n°26 Octobre 2020
#26 October 2020

Lexing Insights

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

CYBERCRIMINALITE

CYBERCRIME

LES CYBERATTAQUES NE CONNAISSENT PAS DE FRONTIERES

- Face aux cyberattaques de plus en plus nombreuses et massives, les failles de sécurité sont devenues une préoccupation majeure et incontournable des entreprises en France et dans tous les pays du monde.
- Dans son rapport annuel 2020 sur les cybermenaces l'Agence européenne de cybersécurité ENISA constate que les attaques ne cessent de se développer, devenant plus sophistiquées, ciblées et massives, et qu'elles sont souvent non détectées. Alors que l'Anssi tire la sonnette d'alarme sur les cyberattaques par rançongiciel, et qu'Interpol et le FBI mettent en garde contre la cybercriminalité liée à la pandémie de Covid-19, notamment en raison de l'intensification du recours au télétravail, il est vivement recommandé de se prémunir contre le risque cyber, aussi bien en se dotant d'outils informatiques performants qu'en adaptant sa police d'assurance pour couvrir ces nouveaux risques informatiques.
- Quel est l'arsenal juridique dont dispose les pays dans le monde pour lutter contre les cyberattaques ? Quels sont les principaux vecteurs de la cybercriminalité ? Comment réagir en cas de failles de sécurité ? Le piratage éthique est-il légal ?

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Espagne, France, Grèce, Royaume-Uni.

CYBER ATTACKS KNOW NO BORDERS

- *Amid the increasing number and scale of cyber attacks, security breaches have become a major and unavoidable concern for organizations in France and in all countries around the world.*
- *According to the European Union Agency for Cybersecurity (ENISA) Threat Landscape 2020 report, cyber attacks are becoming more sophisticated, targeted, widespread and undetected. While the ANSSI is sounding the alarm on ransomware, and Interpol and the FBI are warning against cybercrime linked to the Covid-19 outbreak, particularly because of the increased use of telework, it is strongly recommended to protect yourself against cyber risk, by both possessing high-performance IT tools and adapting your insurance policy to cover these new IT risks.*
- *What laws have been adopted in various countries around the world to combat cybercrime? What are the most common cyber threats? How to respond to a cyber attack? Is ethical hacking legal?*

The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: France, Greece, South Africa, Spain, United Kingdom.

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 leurs pays respectifs.

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.

https://lexing.network

VIRGINIE BENSOUSSAN-BRULE
Directeur du pôle Contentieux numérique du cabinet
Lexing Alain Bensoussan-Avocats

Head of the Digital Litigation division of Lexing Alain Bensoussan-Avocats

AFRIQUE DU SUD

MICHALSONS

▪ La cybercriminalité est, depuis maintenant de nombreuses années, un fléau planétaire. A mesure que les progrès technologiques s'accélèrent, les criminels développent dans le même temps des moyens de plus en plus sophistiqués pour commettre leurs crimes et échapper à la loi. Selon le dernier rapport d'Accenture, l'Afrique du Sud a enregistré une augmentation de la cybercriminalité dans tous les secteurs d'activité **(1)**. Cette augmentation peut s'expliquer par le fait que la législation sud-africaine en matière de cybercriminalité n'est pas aussi consolidée et mature que celle d'autres pays.

Législation actuelle

▪ En Afrique du Sud, l'approche adoptée par les tribunaux a d'abord consisté à traiter les affaires qu'ils avaient à trancher en étendant le champ d'application des infractions de *common law* existantes (telles que la fraude et le vol) pour inclure les infractions commises à l'aide de technologies ou en ligne. Toutefois, cette approche a été source d'incertitude et d'incohérences. Le Parlement est alors intervenu et a inclut les infractions liées aux technologies dans la législation. Actuellement, le principal texte législatif qui traite de la cybercriminalité est la loi sur les communications et les transactions électroniques (loi ETC) **(2)**. C'est cette loi principalement qui régit les transactions et les communications électroniques en Afrique du Sud **(3)**. Son chapitre XIII traite spécifiquement des cybercrimes et introduit des infractions pénales liées à :

- l'accès non autorisé à des données ou à l'interception non autorisée de données (communément désignés par le terme de piratage ou de « hacking ») **(4)** ;
- l'atteinte non autorisée à l'intégrité des données (création ou introduction de virus et attaques par déni de service) **(5)** ;
- l'utilisation illicite de dispositifs conçus en vue de contourner les mesures de sécurité pour la protection des données (création ou utilisation de logiciels utilisés pour le piratage) **(6)** ; et
- l'extorsion, la fraude et la falsification informatiques **(7)**.

