PPP") and an external protection plan ("PPE") etc.

(7) TGI Créteil 23-4-2013 11e ch.

(8) CA Paris 5-2-2014 n°13/04833 Ministère public c. Olivier L.

(9) Legal writers and case law have always been divided on this issue, as theft involves damage to property while data is not capable of appropriation, except where certain information is specifically protected (national defense and trade secret).
On this topic see esp. CA Grenoble ch. corr., 15-2-1995, Cass. crim. 3-3-1992 pourvoi 90-82.964 and TGI Clermont-Ferrand 26-9-2011; *comp*. CA Paris 13e ch. B 25-3-1993; CA Aix-en-Provence 29-2-2000; and CA Paris 13e ch. A 25-11-1992.

▪ L'**article 370C** (paragraphe 2) **du Code pénal grec (1)** punit celui qui accède, sans droit, à des données stockées dans un ordinateur ou dans la mémoire périphérique d'un ordinateur, ou transmises par des systèmes de télécommunication, notamment en violation des interdictions ou des mesures de sécurité prises par le propriétaire des données, d'un peine d'emprisonnement pouvant aller jusqu'à trois mois ou d'une amende d'au moins 29 euros. En outre, si les données en cause relèvent des relations internationales ou de la sécurité de l'Etat, le coupable s'expose aux sanctions prévues par l'article 148 du Code pénal (traitant de l'espionnage et prévoyant une peine d'emprisonnement d'au moins un an, voire dans certaines circonstances, d'une réclusion à perpétuité). Si l'auteur de l'accès frauduleux est un salarié du propriétaire des données, l'acte n'est répréhensible que s'il a été explicitement interdit par le règlement intérieur ou par une décision écrite de l'employeur ou de son représentant.

▪ Bien que l'article 370C ait été introduit dans le Code pénal grec en 1988, c'est-à-dire à une époque où l'utilisation des ordinateurs personnels et des réseaux n'était bien entendu pas aussi répandue qu'elle l'est aujourd'hui **(2)**, la terminologie utilisée est assez large pour pouvoir englober en son sein les différents comportements apparus depuis, au fur et à mesure du développement exponentiel des technologies.

▪ **Accès « sans droit ».** En droit grec, l'accès présente un caractère frauduleux s'il intervient « sans droit », ce qui signifie que l'accès aux données n'est pas autorisé car (a) les données sont *traitées* comme étant de nature privée (en raison des protections techniques appliquées : mot de passe, pare-feu, mesures de cryptage, etc.) ou (b) les données sont *désignées* comme étant de nature privée, soit par la loi (informations classées secret défense, etc.) soit par leur titulaire (par exemple au moyen d'une mention spécifique dans les conditions d'utilisation).

▪ **Mesures de sécurité.** En ce qui concerne la nécessité de l'existence de mesures de sécurité, une interprétation littérale du texte, et en particulier l'utilisation du terme « notamment », ne laisse aucun doute quant au fait que le contournement de mesures de sécurité n'est pas une condition stricte pour l'application de l'article 370C (au contraire de la législation applicable dans nombreux autres pays). La référence aux mesures de sécurité n'a donc qu'un but illustratif, afin de guider l'application de sanctions adéquates.

