Réseau international d'avocats en droit du numérique et des technologies avancées
International lawyers' network for digital and emerging law

Le réseau Lexing vous informe - The Lexing® network informs you

JTIT Internationale n°15 –juin 2017
JTIT Special international issue #15– June 2017

LA CYBERSÉCURITÉ

CYBERSECURITY

▪ Enjeu stratégique majeur pour les entreprises, la cybersécurité est un élément clé de succès et de pérennité. Les récentes attaques informatiques d'ampleur mondiale ont démontré la nécessité de mettre en place des mesures permettant de protéger les acteurs tant sur le plan technique que sur le plan juridique.

▪ Cette édition propose un panorama, à l'échelle internationale, de l'état des législations en matière de cybersécurité.

▪ Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Allemagne, Belgique, Costa Rica, France, Grèce, Portugal et Russie.

A propos de Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et 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.

▪ *A major strategic issue for businesses, cybersecurity is a key element of success and sustainability. Amid the cyberattacks that recently hit computers around the world, there is a growing need to take measures for protection, both technically and legally.*

▪ *This issue provides an overview of cybersecurity laws around the globe.*

▪ *The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: Germany, Belgium, Costa Rica, France, Greece, Portugal and Russia.*

About Lexing®

Lexing® is the first international lawyers' network for digital and emerging 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

Cyberattaques : quels risques pour les entreprises ?

▪ De plus en plus d'entreprises exploitent les nouvelles possibilités offertes par le Big Data, l'Industrie 4.0 et l'internet des objets. Si les entreprises qui ont adopté la dématérialisation de leurs processus métier sont très souvent plus compétitives, elles sont également plus vulnérables aux cyberattaques. Loin d'être anecdotiques, ces attaques informatiques se généralisent : deux tiers des entreprises industrielles en Allemagne déclarent avoir déjà été victimes de vol de données, d'espionnage industriel ou de sabotage ces deux dernières années **(1)**. Sont principalement visés les systèmes informatiques et l'infrastructure de communication. Des pirates ont ainsi utilisé la méthode d'hameçonnage ciblé (« spearphishing ») **(2)** pour accéder au réseau informatique d'une aciérie **(3)**, s'introduire dans le réseau de production et actionner le haut fourneau, et les salariés n'ont pu réussir à stopper cette intrusion sans endommager les machines de leur société **(4)**.

Dommages potentiels d'une cyberattaque

▪ Les dommages occasionnés par les cyberattaques sont multiples et peuvent même aller jusqu'à menacer l'existence même de l'entreprise. Tout d'abord, comme dans l'exemple de l'aciérie donné plus haut, les installations de l'entreprise peuvent être endommagées par les pirates, et nécessiter des réparations, voire un remplacement. En cas d'attaque par un rançongiciel (« ransomware »), l'entreprise pourrait aussi se voir contrainte de payer la rançon exigée afin d'être en mesure de poursuivre ses activités et de préserver ses informations sensibles. En outre, les investissements financiers requis après une cyberattaque sont conséquents, car les mesures à prendre sont nombreuses : le recrutement d'experts informatiques externes afin d'évaluer l'étendue de l'attaque et d'éradiquer complètement les virus des systèmes infectés, la location de serveurs externes pour un environnement de sauvegarde vers lesquels rediriger les systèmes informatiques actuels afin de traiter les commandes en attente et réduire la perte de chiffre d'affaires, l'organisation de campagnes de marketing pour limiter l'atteinte à la réputation et conserver la confiance des clients... Sans oublier, bien entendu, les amendes administratives dont l'entreprise pourrait écoper en cas de manquement à ses obligations légales.

Cadre juridique

▪ L'entreprise victime d'une cyberattaque peut avoir à respecter toute une série d'obligations légales, en fonction de l'ampleur de l'attaque. En effet, lorsque des données à caractère personnel sensibles **(5)** ou des données financières ont été volées, l'entreprise est tenue d'en notifier non seulement l'autorité compétente, mais également les personnes concernées **(6),** faute de quoi, elle encoure une amende pouvant s'élever jusqu'à 300 000 €, à laquelle peut s'ajouter l'amende infligée en cas de violation de données à caractère personnel **(7)**. D'autant plus qu'avec le règlement européen sur la protection des données (dit « RGPD »), applicable directement en Allemagne à compter du 25 mai 2018, cette obligation de notification **(8),** et l'amende associée en cas de manquement, seront davantage renforcées (jusqu'à 10 000 000 € ou 2% du chiffre d'affaires annuel) **(9)**.

▪ Par ailleurs les opérateurs de site Web, les personnes considérées comme des fournisseurs de services au sens de la loi fédérale sur les télémedias **(10)**, les entreprises de télécommunication et les opérateurs d'infrastructures critiques sont astreints aux obligations énoncées par la loi allemande sur la sécurité informatique (« IT-Sicherheitsgesetz », dite « IT-SiG »). Les opérateurs d'infrastructures critiques **(11)** sont invités à prendre en compte « l'état de la technique » pour assurer la

REFERENCES

(1) Selon une étude représentative réalisée par Bitkom, disponible à l'adresse suivante : https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html

(2) Il s'agit d'une technique d'ingénierie sociale où l'attaquant contacte un employé de l'entreprise ciblée par courrier électronique. L'attaquant se fait passer pour un membre de l'entreprise, souvent cadre dirigeant, et demande la communication des identifiants de connexion, ou bien joint à un courrier un document infecté, de sorte que lorsque le salarié ouvre cette pièce jointe, le pirate peut accéder au réseau de l'entreprise.

(3) Les circonstances exactes de cette attaque et des méthodes utilisées n'ont pas été publiquement révélées.

(4) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.html.

(5) Ce sont par exemple les données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données concernant la santé ou la vie sexuelle ou l'orientation sexuelle d'une personne.

(6) Sec. 42a de la loi sur la protection des données personnelles, la « BDSG ».

(7) Sec. 43 (2) Nr. 7, (3) BDSG

(8) Art. 33 et 34 RGDP

(9) Art. 83 (4)(a) RGDP

(10) La loi sur la sécurité informatique ne s'applique ni

sécurité de leurs installations, et tenus de faire vérifier leurs systèmes de sécurité informatique au moins tous les deux ans soit par des salariés de la société qui possèdent une qualification spécifique reconnue par l'agence fédérale pour la sécurité des systèmes d'information (Bundesamt für Sicherheit in der Informationstechnik, ou « BSI »), soit par des auditeurs externes certifiés **(12)**. En l'absence de définition de l'expression « état de la technique » par l'IT-SiG, le BSI a précisé que cette notion devait être interprétée à la lumière des normes nationales ou internationales élaborées par les organismes de normalisation, le DIN ou l'ISO. Tout manquement aux dispositions de l'IT-SiG est puni par une amende à hauteur de 100 000 € **(13)**. La cybersécurité est également encadrée par la directive européenne sur la sécurité des réseaux et des systèmes d'information (« directive NIS ») adoptée en 2016 par le Parlement européen **(14)**, et qui doit être transposée en Allemagne d'ici 2018. A cet égard, les dispositions de l'IT-SiG diffèrent quelque peu de celles de la directive NIS, et le législateur allemand devra être amené à ajuster le texte national en conséquence. Les entreprises soumises aux dispositions de l'IT-SiG sont encouragées à suivre les évolutions législatives en la matière pour garantir leur conformité et éviter de mettre en jeu leur responsabilité.