▪ Pour voir sa responsabilité pénale engagée, l'auteur d'une des infractions prévues par la loi ECT doit avoir eu l'intention de commettre cette infraction **(8)**.

▪ La tentative et la complicité sont également érigées en infraction pénales. **(9)**. Selon l'infraction concernée, les cybercriminels sont passibles d'une amende ou d'une peine d'emprisonnement allant de 12 mois à cinq ans **(10)**.

Législation à venir

▪ En dépit du chapitre XIII de la loi ECT, l'arsenal législatif sur la cybercriminalité n'est pas aussi solide que prévu. C'est pourquoi le Parlement sud-africain a présenté une proposition de loi sur la cybercriminalité **(11)** en 2015. Cette proposition de loi vise à consolider la législation sur la cybercriminalité dans un seul texte législatif en tenant compte du besoin urgent de protéger les citoyens contre la menace croissante de dommages causés par la cybercriminalité. Modifiée à plusieurs reprises en raison des nombreuses consultations publiques

REFERENCES

(1) Insight into the Cyberthreat Landscape in South Africa: https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf#zoom=50 [consulté le 28 septembre 2020]

(2) Electronic Communications and Transactions Act (Loi n°25 de 2002)

(3) https://www.michalsons.com/blog/guide-to-the-ect-act/81

(4) Section 86(1) de la loi ECT

(5) Section 86(2) de la loi ECT

(6) Section 86(3) et (4) de la loi ECT

(7) Section 87 de la loi ECT

(8) https://www.michalsons.com/blog/cyber-crime-explained/2667

(9) Section 88 de la loi ECT

(10) Section 89 de la loi ECT

(11) Cybercrimes Bill B6B-2017: https://www.michalsons.com/wp-content/uploads/2020/06/NA_bills2017_bill06B-2017.pdf

(12) Cybercrimes Bill in South Africa | Overview and Download: https://www.michalsons.com/focus-areas/cybercrime-law/cybercrimes-bill-south-africa

(13) NCOP approves Cybercrimes Bill: https://mybroadband.co.za/news/security/358493-ncop-approves-cybercrimes-bill.html

(12), cette proposition de loi a récemment été adoptée par le Conseil national des provinces et transmise au président pour promulgation (13).

▪ La proposition de loi sur la cybercriminalité étend les infractions créées par la loi ECT et instaure également de nombreuses nouvelles infractions (14). Certaines infractions sont liées aux données, d'autres aux messages, aux ordinateurs ou encore aux réseaux, comme :

- le piratage informatique (15),
- l'interception illégale de données (16),
- la fabrication de faux ou l'usage de faux informatiques (17), ou
- l'extorsion informatique (18).

▪ Ces infractions sont punies d'amendes et de peines d'emprisonnement. Les cybercriminels encourent entre un an et quinze ans en prison, selon le type de l'infraction commise. La proposition de loi sur la cybercriminalité donne également aux tribunaux compétence pour connaître de ces infractions dans certains cas où une incertitude pourrait exister.

▪ La proposition loi sur la cybercriminalité donne aux services de police sud-africains des pouvoirs étendus. Sous réserve de disposer d'un mandat de perquisition, ils peuvent ainsi enquêter, perquisitionner, accéder et saisir des objets, tels qu'un ordinateur, une base de données ou un réseau, où qu'ils se trouvent (19).

▪ Le texte impose également des obligations à certaines organismes. Les fournisseurs de services de communications électroniques et les institutions financières sont en effet tenus de :

- signaler les infractions à la police dans un délai de 72 heures au plus tard,
- préserver toute information qui s'y rapporte (20).

▪ A défaut, ils s'exposent à une amende de 50.000 rands (2.560 euros). Il est important de souligner que ces obligations ne signifient aucunement que les fournisseurs de services de communications électroniques et les institutions financières soient par ailleurs obligés de contrôler les données qu'ils transmettent ou stockent sur leurs systèmes, ou qu'ils aient à rechercher activement les situations qui indiqueraient une activité illégale (21).

▪ Une fois promulguée, la proposition de loi sur la cybercriminalité abrogera les articles de la loi ECT spécifiques à la cybercriminalité (22).

Conclusion

▪ Désireuse de muscler sa législation, l'Afrique du Sud est en voie d'adopter une loi sur la cybercriminalité qui aura, dès son entrée en vigueur, des répercussions importantes pour tous.