▪ **Interdiction explicite par le propriétaire des données.** Que se passe t-il lorsqu'aucune mesure de sécurité n'est en place et qu'aucune autre réglementation pertinente ne s'applique ? Le propriétaire des données est-il tenu d'avoir formellement interdit l'accès à ses données ? En l'absence de jurisprudence hellénique en la matière, la question n'est à ce jour pas tranchée. À notre sens, l'accès à des données non sécurisées pourrait être illégal (accès « sans droit ») en vertu de l'article 370C du Code pénal grec, même en l'absence de mention expresse à destination des tiers par le propriétaire concernant la nature privée et l'accès restreint des données, à condition que le caractère privé des données en question puisse, au regard des circonstances, être raisonnablement présumé. Ainsi, si une personne physique ou morale ne prend aucune mesure, ou prend des mesures inadéquates, pour protéger des données « sensibles » ou ayant une valeur monétaire, n'ayant pas vocation à être publiées, cette défaillance ne devrait pas conduire à considérer automatiquement comme légal l'accès à ces données par un tiers, alors même que ledit tiers aurait dû, compte tenu de la teneur des données, raisonnablement supposer que ces données étaient exclusivement destinées à un usage privé et que le consentement de leur propriétaire est requis afin d'y accéder légalement. Certes, l'article 370C précise qu'une interdiction explicite du titulaire des données est nécessaire, mais seulement dans le cas où le contrevenant est salarié du titulaire des données. Par un raisonnement a contrario, il pourrait donc légitimement en être déduit que cette interdiction explicite n'est pas strictement nécessaire dans tous les autres cas.

REFERENCES

(1) Article 370C du Code pénal grec (Ποινικού Κώδικα) :
"2. Celui qui accède à des données stockées dans un ordinateur ou dans la mémoire périphérique d'un ordinateur, ou transmises par des systèmes de télécommunication, sans droit, notamment en violation des interdictions ou des mesures de sécurité prises par le propriétaire des données, est puni d'un peine d'emprisonnement pouvant aller jusqu'à trois mois ou d'une amende d'au moins 29 euros. En outre, si les données en cause relèvent des relations internationales ou de la sécurité de l'Etat, le coupable s'expose aux sanctions prévues par l'article 148 du Code pénal.
3. Si l'auteur de l'accès est un salarié du propriétaire des données, l'acte visé au paragraphe ci-dessus n'est répréhensible que s'il a été explicitement interdit par le règlement intérieur ou par une décision écrite de l'employeur ou de son représentant compétent. »
(cf. site de la police hellénique : Hellenic Policy, Ministry of public order and citizen protection)

(2) Cf. par example, les chiffres du World Bank and ITU's *Little Data Book on Information and Communication Technology 2014* (page 91) ou du *E-Communications And Telecom Single Market Household Survey* (Special Eurobarometer 414).

GEORGE A. BALLAS
&
THEODORE KONSTANTAKOPOULOS

▪ *According to* ***Article 370C (para 2) of Greek Penal Code (1)****, whoever accesses data stored (input) in a computer or in the peripheral memory of a computer or transmitted by telecommunication systems, provided that said acts have taken place without right, especially in violation of prohibitions or of security measures taken by the legal holder, shall be punished with imprisonment of up to three months or a fine not less than 29 Euro. If the act concerns the international relations or the security of the State, the offender shall be punished in accordance with Article 148 of Penal Code (on espionage, providing for imprisonment of at least one year and under specific circumstances of life imprisonment). If the offender is in the service of the legal holder of the data, the above mentioned act shall be punished only if it has been explicitly prohibited by internal regulations or by a written decision of the holder or a competent employee thereof.*

▪ *Article 370C was introduced in the Greek Penal Code back in the 1988, when the use of personal computers and networks was not as widespread as it is today* ***(2)****. In view of this fact and considering the rapid development of technology, the language used in Article 370C is broad, in an attempt to include future illegal instances and acts within scope.*

▪ ***Access "without right".*** *Noting that access to data must be illegal ("without right"), this short commentary will focus on the element of "security measures" as prerequisite for the application of Article 370C and it will also discuss the need for the expression of explicit prohibition by the legal holder.*

▪ *The law will in principle punish access which is "without right", meaning that the offender must access (a) data treated as private (i.e. technically protected by passwords, firewalls, encryption, etc.) or (b) data which are characterised as private, either by law (e.g. classified state information) or by its legal holder (e.g. via terms of use).*

▪ ***Security measures.*** *Regarding the need for security measures, in particular, a "literal" approach and the use of the term "especially" leaves no doubt that the circumvention of security measures is not a strict prerequisite for the application of Article 370C (the contrary is the case in other jurisdictions). Such reference is, therefore only for explanatory and penalty assessment purposes.*