▪ Les dirigeants ont donc tout intérêt à s'assurer que leur entreprise soit bien protégée contre les cyberattaques. En Allemagne, les membres du conseil d'administration d'une société anonyme sont personnellement responsables en cas de manquement à l'obligation de prendre les mesures préventives nécessaires à la détection des risques potentiels et d'appliquer les mesures de sécurité appropriées à la réduction des conséquences dommageables pour l'entreprise **(15)**. De même, le gérant d'une société à responsabilité limitée se doit de faire preuve, dans la conduite des affaires de sa société, de « la diligence d'un commerçant avisé » **(16)**. A défaut, ils pourraient avoir à réparer les dommages financiers subis par l'entreprise, pouvant se chiffrer en millions d'euros **(17)**.

Préconisations pour réduire le risque de responsabilité en cas de cyberattaques

▪ Avant toute chose, l'efficacité des mesures prises passe par la sensibilisation aux risques et enjeux de la cybersécurité de l'ensemble des membres de l'entreprise, de la direction aux salariés. Grâce à l'organisation de formations et la diffusion de guides pratiques, ils seront en mesure d'identifier les méthodes d'ingénierie sociale et autres techniques utilisées par les cybercriminels pour accéder au réseau de l'entreprise. Le BSI a élaboré des lignes directrices sur la sécurité informatique qui présentent un ensemble de mesures informatiques, organisationnelles et techniques en matière de sécurité **(18)**. Il est vivement recommandé de mettre en œuvre ces mesures, et surtout de les actualiser régulièrement, les cybermenaces évoluant sans cesse. La désignation d'un délégué à la protection des données est, également, un moyen pour l'entreprise de faciliter le respect de ses obligations légales, en vertu des textes actuels ou futurs, et ainsi d'éviter de s'exposer inutilement à des sanctions pécuniaires pour non-conformité. Cela étant, quand bien même tous les garde-fous seraient en en place, une cyberattaque est toujours susceptible de se produire et d'entraîner un ou plusieurs dommages. C'est pourquoi la souscription d'une cyberassurance peut aider à couvrir une partie des dommages causés par une cyberattaque, et notamment les pertes de revenus découlant d'une interruption d'activité en raison de l'arrêt du système informatique, ou le recrutement d'experts informatiques et juridiques.

aux opérateurs non commerciaux ni aux particuliers.

(11) La qualification d'opérateur d'infrastructures critiques est définie par réglementation « BSI-KRITIS » pour les secteurs de l'énergie, de l'eau, de l'alimentation, de l'informatique et des télécommunications.

(12) Sec. 8a (3) de la loi sur l'agence fédérale pour la sécurité des systèmes d'information (« BSIG ») ; cf. également le "guide d'orientation" du BSI.

(13) Sec. 14 (2) BSIG

(14) Directive (UE) 2016/1148

(15) Sec. 91 II, 93 de la loi sur les sociétés anonymes (AktG)

(16) Sec. 43 de la loi sur les sociétés à responsabilité limitée (GmbHG)

(17) Cf. Jugement du LG München I, 10.12.2013 – 5 HKO 1387/10

(18) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/IT-sec-guidelines_pdf.pdf?__blob=publicationFile

SUSANNE KLEIN
&
FLORIAN GROOTHUIS

Liability Risks for Companies due to Cyber Attacks

▪ *The amount of companies that are relying on new technological achievements based on Big Data, Industry 4.0 or the Internet of Things increase continuously. Companies which digitalize their business processes are very often not only more competitive on the market nowadays, but also more vulnerable for cyber attacks. Those attacks are not a random phenomenon anymore: already two thirds of industrial companies in Germany have been a victim of data theft, corporate espionage or sabotage within a two years period* ***(1)****. The prior targets have been the company´s IT system and communication infrastructure. In one case, the attackers used the spear-phishing method* ***(2)*** *to gain access to the office network of a German steel mill company* ***(3)****. Through this, they entered the production network and manipulated the blast furnace, so the employees were not able to shut it down before the company´s facilities got damaged* ***(4)****.*

Potential damages caused by a cyber attack

▪ *Those cyber attacks can cause various damages and might even threaten the company´s existence. The above described steel mill case has shown that sometimes damaged facilities need to be repaired or even replaced due to manipulations. In other cases, where sensitive information got decrypted by ransomware the company might be forced to pay the ransom demand to continue its business. Financially even more substantial are often the accompanying efforts after a cyber attack has been noticed. Usually it will be necessary to hire external IT experts to figure out the scope of the infected computer systems and to remove any virus completely. Furthermore, external servers must be rented for redirecting the current IT systems to a save environment, so that pending orders can be processed and the revenue loss minimized. In addition to this, marketing campaigns might be necessary to limit reputation damages and gain back the trust from customers. Beyond that, a company might also face administrative fines when it does or did not comply with legal requirements.*

Legal framework

▪ *When a company has been the victim of a cyber attack, different legal obligations must be considered depending on the consequences of the attack. When sensitive* ***(5)*** *or financial personal data has been stolen, the company is obligated to notify the competent authority and affected data subject about such incident* ***(6)****. The violation of the notification obligation can be fined with up to 300.000€ which may be imposed by the authority in addition to a potential fine resulting from an actual data breach before* ***(7)****. With the direct applicability of the General Data Protection Regulation ("GDPR") as of May 25th, 2018 the data breach notification obligation will be even more comprehensive* ***(8)*** *and an infringement can be fined with up to 10.000.000€ or 2% of the company´s annual turnover* ***(9)****.*

▪ *Companies acting commercially as website operator or others considered as service providers according to the Federal Telemedia Act* ***(10)****, telecommunication companies and critical infrastructure operators have to consider the requirements of the German IT Security Act ("IT-SiG"). Critical infrastructure operators* ***(11)*** *are obligated to provide an adequate state-of-the-*

(1) According to a representative study made by Bitkom available under: https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html

(2) A social engineering technique where the attacker approaches an employee of the targeted company via email. The attacker disguises himself as an individual within the recipient´s company, often as superior, and asks for login details or attaches an infected document. When the employee opens the attachment, the attacker can gain access to the company´s network.

(3) The exact circumstances of how the attackers used spear-phising in this case are not publicly known.

(4) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.html.

(5) E.g. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health, a natural person's sex life or sexual orientation

(6) Sec. 42a BDSG.

(7) Sec. 43 (2) Nr. 7, (3) BDSG

(8) Art. 33, 34 GDPR

(9) Art. 83 (4) a GDPR

(10) Since the IT-SiG is not applicable to non-commercial operators and private persons, they do not have to comply with its requirements

(11) Whether an operator has to be categorized as critical

art security for their IT and their IT security systems must be checked at least every two years by employees of the company that possess a special qualification accepted by the Federal Office for Information Security ("BSI") or external certified auditors ***(12)****. Whereas the IT-SiG does not define what to understand under "state-of-the art", the BSI specified that the state of the art should be interpreted according to national or international DIN or ISO standards. Violating the requirements of the IT-SiG can be fined with up to 100.000€* ***(13)****. The field of cybersecurity is also regulated by the EU-directive on security of network and information systems ("NIS-Directive") which has been adopted in 2016 by the EU-Parliament* ***(14)****. Since the IT-SiG partly differs from the NIS-Directive and the latter has to be transposed into national law until 2018, the German legislator is forced now to adjust the national IT-SiG accordingly. Thus, companies falling under the scope of the IT-SiG must keep track of legal changes to avoid liability risks.*

▪ *It should be in the interest of board members and CEO´s that their company has safeguards against cyber attacks in place. Board members of a German Stock Corporation are personally liable if they do not monitor developments that might cause damages to the company in the future and implement safety measures accordingly* ***(15)****. Even CEO´s of a private limited company must exercise the "circumspection of a responsible businessman"* ***(16)****. If board members or CEO´s do not implement appropriate preventive safeguards and the company, therefore, suffers from financial damages, they might be faced with compensation claims in the amount of millions of Euros* ***(17)****.*

Exemplary measures to minimize the liability risk from cyber attacks

▪ *First of all, efficient protection measures against cyber attacks require the sensitization of management and employees for cyber-security issues. Seminars and guidelines can help to identify social engineering methods and other techniques attackers use with pleasure to gain access to the company´s network for causing further damage. The BSI published IT security guidelines that provide an overview about organisational, infrastructural and technical IT security safeguards* ***(18)****. Those guidelines must be implemented and renewed regularly since cyber-security standards develop continuously. The appointment of a data protection and a compliance officer will help to comply with current and future legal requirements to avoid unnecessary fines. Even though, if all safety guards are in place, a cyber attack can occur and cause damages like those mentioned above. Therefore, concluding a cyber insurance can help to cover a part of the damages caused by a cyber attack, like revenue losses due to business interruptions when the IT system shuts down or hiring external IT and legal experts.*

infrastructure has been specified by the "BSI-KRITIS"-regulation for the energy, water, food, IT and telecommunications sector

(12) Sec. 8a (3) Act of the Federal Office of Information Security ("BSIG"), see also the "orientation guide" of BSI.