[consulté le 28 septembre 2020]

(14) Proposition de loi sur la cybercriminalité, chapitre 2

(15) Proposition de loi sur la cybercriminalité, section 2

(16) Proposition de loi sur la cybercriminalité, section 3

(17) Proposition de loi sur la cybercriminalité, section 9

(18) Proposition de loi sur la cybercriminalité, section 10

(19) Proposition de loi sur la cybercriminalité, section 29

(20) Proposition de loi sur la cybercriminalité, section 54

(21) Cybercrimes Bill in South Africa | Overview and Download: https://www.michalsons.com/focus-areas/cybercrime-law/cybercrimes-bill-south-africa

(22) La proposition de loi sur la cybercriminalité abroge le chapitre 9 et les sections 85, 86, 87, 88 et 90 de la loi ECT

LISA EMMA–IWUOHA

south-africa@lexing.network

▪ *Cybercrimes is an issue that the entire world has grappled with for a long time. As technology advances at a rapid pace, criminals have also developed smarter ways to use technology to commit crimes and evade the law. In the latest report from Accenture, South Africa has seen increases in cybercrimes across industries* ***(1)****. A possible reason is because our cybercrimes law is not consolidated or as developed as other leading nations.*

Existing legislation

▪ *Cybercrimes law is handled by our courts through some cases and common law. The approach the courts took was extending the scope of existing common law crimes (such as fraud and theft) to include crimes that were committed using technology or online. This approach created uncertainty and inconsistency. Parliament then attempted to address this issue by including cybercrimes in legislation. Currently, the main piece of legislation that deals with cybercrimes in South Africa is the Electronic Communications and Transactions Act* ***(2)****. The Electronic Communications and Transactions Act (ECT Act) mainly regulates electronic transactions and communications in South Africa* ***(3)****. Chapter XIII deals specifically with cybercrimes and introduces criminal offences related to:*

- *unauthorised access or interception of data (essentially "hacking")* ***(4)****;*
- *unauthorised interference with data (such as creating or introducing viruses and denial of service attacks)* ***(5)****;*
- *unlawful use of devices that are designed to overcome security measures for the protection of data (this would include creating or using of software that is used for cracking)* ***(6)****; and*
- *computer related extortion, fraud and forgery* ***(7)****.*

▪ *To be guilty of any of the offences in the ECT Act, you must have the intention to commit the offence* ***(8)****.*

▪ *Additionally, any person who attempts to commit any one of these crimes (or who aids or abets someone to commit these crimes) is also guilty of an offence* ***(9)****. Penalties include a fine or imprisonment between 12 months to five years depending on the specific crime* ***(10)****.*

Forthcoming legislation

▪ *Despite Chapter XIII of the ECT Act, cybercrimes law in South Africa was not robust as intended. To combat this issue, the South African Parliament introduced the Cybercrimes Bill* ***(11)*** *in 2015. The Bill aims to consolidate cybercrimes law in one piece of legislation taking into account the urgent need to protect citizens from the increasing threat of harm caused by cybercrimes. The Bill has gone through several iterations and changes because of many rounds of public participation* ***(12)****. The Bill was recently passed by the National Council of Provinces and has been sent to the President to sign into law* ***(13)****.*

REFERENCES

(1) 'Insight into the Cyberthreat Landscape in South Africa'. Available: https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf#zoom=50 [Accessed on 28 September 2020]

(2) 25 of 2002

(3) https://www.michalsons.com/blog/guide-to-the-ect-act/81

(4) Section 86(1) of the ECT Act

(5) Section 86(2) of the ECT Act

(6) Section 86(3) and (4) of the ECT Act

(7) Section 87 of the ECT Act

(8) https://www.michalsons.com/blog/cyber-crime-explained/2667

(9) Section 88 of the ECT Act

(10) Section 89 of the ECT Act

(11) Cybercrimes Bill B6B-2017 available at: https://www.michalsons.com/wp-content/uploads/2020/06/NA_bills2017_bill06B-2017.pdf

(12) Cybercrimes Bill in South Africa | Overview and Download: https://www.michalsons.com/focus-areas/cybercrime-law/cybercrimes-bill-south-africa

(13) NCOP approves Cybercrimes Bill' Available at: https://mybroadband.co.za/news/security/358493-ncop-approves-cybercrimes-bill.html

▪ *The Cybercrime Bill expands on the offences created in the ECT Act and also creates many new offences **(14)**. Some offences are related to data, messages, computers, and networks. For example:*