▪ ***Explicit prohibition by the legal holder.*** *In the absence of helpful ad hoc case-law, it is debated whether, in cases when no security measures are in place and no other relevant regulation apply, the legal holder of the data should have explicitly declared to third parties that specific content is private and access is not allowed. In our view, it is possible that access to unsecured data could still be illegal ("without right") under Article 370C, even when the legal holder of the data has not positively declared his will that such data are private and not to be accessed by third parties, if the private nature of the data in question is under the circumstances reasonably assumed. For instance, the fact alone that an organisation or an individual has failed (or even missed) to secure "sensitive" data or information of monetary value not intended for publication, should not establish access to such data by a third party as legal, when said third party should, considering the content of the data, reasonably assume that such data are for private use only and consent by its legal holder is required for legal access. An argument* a contrario *in support of this view would be the fact that, according to Article 370C, an explicit prohibition (either by internal regulation or by a written decision) is specifically required in cases when the offender is in the service of the legal holder of the data. Therefore, it would be fair to assume that such explicit prohibition is not strictly required in all other instances.*

REFERENCES

(1) Article 370C of the Greek Penal Code (Ποινικού Κώδικα):
"2. Anyone who gets access to data, introduced to a computer or to a peripheral computer memory or transferred through telecommunication systems, on condition that this act has taken place with no right to do so and in particular, by contravening the restrictions or the security measures established by their legal owner, shall be punished with imprisonment of at least three months or with a fine of at least twenty nine euros. If this act relates to international relations or the security of a state, it shall be punished pursuant to article 148.
3. If the perpetrator is at the service of the legal holder of this data, the act mentioned in the previous paragraph shall be punished, only if it is expressly forbidden by internal rules or by a written decision of the holder or competent employee thereof."
(source: Hellenic Policy, Ministry of public order and citizen protection)

(2) (2) See e.g. World Bank and ITU's *Little Data Book on Information and Communication Technology 2014* (page 91) or *E-Communications And Telecom Single Market Household Survey* (Special Eurobarometer 414).

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

▪ La jurisprudence italienne s'est déjà penchée à plusieurs reprises sur la question de l'accès et du maintien frauduleux à un système informatique.

▪ Aux termes de l'article **615 ter du Code pénal italien (1)** : « Toute personne qui s'introduit frauduleusement dans un système informatique protégé par des mesures de sécurité, ou se maintient dans un tel système, contre la volonté, exprimée ou implicite, de la personne compétente pour en sécuriser l'accès, est puni d'une peine d'emprisonnement allant jusqu'à trois ans ».

▪ Ce texte appelle plusieurs remarques.

▪ Un premier constat immédiat : il n'y a accès frauduleux que si le système est protégé par des **mesures de sécurité**. En l'absence de telles mesures, l'infraction n'est pas caractérisée. En revanche, un défaut technique ayant pour effet de faciliter le contournement des mesures mises en place n'est pas considéré comme un défaut de mesures de sécurité. L'essentiel est qu'il soit prouvé que le propriétaire du système avait l'intention de mettre en place des procédures ou des dispositifs permettant de ne donner l'accès qu'à un nombre limité d'utilisateurs et que, ce faisant, il a exercé son *jus excludendi*, son droit d'exclure autrui de sa propriété.

▪ Deuxième question soulevée par le texte de l'article 615 ter : **quels sont exactement les actes réprimés ?** Le simple fait de s'introduire dans un système sans autorisation, le fait d'outrepasser ses autorisations d'accès ou encore la violation de procédures et codes de sécurité…? Si un utilisateur accède légitimement à un système mais effectue ensuite des opérations pour lesquelles il n'est pas habilité, ce comportement tombe-t-il sous le coup de l'article 615 ter ? Pendant longtemps, la position des tribunaux italiens a fluctué.