(13) Sec. 14 (2) BSIG

(14) Directive (EU) 2016/1148

(15) Sec. 91 II, 93 AktG

(16) Sec. 43 GmbHG

(17) See LG München I, Urteil v. 10.12.2013 – 5 HKO 1387/10

(18) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/IT-sec-guidelines_pdf.pdf?__blob=publicationFile

SUSANNE KLEIN
&
FLORIAN GROOTHUIS

Cyber sécurité en Belgique : l'impact de la Directive NIS

http://www.ccb.belgium.be/

▪ La Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive NIS) vise à protéger les réseaux et systèmes d'information contre les « risques » (toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif **potentiel**) et les « incidents » (tout événement ayant un impact négatif **réel**). La Directive s'applique à deux catégories d'entités, les opérateurs de services essentiels (actifs dans l'énergie, le transport… et repris dans un cadastre à établir par les États Membres) et les fournisseurs de service numérique (entreprises fournissant des services de type place de marché en ligne, moteurs de recherche, services clouds… à l'exclusion des micro et petites entreprises).

▪ Les opérateurs de service essentiels doivent prendre des mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques et prévenir les incidents. En cas d'incident ayant impact significatif sur la continuité des services essentiels qu'ils fournissent, l'opérateur est tenu de notifier celui-ci à l'autorité nationale compétente mise en place conformément à d'autres dispositions de la Directive.

▪ Les fournisseurs de service numérique, quant à eux, doivent identifier les risques et éviter les incidents, en prenant les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer et réduire au minimum leur impact. Tout incident ayant un impact significatif sur la fourniture d'un service devra également être notifié.

▪ La Directive NIS n'est pas encore transposée en droit belge. Elle doit l'être avant mai 2018. Il ne semble pas y avoir de projet de loi déposée à ce sujet à l'heure de la rédaction de la présente.

▪ Toutefois, un Arrêté royal du 10 octobre 2014 a mis en place le Centre pour la Cyber sécurité Belgique (CCB). Celui-ci est chargé de la réflexion sur la transposition de la Directive même si rien n'est encore public. Le CCB devrait servir à la fois d'autorité nationale compétente et de CSIRT (Centres de réponse aux incidents de sécurité informatique). Cette compétence – exercée en Belgique par le CERT - a d'ailleurs déjà été reprise à BELNET pour être confiée au CCB.

ALEXANDRE CASSART

Cyber security in Belgium: the impact of the NIS Directive

http://www.ccb.belgium.be/

▪ *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Directive NIS) aims to protect networks and information systems against "risks" (any reasonably identifiable circumstance or event having a potential adverse effect) and "incidents" (any event having an actual adverse effect). The Directive applies to two categories of entities, operators of essential services (energy, transport... and included in a ledger to be established by Member States) and digital service providers (service providing online marketplace, search engines, cloud services... excluding micro and small businesses).*

▪ *Operator of essential services must take necessary and proportionate technical and organizational measures to manage risks and prevent incidents. In the event of an incident having a significant impact on the continuity of the essential services they provide, the operator is required to notify it to the competent national authority set up in accordance with other provisions of the Directive.*

▪ *Digital service providers, in turn, need to identify risks and avoid incidents by taking appropriate and proportionate technical and organizational measures, in order to manage risk and minimize the impact of incident. Any incident that has a significant impact on the provision of a service should also be notified.*

▪ *The NIS Directive has not yet been transposed into Belgian law. It has to be before May 2018.*

▪ *There does not seem to be any legislation on this subject at the time of writing. However, a Royal Decree of 10 October 2014 established the Center for Cyber Security Belgium (CCB). The latter is responsible for reflection on the transposition of the Directive even if nothing is yet public. The CCB should serve as both a competent national authority and as a CSIRT (Computer Security Incident Response Centers). This competence - exercised in Belgium by CERT - has already been removed from BELNET and transferred to the CCB.*

ALEXANDRE CASSART

▪ **Enjeux et défis.** De nos jours, la sophistication des cyberattaques et l'interdépendance accrue des technologies de l'information font de la cybersécurité une préoccupation majeure. La cybersécurité est l'affaire de tous les utilisateurs du Web, du simple particulier aux multinationales, en passant par les administrations et les entreprises publiques.

▪ **Politique et stratégie.** C'est dans ce contexte que le gouvernement du Costa Rica a mis au point une stratégie numérique nationale. Le pays est en effet doté d'un certain nombre d'organismes chargés des questions relatives à la cybersécurité :

- le gouvernement numérique ;
- le ministère des sciences, de la technologie et des télécommunications (MICITT) ;
- la section de la lutte contre criminalité informatique (pouvoir judiciaire) ;
- l'agence de protection des données (PROHAB) ;
- la Banque centrale du Costa Rica (BCCR) ;
- l'Autorité de régulation des télécommunications (SUTEL) ;
- la Direction des signatures numériques.

▪ Le Costa Rica dispose également d'une équipe de réaction aux incidents en matière de sécurité informatique au niveau national national, la CSIRT-CR (Centro de Respuestas de Incidences de Seguridad Informática,) créée par le MICITT. S'agissant de la cybersécurité, la CSIRT-CR a pour mission d'identifier les menaces, de réduire les risques, d'améliorer la coopération et le partage d'informations, et d'assurer la coordination entre les organismes de l'Etat et les institutions autonomes, les entreprises et les établissements bancaires.

▪ En septembre 2016, l'association des professionnels de l'informatique (Colegio de Profesionales en Informática y Computación / CPIC) a formé une commission sur la cybersécurité chargée d'élaborer des politiques de prévention des menaces cybernétiques et de protection des données, le capital informationnel étant un actif stratégique.

▪ Ces mesures nationales s'accompagnent d'actions au niveau international, l'Organisation des États américains (OEA) apportant son soutien à l'élaboration d'une stratégie nationale de cybersécurité au Costa Rica.

▪ **Éducation, formation et compétences.** Dans le but de faciliter l'échange et la diffusion de connaissances en matière de cybersécurité au-delà de ses frontières et de favoriser la coopération internationale, le Costa Rica participe à divers programmes de formation développés par l'OEA. Les membres de la section de la lutte contre criminalité informatique ont par exemple bénéficié de formations aux États-Unis et au Canada.

▪ Par ailleurs, en septembre 2016, vingt-cinq professionnels costaricains de l'informatique et des technologies de l'information ont pu se spécialiser en cybersécurité en suivant une formation dispensée par l'université costaricaine Georgia Tech. Intitulé « Comprendre et relever les défis de la cybersécurité : concepts fondamentaux et techniques pratiques », et composé de deux modules, ce cours a dans un premier temps permis aux participants de maîtriser les fondamentaux de la cybersécurité, de la sécurité des logiciels, des systèmes d'exploitation et de la base informatique de confiance (TCB), ainsi que des

méthodes d'authentification et d'autorisation puis, dans un second temps, d'approfondir certains thèmes axés sur la cryptographie, la sécurité des réseaux, la sécurité sur le Web et la sécurité des dispositifs mobiles, et enfin de se familiariser avec les futures grandes tendances de la cybersécurité.