- *Hacking **(15)**,*
- *unlawful interception of data **(16)**,*
- *cyber forgery and uttering **(17)**, or*
- *cyber extortion **(18)**.*

▪ *The penalties in the Bill consist of fines, imprisonment, or both. If you commit a crime, you could spend between one year to fifteen years in prison, depending on the cybercrime. The Cybercrime Bill also gives the courts jurisdiction to try these offences in some cases where there is uncertainty.*

▪ *The Cybercrimes Bill gives the South African Police Service (including their members and investigators) extensive powers to investigate, search, access and seize items like a computer, database or network, wherever it might be located, provided they have a search warrant **(19)**.*

▪ *The Bill also places obligations on certain organisations. Electronic Communications Service Providers (ECSPs) and financial institutions must:*

- *report offences to the police no later than 72 hours,*
- *preserve any information that relates to it **(20)**.*

▪ *If an ECSP or a financial institution does not comply, they can pay a fine of R50 000. This does not mean that ESCPs and financial institutions have to monitor the data they transmit or store on their systems. They also don't have to actively look for situations that indicate unlawful activity **(21)**.*

▪ *Once enacted, the Cybercrimes Bill repeals the cybercrime-specific sections of the ECT Act **(22)**.*

Parting thoughts

South Africa is on its way to a more robust law to regulate cybercrimes. Once the Cybercrimes Bill is enacted and fully in force, it will have a significant impact on many organisations and individuals.

[Accessed on 28 September 2020]

(14) Chapter 2 of the Cybercrimes Bill

(15) Section 2 of the Cybercrimes Bill

(16) Section 3 of the Cybercrimes Bill

(17) Section 9 of the Cybercrimes Bill

(18) Section 10 of the Cybercrimes Bill

(19) Section 29 of the Cybercrimes Bill

(20) Section 54 of the Cybercrimes Bill

(21) Cybercrimes Bill in South Africa | Overview and Download: https://www.michalsons.com/focus-areas/cybercrime-law/cybercrimes-bill-south-africa

(22) The Bill repeals Chapter 9, and sections 85, 86, 87, 88 and 90 of the ECT Act

LISA EMMA–IWUOHA

south-africa@lexing.network

▪ La cybercriminalité continue son ascension exponentielle en Espagne, selon le rapport sur la cybercriminalité rendu public récemment par le ministère de l'intérieur. L'année dernière, 218 302 délits commis sur Internet ont été signalés, soit 35,8 % de plus qu'en 2018, où ils étaient 160 729 ; et presque le double des 117 399 enregistrés en 2017. Avec ce nouveau chiffre, la cybercriminalité représente désormais 9,9 % des 2,2 millions d'infractions pénales connues l'année dernière, alors qu'elle représentait 4,6 % de l'ensemble des délits trois ans plus tôt seulement. En 2020, il est prévisible que ces chiffres augmenteront encore plus après que la police aura détecté une augmentation de ces crimes allant jusqu'à 70 % lors du confinement.

▪ La forme de cybercriminalité la plus courante, la fraude sur Internet, est devenue, avec 192 375 cas (88,1 % de la cybercriminalité totale), la deuxième plus fréquente, derrière le vol uniquement et dépassant les autres formes traditionnelles de criminalité telles que le cambriolage et les dommages. Les menaces et la coercition sont les deuxièmes formes de cybercriminalité les plus courantes, avec 12 782 cas, soit pratiquement le même nombre que l'année précédente. Les experts de la police soulignent que ces chiffres ne reflètent que la cybercriminalité connue et signalent que, dans de nombreux cas, lorsque le montant escroqué est faible, les victimes ne le signalent pas.

▪ Le rapport du ministère de l'intérieur - le premier à recueillir des données auprès de toutes les forces de police, y compris les forces régionales et locales - reflète également le faible pourcentage de résolution : seulement 30 841 cas ont été résolus, soit 15,1 % du total, contre près de 90 % de succès de la police dans d'autres crimes comme les homicides. Au total, 8 914 personnes ont été arrêtées ou ont fait l'objet d'une enquête pour ces crimes l'année dernière. Le profil de ces personnes est celui d'un homme (6 625, 74,3 %), âgé de 26 à 40 ans et de nationalité espagnole (7 098, 79,6 %).