▪ Les hésitations de la jurisprudence sur ce point sont mises en évidence par différentes décisions de la Cour suprême italienne **(2)**. Certaines décisions y ont ainsi répondu par l'affirmative **(3)**, tandis que dans d'autres la haute juridiction a adopté un raisonnement plus restrictif en énonçant que seul l'accès non autorisé à un système était visé **(4)**. Par exemple, dans une affaire en matière de concurrence, n'a pas été considéré comme entrant dans le champ de l'article 615 ter le fait pour un revendeur, après avoir légitimement pénétré le système informatique de son partenaire, d'en donner accéder accès à un concurrent de ce dernier, lui permettant de fait de consulter des informations sensibles. Ce conflit de jurisprudence a finalement été tranché par l'assemblée plénière de la Corte Suprema di Cassazione en 2011 **(5)**. Il en ressort désormais le principe suivant : la loi interdit l'accès et l'utilisation du système informatique par une personne qui, bien que dûment autorisée à y accéder, enfreint les limites imposées à son profil d'habilitation, en réalisant des opérations qu'elle n'est pas autorisée à effectuer.

▪ Enfin, s'agissant de la **juridiction compétente** pour connaître des accès frauduleux, cette question controversée a également été récemment arbitrée par la cour suprême italienne **(6)**. Le tribunal de Rome et le tribunal de Florence étaient en désaccord sur leur compétence respective dans une affaire impliquant un accès non autorisé à un système informatique. En l'espèce, la personne à l'origine de l'accès frauduleux était établie à Florence, mais le serveur auquel elle avait frauduleusement accédé était, quant à lui, situé physiquement à Rome. Pour la Corte Suprema di Cassazione, l'infraction se matérialise à l'endroit où sont enfreintes les mesures de protection et de sécurité, puisque qu'il s'agit du lieu où l'accès s'effectue. Par conséquent, le tribunal compétent est le tribunal dans le ressort duquel le serveur est physiquement situé.

REFERENCES

(1) ""Accesso abusivo ad un sistema informatico e telematico: Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni".

(2) Corte Suprema di Cassazione, www.cortedicassazione.it

(3) Sez. V, n°12732 du 7-11-2000; Sez. V, n°37322 du 8-7-2008, et Sez. V, n°1727 du 30-9-2008

(4) Cf. Sez. V, n°2534 du 20-12-2007; Sez. V, n°26797 du 29-5-2008 et Sez. VI, n°3290 du 8-10- 2008

(5) SU, n°4694/12 du 27-10-2011

(6) Décision n°40303 du 20-5-2013 au 27-9-2013

RAFFAELE ZALLONE

REFERENCES

▪ *Italian Case law has addressed several times the issues of fraudulent access to an IT system.*

▪ ***Sec 615-ter of the Italian criminal code (1)*** *states the following: "Anyone who fraudulently introduces himself in an IT system protected by security measures, or remains in such system against the will, expressed or implied, of the subject who has the right to secure access, is punished with a term of imprisonment up to three years".*

▪ *The first thing to notice is that the crime is committed only if the system is protected by* ***security measures****; if no security measures are in place, then there is no violation. Of course, a technical default that makes it easy to overcome the access procedures is not regarded as a "lack of security measures". What is important is the evidence that the owner of the system wanted to use procedures and devices to grant access to a limited, authorized number of users and that by doing so he exercised the so called "jus excludendi".*

▪ *The main point that case law has debated has been the* ***definition and the extent of the forbidden conduct****. The question that cases have debated has been: what is the conduct forbidden and punished by the law? Is it the simple act of introducing oneself into a system without authorization, violating access procedures and codes, or once a legitimate user has accessed the system, is it also forbidden to perform a set of operations to which one is not authorized? In other words, assume a legitimate user access the system and then operates in a way to exceed its authorization, performing operations to which he/she is not authorized, is this also a conduct in violation of sec. 615-ter?*