▪ De nombreux autres organismes proposent un riche éventail de formations autour de la cybersécurité et de la cybercriminalité au Costa Rica, telles que notamment la spécialisation en cybersécurité du Centre pour la formation des TIC (CENFOTEC) et la spécialisation en sécurité de l'information de l'Université latino-américaine des sciences et des technologies (ULACIT).

▪ **Cadre juridique et réglementaire.** Plusieurs textes législatifs encadrent la cybersécurité au Costa Rica :

- la loi sur la cybercriminalité ;
- la loi sur la protection des données à caractère personnel ;
- la loi sur les certificats, les signatures numériques et les documents électroniques ;
- la loi sur les perquisitions, la saisie et l'examen de documents privés et l'interception des communications ;
- la loi sur la protection des enfants et des jeunes contre les contenus nuisibles sur internet et autres médias électroniques.

▪ Sont notamment punis par ces textes le piratage de logiciels, le piratage informatique, la distribution de logiciels malveillants, l'hameçonnage (en anglais, « phishing »), les violations de données, ou encore les chevaux de Troie bancaires.

GABRIEL LIZAMA
&
MELISSA RAMIREZ

▪ ***Main Challenges.*** *Currently, sophistication of cyber-attacks and increased interdependence on information technology have converted Cybersecurity in one of the most important concerns for enterprises, government organizations and for anyone on the web.*

▪ ***Policy and Strategy.*** *A National Digital Strategy has been adopted by the government. Costa Rica has a number of different organizations responsible for Cybersecurity:*

- *Digital Government;*
- *Ministry of Science and Technology (MICITT);*
- *Computer Crime Section, Judiciary;*
- *Data Protection Agency (PROHAB);*
- *Central Bank of Costa Rica (BCCR);*
- *Superintendency of Telecomunications (SUTEL);*
- *Digital Signature Directory.*

▪ *Costa Rica, also has an officially recognized national CIRT known as CSIRT-CR (Centro de Respuestas de Incidencias de Seguridad Informática) established under the Ministry of Science, Technology and Telecommunications. CSIRT-CR is mandated to coordinate among entities of the State and autonomous institutions but also companies and banks to identify threats, minimize risks, and improve cooperation and information-sharing on relevant cybersecurity-related matters.*

▪ *Last September (2016), the Computer Science Professionals College (CPIC) appointed the Cybersecurity Commission to dictate policies in order to prevent cyber threats and protect data, the most valuable capital currently.*

▪ *Additionally, in the international cooperation frame, the Organization of American States (OAS) supports the development of a National Cybersecurity strategy in Costa Rica.*

▪ ***Education, training & skills.*** *To facilitate sharing of cybersecurity assets across borders or with other states Costa Rica has participated in various training programs by the OAS. Personnel of the computer crime section have received training in the United States and Canada.*

▪ *On September 2016, twenty five Costa Ricans with an academic background in computer science, related disciplines or with professional experience in the development and management of information technology systems received a training "Understanding and addressing Cybersecurity Challenges: Fundamental concepts and practical techniques" from Georgia Tech University. The course was divided on two modules, the first focusing on basic elements of Cybersecurity, software security, operating systems and the trusted computing base and authentication and authorization methods. The second module comprises topics such as cryptography basics, network security, web and mobile security, and the future of Cybersecurity.*

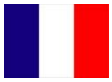
▪ *Additionally, the Centre for the Formation of ICTs (CENFOTEC) offers a specialization in cybersecurity; and the Latin American Science and Technology University (ULACIT) offers a specialization in information Security. Other institutions in Costa Rica offer cybersecurity and cybercrime relevant courses.*

▪ ***Legal & regulatory framework.*** *Specific legislation and regulation related to Cybersecurity has been enacted through the following instruments:*

- *Cybercrime Law;*
- *Data Protection Law;*
- *Law on the Certificates, Digital Signatures and Electronic Documents;*
- *Law on Registration, Seizure and Examination of Private Documents and Intervention in Communications;*
- *Law on Protection of Children and Young from harmful content on the internet and other electronic media.*

▪ *The legislation criminalizes software piracy, hacking, malware distribution, phishing, data breaches, banking trojans, among other online wrongdoings.*

GABRIEL LIZAMA
&
MELISSA RAMIREZ



REFERENCES

▪ **Enjeux.** Devant l'augmentation des incidents de cybersécurité, qu'ils soient causés par des « erreurs humaines, des catastrophes naturelles, des défaillances techniques ou des actes de malveillance » et les enjeux économiques et stratégiques de tels incidents, la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union du 6 juillet 2016 (dite « SRI ») **(1)** vise à « assurer un niveau commun élevé de sécurité des réseaux et de l'information dans l'Union ». Afin d'atteindre cet objectif :

- « elle fixe des obligations à tous les États membres en ce qui concerne la prévention et la gestion de risques et incidents touchant les réseaux et systèmes informatiques ainsi que les interventions en cas d'événement de ce type » ;
- « elle crée un mécanisme de coopération entre les États membres, destiné à garantir une application uniforme de la présente directive dans l'Union et, le cas échéant, un traitement et une intervention coordonnés et efficaces en cas de risques et d'incidents touchant les réseaux et systèmes informatiques » ;
- « elle établit des exigences en matière de sécurité pour les acteurs du marché et les administrations publiques ».

▪ Chaque Etat-membre devra adopter une stratégie nationale en matière de SRI qui permettra de parvenir à un niveau élevé de SRI et à le maintenir.

▪ **Acteurs.** La directive SRI impose ainsi aux administrations publiques et aux « acteurs du marché » des mesures de prévention des risques en termes de cybersécurité et des mesures de notification à l'autorité compétente (en France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI **(2)**) qui est depuis 2009, l'autorité nationale en matière de sécurité et de défense des systèmes d'information) des incidents « qui ont un impact significatif sur la sécurité des services essentiels qu'ils fournissent ».

▪ Les « acteurs du marché », qu'il appartiendra à chaque Etat-membre de lister, sont définis par la directive SRI. Il s'agit ainsi notamment :

- pour les acteurs d'internet : des plateformes de commerce électronique, des passerelles de paiement par internet, des réseaux sociaux, des moteurs de recherche, des fournisseurs de cloud. Les fournisseurs d'accès à internet, les fournisseurs de messagerie électronique et les hébergeurs en sont expressément exclus, car ils sont concernés par d'autres dispositions spécifiques ;
- pour les autres acteurs « opérateurs fournissant des services essentiels », il s'agit principalement des acteurs de l'énergie, des transports (notamment aériens), des services bancaires, des infrastructures de marchés financiers et des entreprises du secteur de la santé.

▪ L'autorité compétente pourra procéder à des audits de sécurité.

▪ **Coopération internationale.** Enfin, une coopération renforcée entre Etats-membres est mise en place pour signaler les incidents, sous l'égide de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) **(3)**.

▪ Tous ces acteurs seront ainsi soumis aux nouvelles obligations de sécurité telles qu'elles découleront de la transposition de cette directive qui devra encore être approuvée formellement par le Parlement et le Conseil.

▪ **Délais.** La directive ayant été publiée au Journal Officiel du 19 juillet 2016, les Etats-membres disposeront d'un délai de 21 mois, soit jusqu'au 19 avril 2018, pour transposer la directive dans leur droit national et d'un délai de 6 mois complémentaire pour identifier les « opérateurs de services indispensables ».