▪ L'augmentation de ces crimes est liée à leur « haute rentabilité », au coût de plus en plus faible du matériel nécessaire pour les commettre et à la réduction du risque pour leurs auteurs. En fait, les chercheurs ont détecté que des criminels qui avaient commis d'autres délits auparavant ont « migré » vers la cybercriminalité. La stratégie nationale contre le crime organisé - document élaboré en février 2019 par le ministère de l'intérieur pour définir les lignes d'action de la police pour les années à venir afin de lutter contre cette nouvelle criminalité - a également mis en garde contre l'augmentation de la cybercriminalité chez les « entrepreneurs individuels du crime ». Il s'agit de cybercriminels qui vendent leurs services à des groupes de crime organisé, comme des listes de numéros de cartes de crédit avec leurs mots de passe pour le pillage de comptes.

▪ En Espagne, le code pénal a été modifié en 2016 pour couvrir des types spécifiques de cybercriminalité, à savoir le piratage, les attaques par déni de service, le phishing, l'infection de systèmes informatiques par des logiciels

malveillants (y compris les logiciels de rançon, les logiciels espions, les vers, les chevaux de Troie et les virus), la possession ou l'utilisation de matériel, de logiciels ou d'autres outils utilisés pour commettre des cyberdélits, l'usurpation d'identité ou la fraude à l'identité, le vol électronique (abus de confiance par un employé actuel ou ancien, ou violation criminelle des droits d'auteur) et toute autre activité qui affecte ou menace la sécurité, la confidentialité, l'intégrité ou la disponibilité de tout système informatique, infrastructure, réseau de communication, dispositif ou données.

▪ Le défaut de mise en œuvre de mesures de cybersécurité par une organisation n'est pas prévu par le code pénal espagnol. Toutefois, en vertu du RGPD, les organisations peuvent se voir infliger une amende si elles ne mettent pas en place des mesures appropriées pour prévenir les violations de données, en tenant compte des développements techniques les plus récents, des risques, de la nature des données personnelles traitées et des atteintes aux droits et libertés de la personne concernée.

▪ En vertu de la législation espagnole, l'assurance contre les incidents est autorisée. Par conséquent, la tendance à la cyberassurance se développe rapidement, de nombreux grands fournisseurs proposant des cyberassurances pour faire face à ces nouveaux risques.

▪ L'Espagne a signé la Convention de Budapest sur la cybercriminalité, le premier traité international visant à lutter contre la cybercriminalité en harmonisant les lois nationales, en améliorant les techniques d'enquête et en renforçant la coopération entre les nations.

▪ L'Espagne a publié un Code de cybersécurité qui répertorie toutes les lois applicables en matière de cybersécurité (1).

(1) https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1

MARC GALLARDO

spain
@lexing.network

▪ *Cybercrime continues its exponential rise in Spain, according to the report on cybercrime made public recently by the Ministry of the Interior. Last year, 218,302 crimes committed on the Internet were reported, 35.8% more than in 2018, when there were 160,729; and almost double the 117,399 registered in 2017. With this new figure, cybercrime now represents 9.9% of the 2.2 million criminal offenses known to have been committed last year, when just three years earlier it accounted for 4.6% of all crime. In 2020, it is foreseeable that these figures will increase even more after the police have detected an increase in these crimes of up to 70% during confinement.*

▪ *The most common form of cybercrime, Internet fraud, has become, with 192,375 cases (88.1% of total cybercrime), the second most common, behind only theft and surpassing other traditional forms of crime such as burglary and damage. The second most common cybercrime is threats and coercion, with 12,782 cases, practically the same number as the previous year. Police experts stress that these figures only reflect known cybercrime and point out that on many occasions, when the amount defrauded is small, victims do not report it.*

▪ *The report from the Ministry of the Interior -the first to collect data from all police forces, including regional and local ones- also reflects the low percentage of resolution: only 30,841 were solved, 15.1% of the total, compared to nearly 90% of police success in other crimes such as homicides. In total, 8,914 people were arrested or investigated for these crimes last year. The profile of these is that of a man (6,625, 74.3%), between 26 and 40 years old and of Spanish nationality (7,098, 79.6%).*

▪ *The increase in these crimes is linked to their "high profitability", the increasingly lower cost of the equipment needed to commit them and the reduced risk for their perpetrators. In fact, researchers have detected that criminals who previously committed other crimes have "migrated" to cybercrime. The National Strategy against Organized Crime -the document drawn up in February 2019 by the Ministry of the Interior to set out the lines of police action for the coming years in order to tackle the new criminality- also warned about the increase in cyber criminality among the so-called "individual crime entrepreneurs". These are cybercriminals who sell their services to organized crime groups, such as lists of credit card numbers with their passwords for looting accounts.*