▪ *Several decisions of the Italian Supreme Court* ***(2)*** *support this latter case* ***(3)****. Other opinions of the same Supreme Court have concluded in an opposite sense, i.e. that the only conduct forbidden by the law is the act of accessing a system without authorization* ***(4)****. In one of these cases, for instance, an authorized dealer had accessed the system of his proponent and then had allowed a competitor of the proponent to access information of sensitive, competitive nature. This conduct was not considered to be in violation of sec. 615-ter. This conflict in case law has been finally stopped by the decision of the United Sections of the Supreme Court laid down in 2011* ***(5)****. What is forbidden by the law is the access and the use of the system by someone who, albeit duly authorized to access, violates the limitations imposed to his profile of authorization, exceeding the boundaries of the operations to whom he/she was admitted to perform.*

▪ *Another key point is the* ***definition of the competent court****. This has been recently decided again by the Supreme Court* ***(6)****. The Tribunal of Rome and the Tribunal of Florence where in disagreement on who was the competent Tribunal in a case of unauthorized access to a computer system. The dispute arose because the person who had illegally accessed the system was in Florence, but the server fraudulently accessed was physically located in Rome. The Court has decided that the conduct takes place in the location where the security measures and protections are violated, since that's where the access procedures are active and that's where the access takes place; hence, the competent court is the court where the server is physically located.*

(1) "Accesso abusivo ad un sistema informatico e telematico: Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni".

(2) Corte Suprema di Cassazione, www.cortedicassazione.it

(3) Sez. V, No. 12732 of 7-11-2000; Sez. V, No. 37322 of 8-7-2008, and Sez. V, No. 1727 of 30-9-2008

(4) Cf. Sez. V, n°2534 du 20-12-2007; Sez. V, n°26797 du 29-5-2008 et Sez. VI, n°3290 du 8-10- 2008

(5) SU, No. 4694/12 of 27-10-2011

(6) Decision No. 40303 of 20-5-2013 to 27-9-2013

RAFFAELE ZALLONE

▪ L'accès frauduleux à un système informatique, communément appelé « **piratage** », est l'une des formes de criminalité informatique les plus connues. L'accès illégal à un système informatique a été érigé en infraction pénale par la Convention sur la cybercriminalité signée à Budapest en 2001 **(1)**, transposée en droit portugais par la loi 109/2009 sur la cybercriminalité du 15 septembre 2009 (« ***Lei do Cibercrime*** ») **(2)**. Aux termes de l'article 6 « *Acesso ilegítimo* » de cette loi « celui qui accède à un système informatique ou une partie de celui-ci de quelque manière que ce soit, sans autorisation légale ou sans autorisation de son propriétaire, est puni d'une peine de prison pouvant aller jusqu'à un an ou une amende pouvant aller jusqu'à 120 jours » **(3)**.

▪ A ce jour, les **juridictions portugaises** n'ont pas eu à se prononcer sur un cas similaire à celui de M. Olivier L., le blogueur français qui a récemment été condamné par la cour d'appel de Paris à une amende 3 000 € après avoir accédé illégalement à des données trouvées sur le site Web d'une agence de l'Etat à la suite d'une simple recherche Google. Toutefois, la jurisprudence portugaise comporte **plusieurs décisions en matière d'accès frauduleux** aux systèmes informatiques protégées, qui dessine les contours du sort qui aurait pu être réservé à l'affaire Bluetouff au Portugal.

▪ Ainsi, l'arrêt de la cour d'appel de Guimarães en date du 17 novembre 2008 **(4)** a qualifié l'accès frauduleux à des données de « délit abstrait de mise en danger » (c'est à dire que cet acte est automatiquement de nature criminelle, indépendamment de son résultat) **(5)**. Cette classification tient aux enjeux des intérêts protégés, à savoir l'intégrité et la sécurité des systèmes d'information (à cet égard, voir notamment les décisions de la cour d'appel de Coimbra du 15 octobre 2008 **(6)** et de la cour d'appel de Porto du 8 janvier 2014 **(7)**. En outre, l'infraction existe qu'elle soit ou non motivée par l'obtention d'un gain pécuniaire (même si une peine plus sévère de un à cinq ans de prison s'applique si l'accès est réalisé dans le but d'en retirer un bénéfice « d'une valeur considérable »). Un arrêt de la cour de Lisbonne du 19 juin 1997 **(8)** a, quant à lui, estimé que l'accès à une base de données en ligne est frauduleux s'il intervient sans autorisation. Les magistrats de la cour d'appel de Guimarães ont eu l'occasion de préciser le 26 juin 2007 **(9)** que l'infraction est constituée quand bien même le pirate informatique n'était animé que par le simple plaisir, le frisson ou la fierté pouvant être retiré de l'acte d'intrusion.