(1) http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L1148&from=FR

(2) https://www.ssi.gouv.fr/

(3) https://www.enisa.europa.eu

VIRGINIE BENSOUSSAN-BRULÉ
&
CHLOÉ LEGRIS

▪ ***Issues & Stakes.*** *Given the increasing number of cybersecurity incidents, whether caused by "human mistakes, natural events, technical failures or malicious attacks", and the economic and strategic challenges of such incidents, the Directive concerning measures for a high common level of security of network and information systems across the Union of 6 July 2016 (known as the NIS Directive)* ***(1)*** *aims to achieve "a high common level of security of network and information systems within the Union". To that end, this Directive:*

- *"lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;*
- *creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems;*
- *establishes security requirements for market operators and public administrations."*

▪ *Each Member State shall adopt a national NIS strategy to achieve and maintain a high level of network and information security.*

▪ ***Stakeholders.*** *The NIS Directive requires public administrations and "market operators" to take measures for the prevention of cybersecurity risks and for the notification to the competent authority of incidents "having a significant impact on the security of the core services they provide". In France, the competent authority is the Agence nationale de la sécurité des systèmes or "ANSSI"* ***(2)****, which has been the national authority in the area of cyberdefence and network and information security since 2009.*

▪ *Each Member State shall establish a list of "market operators", which pursuant to the NIS Directive include:*

- *Internet players: e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services. Internet service providers, e-mail providers and web hosting providers are expressly excluded insofar as they are covered by other specific provisions;*
- *other operators providing "essential services": these are mainly operators in the following sectors: energy, transport (e.g., air carriers), banking, financial market infrastructures, and health.*

▪ *The competent authority may carry out security audits.*

▪ ***International cooperation.*** *Lastly, the Directive improves cooperation for the notification of incidents between Member States under the auspices of the European Union Agency for Network and Information Security (ENISA)* ***(3)****.*

▪ *All these operators are thus subject to the new security obligations that will result from the transposition of this Directive, which still has to be formally approved by the Parliament and the Council.*

▪ ***Timeline.*** *Since the Directive was published in the Official Journal of 19 July 2016, Member States will then have 21 months, i.e. until 19 April 2018, to transpose the Directive into their national laws and six additional months to identify "operators of essential services".*

(1) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

(2) https://www.ssi.gouv.fr/

(3) https://www.enisa.europa.eu/

VIRGINIE BENSOUSSAN-BRULÉ
&
CHLOÉ LEGRIS

▪ **La cybercriminalité aujourd'hui.** La cybercriminalité peut être définie, au sens large, comme l'ensemble des infractions commises en ligne par l'utilisation des réseaux de communications électroniques et des systèmes d'information. Protéiforme, elle regroupe notamment : a) les infractions propres à internet (hameçonnage ou « phishing »), b) la fraude et la contrefaçon en ligne (vol d'identité) et c) les contenus illégaux en ligne (pédophilie). Tous les ans, le centre européen de lutte contre la cybercriminalité (EC3) d'Europol, l'agence européenne spécialisée dans la répression de la criminalité, publie un rapport qui évalue la menace que représente la criminalité organisée sur internet, connu sous le nom de rapport IOCAT (Internet Organised Crime Threat Assessment). L'édition de 2016 constate l'augmentation des cyberattaques en termes d'intensité, de volume et de sophistication **(1)**, et identifie un certain nombre de points clés parmi lesquels : l'identification des rançongiciels (« ransomware ») chiffrants (les « cryptoware ») comme la menace n°1 parmi les logiciels malveillants, l'augmentation du nombre de contenus pédopornographiques échangés sur le Darknet, la progression, en intensité et en complexité, des attaques en déni de service (DDoS) et, de manière générale, l'aptitude des cybercriminels à adapter rapidement leurs pratiques illégales aux nouvelles technologies émergentes.

▪ **La cybersécurité, une priorité stratégique de l'UE.** Le programme européen en matière de sécurité **(2)** érige la cybercriminalité en priorité absolue du mandat actuel de la Commission européenne dans le domaine de la sécurité, au même titre que le terrorisme et la criminalité organisée. Les thèmes de la cybersécurité et de la cybercriminalité s'inscrivent dans les domaines d'action de la stratégie pour un marché unique numérique, dont les objectifs sont notamment d'améliorer les moyens disponibles pour la cybersécurité dans les États membres, de renforcer la coopération des États membres en ce qui concerne la cybersécurité, de favoriser l'industrie européenne de la cybersécurité, et d'intégrer la cybersécurité dans les futures initiatives politiques de l'UE dès la départ, en particulier en ce qui concerne les nouvelles technologies et les secteurs émergents tels que les voitures connectées, les réseaux intelligents et l'internet des objets **(3)**. Les initiatives et les activités menées par l'UE en faveur de la sécurité des réseaux et de l'information s'appuient sur l'agence européenne de cybersécurité, c'est-à-dire l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), ainsi que sur le CERT-EU, le centre d'alerte et de réaction aux attaques informatiques de l'UE, constitué d'experts en sécurité informatique des principales institutions de l'UE.

▪ **La directive NIS.** Première loi européenne sur la cybersécurité, la directive (UE) 2016/1148 sur la sécurité des réseaux et des systèmes d'information (dite directive NIS), a été adoptée par le Parlement européen le 6 juillet 2016 **(4)**. La directive NIS s'applique aux opérateurs de services essentiels (dans les secteurs de l'énergie, des transports, de la banque et de la santé, etc.) ainsi qu'aux fournisseurs de service numérique, tels que les places de marchés en ligne, les services d'informatique en nuage (« cloud computing »), et les moteurs de recherche en ligne. L'objectif de la directive est d'assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'UE, et à cette fin, elle impose aux Etats membres l'obligation d'adopter une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, institue un groupe de coopération afin de faciliter la coopération stratégique et l'échange d'informations entre les États membres, et établit des exigences de gestion des risques et de notification des incidents pour les opérateurs de services essentiels et les fournisseurs de service numérique. Les États membres, dont la Grèce, ont jusqu'à mai 2018 pour transposer la directive NIS dans leur droit national.

(1) https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

(2) Programme européen en matière de sécurité, Strasbourg, 28.4.2015, COM (2015), 185 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_fr.pdf

(3) Marché unique numérique, Cybersecurité, https://ec.europa.eu/digital-single-market/en/cybersecurity

(4) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

GEORGE A. BALLAS
&
THEODORE KONSTANTAKOPOULOS

▪ ***Cybercrime today.*** *Cybercrime can be broadly defined as criminal acts committed online with use of electronic communications networks and information systems, including (a) crimes specific to the Internet (e.g. phishing), (b) online fraud and forgery (e.g. identity theft), and (c) illegal online content (e.g. child sexual abuse material). According to the 2016 Internet Organised Crime Threat Assessment (IOCTA), a yearly report on developments and emerging threats in cybercrime produced by Europol's European Cybercrime Centre (EC3), cyber-attacks are increasing in terms of intensity, volume and quality* ***(1)****: Cryptoware (encryption ransomware) has become the most prominent malware threat, the volume of child sexual exploitation material exchanged on the Darknet increases in volume, DDoS attacks continue to grow in intensity and complexity, and generally findings demonstrate that criminals quickly adapt to and abuse emerging technologies.*

▪ ***Cybersecurity, a strategic EU priority.*** *The European Agenda on Security* ***(2)*** *lists cybercrime, along with terrorism and organised crime, as a top priority for the current mandate of the European Commission in the field of security. The Digital Single Market strategy is also part of the framework for the EU initiatives on cybersecurity and cybercrime, with its key objectives being to increase cybersecurity capabilities and cooperation between Member States, foster the European cybersecurity industry and to embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the Internet of Things (IoT)* ***(3)****. The EU initiatives and activities on network and information security are supported by the European Network and Information Security Agency (ENISA), the EU's Agency for cyber security, as well as by the Computer Emergency Response Team for the EU institutions (CERT-EU), a team made up of IT security experts from the main EU Institutions.*