▪ *In Spain, the Criminal Code was amended in 2016 to cover specific types of cybercrime, i.e. hacking, denial-of-service attacks, phishing, infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses), possession or use of hardware, software or other tools used to commit cybercrime, identity theft or identity fraud, electronic theft (breach of confidence by a current or former employee, or criminal copyright infringement) and any other activity that*

affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

▪ *Failure by an organization to implement cybersecurity measures is not foreseen by the Spanish Criminal Code. However, under the GDPR, organizations may be fined if they do not have in place appropriate measures to prevent data breaches, taking into account the most recent technical developments, risks, the nature of personal data being processed and the damages to the rights and freedom of the data subject.*

▪ *Under Spanish law, insurance against incidents is permitted. Therefore, the cyber-insurance trend is growing rapidly with many major providers offering cyber-insurance in order to cope with these new risks.*

▪ *Spain has signed the Budapest Convention on Cybercrime, the first international treaty seeking to address cybercrime by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.*

▪ *Spain has published a Cybersecurity Code listing all the applicable laws related to cybersecurity* ***(1)****.*

(1) *https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1*

MARC GALLARDO

spain
@lexing.network

Cyberattaques : comment réagir en cas de failles de sécurité ?

▪ Face aux cyberattaques de plus en plus nombreuses et massives, les failles de sécurité sont devenues une préoccupation majeure et incontournable des entreprises en France et dans tous les pays du monde.

▪ Les cyberattaques sont en constante augmentation (1) et, en raison de la crise sanitaire, il y a tout lieu de penser que l'on enregistrera prochainement une nouvelle hausse de la cybercriminalité (2). La société Google a annoncé intercepter chaque jour plus de 18 millions de courriers électroniques malveillants ou d'hameçonnage liés à la Covid-19 (3).

▪ Or, selon le baromètre IPSOS pour PwC sur la cybersécurité publié en octobre 2018, les entreprises françaises seraient généralement plutôt dans la sous-estimation, voire le déni, du risque de cybercriminalité. En effet, seule 1 entreprise française sur 2 avait mis en place une stratégie de cybersécurité et seules 2 entreprises sur 10 se disaient « tout à fait capables » de gérer une cyberattaque (4).

▪ Parallèlement, les conséquences financières explosent. Une étude menée par l'assureur Hiscox début 2020, avant la pandémie de coronavirus, auprès de plus de 5500 professionnels, a montré qu'en France le coût moyen des cyberattaques s'élevait à 35.000 € contre 9.000 € en 2019, soit une augmentation de 290%. Pour les grandes entreprises (+1000 employés), la moyenne des pertes culmine à 458.000 €. (5)

▪ Paradoxalement, malgré l'augmentation des cyberattaques et du coût attribué aux incidents de cybersécurité, près de la moitié des plus grandes entreprises françaises se préparent à stabiliser leurs budgets en matière de cybersécurité, tandis que pour l'autre moitié, un quart va les baisser et un autre quart reste dynamique (6).

▪ Que l'attaque provienne d'une erreur, d'une négligence ou de procédés illicites, les enjeux sont devenus cruciaux : piratage des systèmes de traitement automatisé de données (STAD), perte d'informations confidentielles et stratégiques, vol de données personnelles, et lourds de conséquences sur le plan financier. A cet égard, l'entreprise victime devra vérifier sa police d'assurance pour vérifier si elle est couverte pour les risques informatiques.

▪ Aussi, dès la découverte d'une faille de sécurité, et préalablement à toute action contentieuse, plusieurs actions doivent rapidement être mises en œuvre.

▪ **Identification et correction de la faille.** En interne d'abord, il est recommandé au RSSI, au DSI, ou, le cas échéant, à la société d'expertise informatique, d'identifier la faille, de la corriger avant de mettre en place un audit de sécurité et de procéder aux mises à jour des procédures internes.

REFERENCES

(1) ENISA, rapport annuel 2020 sur les cybermenaces, 20-10-2020

(2) « Un rapport d'INTERPOL fait état d'un taux de cyberattaques très préoccupant durant le COVID-19 », 4-8-2020

(3) « Coronavirus : 18 millions de spams malveillants bloqués chaque jour par Google », 19-4-2020, www.lepoint.fr

(4) « Les entreprises françaises dans le déni : 1 entreprise sur 2 a mis en place une stratégie de cybersécurité », Communiqué de presse PwC, 2-10-2018

(5) Rapport Hiscox 2020 sur la gestion des cyber-risques https://www.hiscox.fr/courtage/sites/courtage/files/documents/2020_RAPPORT_CYBER_HISCOX.pdf