▪ Ceci étant, les dispositions de l'**article 16 du Code pénal portugais (10)** précisent qu'en cas d'**erreur de fait**, c'est-à-dire lorsqu'une personne n'a pas conscience qu'elle est en train de commettre une infraction et agit donc sans intention dolosive, la responsabilité pénale est exclue, pour autant que l'erreur soit considérée raisonnable.

▪ Partant, quelle aurait donc pu être l'issue de l'affaire Bluetouff si les tribunaux portugais avaient eu à en connaitre ? A la lumière des critères pris en compte par la jurisprudence portugaise, les actes de Bluetouff pourraient être qualifiés d'accès frauduleux à un système informatique tant au regard de l'intérêt légal en jeu (à savoir l'intégrité du système d'information) que du fait qu'aucune intention de retirer un avantage pécuniaire n'est nécessaire. En effet, l'intention criminelle est présumée exister dès lors qu'une personne accède à un système sans autorisation, comme ce fut le cas pour Bluetouff. Toutefois, Bluetouff pourrait renverser cette présomption en apportant la preuve qu'il ne savait pas, et n'aurait pas raisonnablement pu savoir (notamment au regard du fait que le site était affecté par un bug de sécurité qui a rendu sa base de données facilement accessible via Google), qu'il accédait à un système informatique protégé. Dans ce cas, il ne serait pas tenu responsable pénalement en vertu de l'article 6 de la loi portugaise sur la cybercriminalité.

REFERENCES

(1) Convention sur la cybercriminalité (en portugais et en français)

(2) « Lei do Cibercrime » (en portugais et en anglais)

(3) « Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias »

(4) Acórdão do Tribunal da Relação de Guimarães, Secção Criminal, 17-11-2008

(5) « crime de perigo abstracto »

(6) Acórdão do Tribunal da Relação de Coimbra, 15/10/2008, disponible en ligne sur : http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/ae4145b5e5a62059802574f70058c7fe?OpenDocument

(7) Acórdão do Tribunal da Relação do Porto, 08/01/2014 disponible en ligne sur : http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b54faf2d4330b8d480257c6e004ff2df?OpenDocument

(8) Tribunal Judicial da Comarca de Lisboa, Sentença de 19-6-1997

(9) Acórdão do Tribunal Judicial da Comarca de Guimarães, 26-6-2007

(10) Código Penal Português, "Erro sobre as circunstâncias do facto" (versión anglaise non officielle : http://www.verbojuridico.com/download/portuguesepenalcode.pdf)

JOÃO P. ALVES PEREIRA
&
SOFIA LIMA

▪ *Fraudulent access to an IT system, commonly known as "**hacking**", is one of the most well-known cyber crimes. It is regulated by the Convention on Cybercrime signed in Budapest in 2001 **(1)**, which was adopted by Portuguese Law under Law 109/2009, of 15 September ("**Lei do Cibercrime**") **(2)**. According to its section 6 ("Fraudulent Access"): "whoever accesses an IT system or part of it in any way without legal permission or authorisation from its owner shall be punished with a penalty of prison of up to one year or fine of up to 120 days" **(3)**.*