▪ ***The NIS Directive.*** *The Directive (EU) 2016/1148 on security of network and information systems (NIS Directive), adopted by the European Parliament on 6 July 2016* ***(4)****, is the first piece of EU-wide legislation on cybersecurity. The NIS Directive applies to operators of essential services (e.g. in the energy, transport, banking, health sectors) and to digital service providers (including online marketplaces, cloud computing services and search engines). Its objective is to achieve a high common level of security of network and information systems within the EU, introducing an obligation to adopt national strategies on the security of network and information systems, facilitating strategic cooperation and the exchange of information among Member States, and imposing risk management and incident reporting obligations for operators of essential services and digital service providers. Member States, including Greece, must transpose the NIS Directive into national law by May 2018.*

(1) https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

(2) The European Agenda on Security, Strasbourg, 28.4.2015 COM (2015), 185 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

(3) Digital Single Market, Cybersecurity, https://ec.europa.eu/digital-single-market/en/cybersecurity

(4) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

GEORGE A. BALLAS
&
THEODORE KONSTANTAKOPOULOS

▪ **Stratégie nationale de sécurité du cyberespace.** Par une résolution n°36/2015 du Conseil des ministres du 12 juin 2015, le Portugal a adopté une stratégie nationale pour la sécurité du cyberespace. Elle énonce les lignes d'action stratégiques dans divers domaines afin d'assurer la protection et la sauvegarde des infrastructures essentielles et des services d'information d'importance vitale, et de promouvoir une utilisation gratuite, sûre et efficace du cyberespace pour tous les citoyens, les entreprises et les organismes publics et privés.

▪ Cette stratégie s'articule autour de quatre objectifs, à savoir :

- la promotion d'une utilisation consciente, gratuite, sûre et efficace du cyberespace ;
- la protection des droits fondamentaux, de la liberté d'expression, des données à caractère personnel et de la vie privée des citoyens ;
- le renforcement de la sécurité du cyberespace, des infrastructures essentielles et des services nationaux d'importance vitale ; et
- l'affirmation du cyberespace comme domaine d'innovation et de développement économique.

▪ Afin d'atteindre ces objectifs, la stratégie nationale pour la sécurité du cyberespace prévoit différents domaines d'intervention, au premier rang desquels la lutte contre la cybercriminalité. Dans ce domaine, l'ambition du Portugal est de :

- réviser et mettre à jour la législation sur la cybercriminalité (ce point n'a pas encore été mis en œuvre) ; et
- favoriser les capacités de maintien de l'ordre, avec la création de l'unité nationale pour la lutte contre la cybercriminalité et la criminalité technologique (« UNC3T »). L'une des responsabilités de l'UNC3T est précisément la prévention, la détection, et l'enquête en ce qui concerne les infractions énoncées dans la loi n°109/2009 du 15 septembre 2009, ainsi que la coopération avec les tribunaux en la matière.

▪ **Cybercriminalité.** La loi n°109/2009 du 15 septembre 2009 sur la cybercriminalité établit un ensemble de règles pénales matérielles et procédurales (articles 3 à 8, et 11 à 19), et contient des dispositions relatives à la coopération internationale en matière pénale (articles 20 à 26), dans le domaine de la cybercriminalité et de la collecte de preuves sous forme électronique. La loi sur la cybercriminalité érige en infractions les actions suivantes :

- la falsification informatique (article 3) ;
- l'atteinte aux programmes ou aux autres données informatiques (article 4) ;
- le sabotage informatique (article 5) ;
- l'accès frauduleux (article 6) ;
- l'interception illégale (article 7) ; et
- la reproduction illégale de programmes protégés (article 8).

▪ D'autres cyberinfractions sont régies par le code pénal portugais, telles que i) l'intrusion par la voie des technologies de l'information (article 193), ii) l'atteinte au secret des correspondances ou des télécommunications (article 194), et iii) la fraude informatique et de communication (article 221).

▪ Il convient par ailleurs de mentionner la récente inclusion dans le code pénal portugais de l'article 176-A (1), qui réprime spécifiquement la sollicitation de mineurs à des fins sexuelles « par le biais des technologies de l'information et de la communication ».

▪ Enfin, il ne faut pas oublier que la cybercriminalité englobe également toutes les infractions « traditionnelles » commises par l'utilisation d'outils informatiques : c'est le cas par exemple de la diffamation ou de la calomnie, lorsque des propos portant atteinte à l'honneur sont tenus dans des publications ou de commentaires diffusés sur les réseaux sociaux.

▪ Cybersurveillance**.** Dans le domaine de la cybersurveillance, le principe consacré de l'inviolabilité des communications électroniques souffre de plusieurs exceptions légales. Sont ainsi autorisés :

- l'enregistrement des communications et des données associées effectué dans le cadre d'une pratique commerciale légale en vue de prouver une transaction commerciale ou toute autre communication faite dans le cadre d'une relation contractuelle, à condition que la personne concernée en ait été informée et ait donné son consentement ;
- l'enregistrement de communications relatives à des situations d'urgence à destination et en provenance des services publics ;
- le traitement de données à des fins de facturation ;
- l'enregistrement, le traitement et la transmission de données de géolocalisation ou de localisation par des organismes habilités à recevoir et à traiter des appels d'urgence ; et
- la sauvegarde et la transmission de données relatives aux personnes physiques et morales, ainsi que les données associées, nécessaires pour l'identification, par les autorités compétentes, d'abonnés ou d'utilisateurs enregistrés, aux fins d'enquête, de détection et de poursuite de crimes graves.

▪ En principe, le responsable du traitement ne peut procéder au traitement de ces données qu'après avoir obtenu une autorisation préalable accordée par l'autorité portugaise de protection des données, la CNPD, conformément à l'article 28, paragraphe 1, alinéa a, de la loi n°67/98 du 26 octobre 1998 sur la protection des données à caractère personnel.

▪ En ce qui concerne la collecte de preuves dans les procédures pénales, trois régimes distincts s'appliquent respectivement aux écoutes téléphoniques, au stockage des preuves électroniques dans les systèmes informatiques et, aux données générées ou traitées dans le cadre de la fourniture de services de communications électroniques (l'exemple classique étant la géolocalisation des téléphones portables).

▪ Premièrement, l'interception et l'enregistrement de conversations ou d'appels téléphoniques peuvent être autorisés lors de l'enquête sur une infraction lorsque ces opérations sont jugées essentielles pour la découverte de la vérité, ou lorsque que la preuve est impossible ou très difficile à obtenir d'une autre manière. Dans ce cas, une ordonnance judiciaire autorisant l'écoute téléphonique reste toutefois requise et une demande à cet effet doit être déposée par le ministère public. En outre, cette possibilité n'est ouverte que pour certains types d'infraction (article 187 du code de procédure pénale).

▪ Deuxièmement, la loi sur la cybercriminalité comprend des règles de procédure relatives au stockage des preuves électroniques dans les systèmes informatiques. Entrent dans le champ de ces règles les infractions prévues expressément dans ladite loi, ainsi que les infractions commises par l'utilisation un système informatique (infractions « traditionnelles » commises par l'intermédiaire d'outils informatiques) et les infractions pour lesquelles il est nécessaire de recueillir des preuves sous forme électronique.

▪ Enfin, troisièmement, aux termes de la loi n°32/2008 du 17 juillet 2008 qui a transposé en droit portugais la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, les données ne peuvent être conservées et transmises qu'aux fins de la détection et de la poursuite d'infractions graves par les autorités compétentes. En tout état de cause, la transmission de données aux autorités compétentes ne peut être autorisée que par une ordonnance du tribunal.