(6) « Cybersécurité : en difficulté, le CAC 40 réduit ses budgets », 6-7-2020, www.lesechos.fr

(7) art. 323-1 du Code pénal

(8) art. 323-1 du Code pénal

(9) art. 323-3 du Code pénal

(10) art. 323-3-1 du Code pénal, modifié par la loi n°2014-1353 du 13 novembre 2014, renforçant les dispositions relatives à la lutte contre le terrorisme

(11) art. 323-3-1 du Code pénal

(12) art. 323-4 du Code pénal

(13) art. 226-4-1 du Code pénal

(14) art. 312-1 à 312-9 du Code pénal

(15)

▪ **Constitution d'un dossier de preuve technique.** Parallèlement, il est vivement conseillé au RSSI, au DSI ou à la société d'expertise informatique, de réaliser un dossier de preuve technique, comprenant a minima un rapport d'incident et les logs de connexion aux serveurs.

▪ **Qualification juridique des faits.** A l'appui de ces éléments, il sera ensuite possible de qualifier juridiquement les faits et de les rattacher notamment à l'une ou plusieurs des infractions suivantes :

- accès frauduleux dans un STAD **(7)** ;
- maintien frauduleux dans un STAD **(8)** ;
- introduction frauduleuse de données dans un STAD **(9)** ;
- extraction, détention, reproduction ou transmission de données dans un STAD **(10)** ;
- détention de programmes informatiques conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions **(11)** ;
- association de malfaiteurs informatiques **(12)** ;
- usurpation d'identité numérique **(13)** ;
- extorsion de fonds **(14)**.

▪ **Dépôt de plainte.** Une plainte devra être déposée auprès du procureur de la République territorialement compétent, qui diligentera une enquête préliminaire confiée aux services de police ou de gendarmerie spécialisés que sont :

- la Brigade de lutte contre la cybercriminalité (BL2C, anciennement appelée Befti) **(15)**, service de la Police Judiciaire dévolu aux infractions informatiques sur la région parisienne ;
- la Sous-direction de lutte contre la cybercriminalité, qui relève de la Direction centrale de la police judiciaire (SDLC) **(16)**, compétente pour les attaques à l'encontre d'un système d'information situé à l'extérieur du périmètre d'intervention de la Befti ;
- l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) **(17)**, compétente sur tout le territoire français.

▪ Les violations de données personnelles doivent être notifiées par le responsable de traitement à l'autorité de contrôle nationale (la Cnil en France) **(18)**.

▪ **Plan média.** L'entreprise confrontée à une atteinte à son système informatique ayant conduit à une violation des données personnelles devra communiquer sur cet incident en interne et auprès de toutes personnes susceptibles de la solliciter (journalistes ou clients) et réagir très rapidement pour éviter toute diffusion d'information erronée ou inexacte, toute atteinte à sa réputation, ou encore mauvaise appréciation de l'impact de l'événement sur son activité économique.

▪ Si la répression des atteintes au système d'information a été largement renforcée par la loi 2014-1353 du 13 novembre 2014 **(19)** introduisant le délit d'extraction de données dans un STAD et par l'arrêt « Bluetouff » **(20)** de la Cour de cassation du 20 mai 2015 qui consacre le vol de données, la sécurisation du système d'information reste encore le meilleur moyen de lutter contre les failles de sécurité.

https://www.prefecturedepolice.interieur.gouv.fr/Cybersecurite/Les-actions-PP/Les-brigades-de-police-judiciaire/La-BEFTI
et
https://t.co/GLLfZa62tR?amp=1

(16) http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite

(17) http://www.police-nationale.interieur.gouv.fr/Actualites/L-actu-police/Plateforme-Signalement-sur-Internet/Decouvrez-l-OCLCTIC

(18) www.cnil.fr

(19) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000029754374/

(20) https://www.alain-bensoussan.com/wp-content/uploads/2015/06/31182452.pdf
V. aussi "Lexing Insights" # 7, « Accès et maintien frauduleux dans un STAD » (juin 2014) et notamment l'article de la France (p.10) avec un focus sur l'affaire "Bluetouff".

VIRGINIE BENSOUSSAN-BRULE

france@lexing.network

How to respond to a cyber attack or security breach?