▪ *So far the Portuguese courts have not had to deal with a case as peculiar as the one involving Mr. Olivier L., the French blogger who was recently sentenced by the Paris Appellate Court to pay a €3,000 fine for illegally accessing data that he found on a government website with a simple Google search. However, **Portuguese case law** includes **several judicial decisions on fraudulent access to protected IT systems**, which give us an indication on how the case of Olivier L. would have been handled in Portugal.*

▪ *For instance, the ruling of the Guimarães Appellate Court of 17th November 2008 **(4)** has classified fraudulent access to data as an "abstract crime of danger" (i.e. it has criminal relevance regardless of any unlawful result) **(5)**. Such a classification derives from what case law considers to be the legal interest at the core of fraudulent access: the integrity and security of IT systems (also, inter alia, the rulings of the Coimbra Appellate Court of 15th October 2008 **(6)** and the Oporto Appellate Court of 8th January 2014 **(7)**). Furthermore, fraudulent access does not need to be motivated by an intention to obtain any pecuniary gain in order to be punishable as a crime (although a harsher sentence of one to five years of prison will be applicable if the access results in a benefit of "considerably high value"). The ruling of the Lisbon Court of 19th June 1997 **(9)** considered that there is a fraudulent access as long as someone accesses an online database without the authorisation to do so. Also, according to the ruling of the Guimarães Court of 26th June 2007 **(10)**, for prosecution purposes it is considered enough that a person has breached an IT system for the simple pleasure of intrusion, the thrill of the challenge or the pride in the act itself.*

▪ *However, one cannot ignore the provision of **Sec. 16 of the Portuguese Criminal** Code on **error facti (11)**, which sets forth that an agent who acts without the knowledge that his actions constitute a crime is actually acting without criminal intent as long as his misinterpretation is considered reasonable and, as such, he cannot be prosecuted. In a similar case to the one of Bluetouff, one would have to ponder if (i) the agent was unaware of the unlawfulness of his actions and (ii) this lack of knowledge was reasonable, considering that the website had a security bug that made the database easily accessible via Google.*

▪ ***In conclusion**, according to Portuguese case law Bluetouff's actions would be enough to fulfil the criminal type of fraudulent access to an IT system considering the legal interest at stake at the core of this crime (i.e. the integrity of the IT system). No intention to obtain a pecuniary gain is required for a person to be prosecuted for fraudulent access. In fact, criminal intent is considered to be verified if the person merely accesses the system without due authorisation, as Bluetouff did. However, if proven that Bluetouff did not know, and should not have reasonably known, that he was accessing a protected IT system, he would not be criminally liable under section 6 of the Cyber Crime Act.*

REFERENCES

(1) Cybercrime Convention: (in Portuguese and in English)

(2) "Lei do Cibercrime" (in Portuguese and in English)

(3) "*Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias*"

(4) Acórdão do Tribunal da Relação de Guimarães, Secção Criminal, 17-11-2008

(5) "crime de perigo abstracto"

(6) Acórdão do Tribunal da Relação de Coimbra, 15/10/2008, available online: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/ae4145b5e5a62059802574f70058c7fe?OpenDocument

(7) Acórdão do Tribunal da Relação do Porto, 08/01/2014, available online: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b54faf2d4330b8d480257c6e004ff2df?OpenDocument

(8) Tribunal Judicial da Comarca de Lisboa, Sentença de 19-6-1997

(9) Acórdão do Tribunal Judicial da Comarca de Guimarães, 26-6-2007

(10) Código Penal Português, "Erro sobre as circunstâncias do facto" (unofficial English versión: (http://www.verbojuridico.com/download/portuguesepenalcode.pdf)

JOÃO P. ALVES PEREIRA
&
SOFIA LIMA

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*	Schulte Riesenkampff	Tim Caesar	+49 (69) 900 26 876	tim.caesar@schulte-lawyers.com
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@lkd.ca
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
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
Portugal *Portugal*	Alves Pereira & Teixeira de Sousa	João P. Alves Pereira	+ 351 21 370 01 90	jpereira@alvespereira.com
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 –
ISSN 1634-0701
Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-juristendance/