▪ L'articulation de ces trois régimes peut causer une certaine confusion, selon les moyens de preuve et le type d'infraction concernés, et fait d'ailleurs l'objet de nombreux débats au sein de la doctrine et de la jurisprudence portugaises.

JOÃO P. ALVES PEREIRA

&

MIGUEL GASPAR

▪ ***National Cyberspace Security Strategy.*** *Council of Ministers resolution No. 36/2015, of 12 June, approved the National Cyberspace Security Strategy, setting forth the strategic lines of action in various fields as a way to ensure the protection and safeguard of critical infrastructure and vital information services, and potentially a free, safe and efficient use of cyberspace for all citizens, companies and public and private entities.*

▪ *This strategy aims at four strategic objectives, namely:*

- *To promote a conscious, free, safe and efficient use of cyberspace;*
- *To protect fundamental rights, freedom of expression, personal data and the privacy of citizens;*
- *To ensure and strengthen cyberspace security, critical infrastructures and national vital services; and*
- *To affirm cyberspace as a domain of innovation and economic development.*

▪ *For the achievement of the abovementioned objectives, the National Cyberspace Security Strategy has different fields of intervention, including the fight against cybercrime by means of the following measures:*

- *Revision and update of legislation on cybercrime (which has not been implemented yet); and*
- *Fostering policing capacities, with the creation of the National Unit For Cybercrime and Technological Crime Combat ("UNC3T"). One of the responsibilities of UNC3T is precisely the prevention, detection, criminal investigation and articulation with the courts in relation to the crimes provided for in Law No. 109/2009 of 15 September (i.e. Cybercrime Law).*

▪ ***Cybercrime.*** *Law No. 109/2009 of 15 September (Cybercrime law) establishes a set of material and procedural criminal rules (articles 3 to 8 and 11 to 19), as well as provisions on international cooperation in criminal matters (articles 20 to 26), concerning the field of cybercrime and the collection of evidence in electronic format. The Cybercrime law typified the following crimes:*

- *The crime of computer falsehood (article 3);*
- *Damage related to programs or other computer data (article 4);*
- *Computer sabotage (article 5);*
- *Illegitimate access (article 6);*
- *Illegitimate interception (article 7); and*
- *Illegitimate reproduction of protected program (article 8).*

▪ *We can also find several types of cybercrimes ruled by the Portuguese Criminal Code, namely (i) the crime of intrusion through information technology (article 193), (ii) the crime of violation of the secrecy of correspondence or telecommunications (article 194), and (iii) the crime of computer and communication fraud (article 221).*

▪ *It is also worth mentioning the recent inclusion in our Criminal Code of article 176-A (1), that specifically provides for the crime of solicitation of minors for sexual purposes "*through information and communication technologies*".*

▪ *Finally, one must also consider the "so-called" common crimes committed through the use of computer tools (e.g. crimes against honour, such as defamation or slander, which are practiced through publications or comments on social networks).*

▪ ***Cyber-surveillance.*** *In the area of Cyber-surveillance the principle of inviolability of electronic communications is applicable, although there are several legal exceptions to this principle including:*

- *The authorised recording of communications and respective data, when carried out in the course of a lawful business practice for the purpose of serving as proof of a commercial transaction or of any other communication made in the course of a contractual relationship, provided that the data subject has been informed and that has given his consent;*
- *The recording of communications to and from public services dealing with emergency situations of any kind;*
- *He processing of data for billing purposes;*
- *The registration, processing and transmission of geolocation or location data to organizations with legal powers to receive emergency calls for the purpose of responding to such calls; and*
- *The safeguard and transmission of data relating to individuals and legal persons, as well as related data required to identify the subscriber or registered user, for purposes of investigation, detection and prosecution of serious crimes by the competent authorities.*

▪ *In principle, a prior authorization granted by the Portuguese Data Protection Authority ("CNPD") is required for the processing of this data by the data controller, pursuant to Article 28 (1)(a) of Law no. 67/98 of 26 October ("Law on Protection of Personal Data").*

▪ *With regard to the collection of evidence in criminal proceedings, it is necessary to distinguish between three applicable procedural regimes, i.e. the procedural rules for wiretapping, the procedural rules on the storage of electronic evidence in computer systems and, finally, the procedural rules for data generated or processed in connection with the provision of electronic communications services (the classic example is cell phone geolocation).*

▪ *The interception and recording of conversations or telephone calls can be authorised during the investigation of a crime if the procedural step is found to be essential for the discovery of truth or provided that the evidence is either impossible or very difficult to obtain in any other way. However, a court order authorising the wiretapping is required and an application to such effect must be filed by the Public Prosecutor's Office. Furthermore, this option is only available for certain types of crime (article 187 of the Criminal Procedure Code).*

▪ *On the other hand, Cybercrime law includes procedural rules on the storage of electronic evidence in computer systems, and such rules are applicable to the crimes provided for in such law, to offences committed through a computer system (the so-called common crimes committed through computer tools) and/or to crimes for which it is necessary to collect evidence in electronic format.*

▪ *Finally, Law No. 32/2008 of July 17, which implemented Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, sets forth that the investigation, detection and prosecution of serious crimes by the competent authorities is the sole aim of the retention and transmission of data research. In any case, the transmission of data to the competent authorities can only be authorized by a court order.*

▪ *The articulation of these three differentiated procedural regimes can generate some confusion, depending on the means of evidence and the type of crime. In fact, such articulation is the subject of much debate in Portuguese doctrine and case law.*

JOÃO P. ALVES PEREIRA

&

MIGUEL GASPAR

▪ **Définition de la cybercriminalité :** il n'existe pas de définition unifiée de la cybercriminalité dans la législation pénale russe. Le code pénal de la Fédération de Russie distingue en effet plusieurs types d'infractions dans le domaine de la cybersécurité **(1)** : a) l'accès illicite à des données informatiques protégées par la loi, si celui-ci entraîne la destruction, le blocage, la modification ou la copie de ces données, b) la création, la distribution et l'utilisation de logiciels conçus pour l'accès, la destruction, la modification, la copie ou le blocage illicite de données informatiques, c) la violation des règles de sécurité en matière de stockage, de traitement et de transfert de données si celle-ci résulte dans les conséquences susmentionnées, d) la fraude dans le domaine des données informatiques. Les données légalement protégées s'entendent de toute information bénéficiant d'un régime de sécurité spécial, telle que par exemple les informations relevant du secret d'État, du secret médical, du secret bancaire, du secret commercial, ou encore les données à caractère personnel. **(2)**

▪ **Doctrine en matière de sécurité de l'information :** aujourd'hui, la cybersécurité est indéniablement un enjeu majeur **(3)**. C'est pourquoi la Russie s'est dotée d'une doctrine de cybersécurité. Ce texte dresse l'état actuel de la sécurité de l'information en Russie, en identifiant les intérêts nationaux ainsi que les principales menaces pesant sur la sécurité de l'information, et fixe les objectifs fondamentaux ainsi que les grandes orientations du pays dans ce secteur. Cette doctrine tend à axer la réglementation future sur la protection des intérêts publics, plutôt que les intérêts privés.

▪ **Projet de loi sur la sécurité des infrastructures d'information critiques (4)** : Adopté en première lecture par la Douma d'État de la Fédération de Russie (chambre basse du Parlement russe) le 27 janvier 2017, ce projet de loi marque la première étape de la mise en œuvre de la doctrine de cybersécurité **(3)**. Une infrastructure d'information critique (« IIC ») est définie comme un ensemble d'« installations d'infrastructure critique » **(5)**, appartenant généralement à des secteurs industriels stratégiques. Les ICC devraient notamment être recensées dans un registre spécial, tenu par un organisme autorisé. Si ce projet de loi est approuvé, il imposera, dès son entrée en vigueur, des obligations spécifiques pour tout ce qui a trait à la sécurité informatique aux exploitants d'ICC. En particulier, lorsque ces installations impliquent le traitement de secrets d'Etat, l'utilisation d'outils de chiffrement certifiés sera obligatoire. L'enjeu pour les fournisseurs de solutions de chiffrement et de sécurité technique sera alors de décocher cette certification. Le projet de loi prévoit, par ailleurs, de modifier certaines dispositions du code pénal **(6)**. Des sanctions sont ainsi prévue pour : a) la création et l'utilisation d'un logiciel ou d'une information dans le but d'entraver illégalement une IIC, b) l'accès illégal aux informations sécurisées contenues dans une IIC, notamment par l'utilisation d'un tel logiciel, et c) le non-respect des règles relatives au stockage, au traitement et au transfert de données sécurisées ou des règles d'accès à ces informations et systèmes d'information.

REFERENCES

(1) Code pénalde la Fédération de Russie au 13 juin 1996 n°63-FZ.

(2) Lignes directrices des concernant les activités de surveillance dans le domaine des cyberinfractions à destination des procureurs adoptées par le Bureau du Procureur général.

(3) Doctrine de la cybersécurité en Fédération de Russie adoptée par l'Ordre du Président de la Fédération de Russie du 5 décembre 2016.

(4) Projet de loi sur la sécurité de l'infrastructure d'information critique n ° 47579-7.

(5) Les installations d'infrastructure d'information critiques sont définies très largement et regroupent : les systèmes d'information et les réseaux de télécommunication utilisés par les pouvoirs publics, ainsi que les systèmes d'information, réseaux de télécommunication et les systèmes de traitement automatisés utilisés par les industries de la défense, de la santé, des transports, des communications, de l'énergie et du nucléaire, de l'aérospatiale, de l'acier et du métal et de la chimie.

(6) Projet de loi n°47591 de modification du code pénal de la Fédération de Russie et du code de procédure pénale de la Fédération de Russie dans le cadre de l'adoption du projet de loi fédérale sur la sécurité des infrastructures d'information critiques (adopté par la Douma d'Etat en première lecture le 27 janvier 2017).

MARIA OSTASHENKO

▪ ***Cybercrime today:*** *There is no unified definition of a cyber-crime in Russian criminal legislation. The Criminal Code distinguishes several types crimes in the sphere of cyber security* ***(1)****: a) illegal access to legally protected information that leads to its destruction, blocking, modification or copying, b) creation, distribution and use of software designed for such illegal access, destruction, modification, copying or blocking of computer information, c) breaking rules of secured data storage, processing and transfer that led to the mentioned consequences, d) fraud in the sphere of computer information. Legally protected information covers any type of information, which is provided with a special security regime, including state, medical, banking and commercial secrets, personal data etc.* ***(2)***

▪ ***Information Security Doctrine:*** *Cybersecurity is a recognized core strategical issue* ***(3)****. The Doctrine determines national interests in the sphere of information, main information security threats and the current state of information security, core aims and directs of further development in the given sphere and organizational basics of information security. The common sense of the Doctrine is that further regulatory development will move towards protection of public interests rather than private.*

▪ ***Draft Law on Security of Critical Information Infrastructure (4)*** *was adopted by the Russian State Duma (lower bench of Russian Parliament) in the first hearing of three on January 27, 2017. The Draft Law is the first step on realization the Doctrine* ***(3)****. Critical Information Infrastructure is a scope of Critical Infrastructure Objects* ***(5)****, which are generally the objects of strategic industrial areas. For the accounting of Important Objects special Register of the Important Critical Informational Infrastructure shall be maintained by an authorized executive body. The Draft Law, if it is approved and enters into force, will impose specific cyber security obligations to the players owning objects attributed to critical infrastructure. In particular, as operation of such Objects implies processing of state secrecy, organisations owning the Object will have to use certified encryption tools. This will have an impact both on owners of the Objects and suppliers of technical security means. Challenge for the latter refers to certification of technical security means, which is obligatory for processing of state secrecy. The Draft law is accompanied by amendments to the Criminal Code* ***(6)****. Liability measures are imposed for a) creation and use of a software or information aimed to illegally influence Critical Information Infrastructure, b) illegal access to secured information contained in Critical Information Infrastructure, i.a. with use of the mentioned software, and c) breaking rules of secured data storage, processing and transfer, or access rules to such information and information systems.*

REFERENCES

(1) Criminal Code of the Russian Federation as of June 13, 1996 No. 63-FZ.

(2) Guidelines on supervisory activities in the sphere of cyber-crimes carried out by public prosecutors adopted by General Prosecutor's Office.

(3) Doctrine of Cybersecurity in the Russian Federation adopted by the Order of the President of the Russian Federation of December 5, 2016.

(4) Draft Law on Security of Critical Information Infrastructure No. 47579-7.

(5) Critical Information Infrastructure Objects are defined very broadly. They are information systems, telecommunication networks of governmental bodies, as well as information systems, telecommunication networks and automated systems of technological processes operation functioning in defence industry, healthcare, transport, communications, fuel and nuclear industries, aerospace industry, steel and metal, and chemical industries.

(6) Draft Law on Amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation in connection with adoption of the Federal Law on Security of Critical Information Infrastructure No. 47591 (also adopted by the State Duma in the first hearing of three on January 27, 2017).

MARIA OSTASHENKO

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	john@michalsons.com
Allemagne *Germany*	Beiten Burkhardt	Andreas Lober	+49 69 756095-0	andreas.lober@bblaw.com
Australie *Australia*	Madgwicks Lawyers	Dudley Kneller	+61 3 9242 4744	dudley.kneller@madgwicks.com.au
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	jf.henrotte@lexing.be
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Jean-François De Rico	+1 (418) 650 7000	jean-francois.derico@langlois.ca
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	jun.yang@jadefountain.com
Costa Rica *Costa Rica*	Lexing Costa Rica	Gabriel Lizama	+506 2253-1726	glizama@lexing.legal
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	marc.gallardo@lexing.es
États-Unis *USA*	Greenberg Traurig	Françoise Gilbert	+1 650-804 1235	gilbertf@gtlaw.com
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	paris@lexing.law
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	central@balpel.gr
Guatemala *Guatemala*	Morales, Redondo & Vargas	Ada Lissette Redondo Aguilera	+(502)2331-8057	aredondo@consejeros-legales.com
Inde *India*	Poovayya and Co	Siddhartha George	+91 80 4115 6777	siddhartha@poovayya.net
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	r.zallone@studiozallone.it
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	koki.tada@halaw.jp
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	info@kouatlylaw.com
Maroc *Morocco*	Fayçal Elkhatib et Associés S.C.P.A	Hatim Elkhatib	+212 5 39 94 05 25	hatim.elkhatib@elkhatiblawfirm.ma
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	eochoa@carpio.law
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Arve Føyen	+47 21 93 10 00	af@foyentorkildsen.no
Nouvelle-Calédonie *New Caledonia*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	fr.avocat@cabinetroyanez.com
Pologne *Ploand*	Traple Konarski Podrecki i Wspòlnicy	Xawery Konarski	(+48) 12 426 05 30	office@trapel.pl
Portugal *Portugal*	Alves Pereira & Teixeira de Sousa	João P. Alves Pereira	+ 351 21 370 01 90	jpereira@alvespereira.com
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	dpreiskel@preiskel.com
Russie *Russia*	ALRUD	Maria Ostashenko	+ +7 495 234 96 92	mostashenko@alrud.com
Sénégal *Senegal*	SCP Faye & Diallo	Cheikh Faye Mamadou Seye	:(+221) 33 823 60 60	fayetdiallo@orange.sn seyemamadou9@gmail.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 98 37 37 28	yassine.younsi@younsilawyers.com

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 : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/