▪ *Amid the increasing number and scale of cyber attacks, security breaches have become a major and unavoidable concern for organizations in France and in all countries around the world.*

▪ *Cyber attacks are constantly on the rise* ***(1)*** *and, because of the health crisis, a further increase in cybercrime is highly likely in the near future* ***(2)****. Google said it was blocking more than 18m coronavirus scam and phishing emails a day.* ***(3)***

▪ *However, according to the IPSOS survey for PwC on cybersecurity published in October 2018, French companies generally underestimate or even deny the risk of cybercrime. Indeed, only 1 out of 2 French companies had implemented a cybersecurity strategy and only 2 out of 10 companies said they were "fully capable" of managing a cyber attack* ***(4)****.*

▪ *At the same time, the financial consequences of cybercrime are exploding. A survey carried out by the insurer Hiscox in early 2020, before the coronavirus pandemic, among more than 5500 professionals, showed that in France the medium cost of cyber attacks was €35,000 compared to €9,000 in 2019, an increase of 290%. For large companies (+1000 employees), the average loss peaks at €458,000.* ***(5)***

▪ *Paradoxically, despite the increase in cyber attacks and in the cost attributed to cybersecurity incidents, nearly half of the largest French companies are preparing to stabilize their cybersecurity budgets, while for the other half, a quarter will reduce them and another quarter remains dynamic* ***(6)****.*

▪ *Whether the attack comes from an error, negligence or unlawful processes, the stakes are high — hacking of automated data processing systems, loss of confidential and strategic information, theft of personal data — and the financial consequences are serious. A first step for a company hit by a cyber attack will be to check its insurance policy to see if it is covered for IT risks.*

▪ *As soon as you discover a security breach, and prior to any legal action, you need to quickly take the following actions:*

▪ ***Identification and correction of the breach.*** *Internally, first of all, it is recommended that the CISO, the CIO, or, where applicable, the IT consulting firm, identify and correct the breach before implementing a security audit and updating internal procedures.*

▪ ***Creation of a technical evidence file.*** *At the same time, the CISO, the CIO or the IT consulting firm is strongly advised to compile a technical evidence file, including at least an incident report and server connection logs.*

REFERENCES

(1) ENISA, Threat Landscape 2020 report, 20-10-2020

(2) "INTERPOL report shows alarming rate of cyberattacks during COVID-19", 4-8-2020

(3) "Coronavirus : 18 millions de spams malveillants bloqués chaque jour par Google", 19-4-2020, www.lepoint.fr

(4) "Les entreprises françaises dans le déni : 1 entreprise sur 2 a mis en place une stratégie de cybersécurité", PwC press release, 2-10-2018

(5) Rapport Hiscox 2020 sur la gestion des cyber-risques https://www.hiscox.fr/courtage/sites/courtage/files/documents/2020_RAPPORT_CYBER_HISCOX.pdf

(6) "Cybersécurité : en difficulté, le CAC 40 réduit ses budgets", 6-7-2020, www.lesechos.fr

(7) Art. 323-1 of the Penal Code

(8) Art. 323-1 of the Penal Code

(9) Art. 323-3 of the Penal Code

(10) Art. 323-3 of the Penal Code, amended by law n°2014-1353 of 13 November 2014, reinforcing the provisions relating to the fight against terrorism

(11) Art. 323-3-1 of the Criminal Code

(12) Art. 323-4 of the Penal Code

(13) Art. 226-4-1 of the Penal Code

(14) Art. 312-1 to 312-9 of the Penal Code

(15)

▪ ***Legal qualification of the facts.*** *On the basis of these elements, it will then be possible to legally qualify the facts and link them to one or more of the following offences:*

- *fraudulently accessing an automated data processing system* ***(7)****;*
- *fraudulently remaining in an automated data processing system* ***(8)****;*
- *fraudulently introducing data into an automated data processing system* ***(9)****;*
- *retrieving, possessing, reproducing or transmitting data in an automated data processing system* ***(10)****;*
- *possessing computer programmes designed or specially adapted to commit one or more of the offences set out above* ***(11)****;*
- *participating in a group or conspiracy established with a view to the preparation of one or more offences of the set out above* ***(12)****;*
- *digital identity theft* ***(13)****;*
- *extortion* ***(14)****.*

▪ ***Filing a complaint.*** *A complaint must be lodged with the public prosecutor having territorial jurisdiction, who will entrust specialized police or gendarmerie services with carrying out a preliminary investigation:*

- *the Brigade for the Fight Against Cybercrime (BL2C, formerly known as Befti)* ***(15)****, a judicial police department dedicated to computer-related offences in the Paris region;*
- *the sub-Directorate for the Fight Against Cybercrime, which reports to the Central Directorate of the Judicial Police (SDLC)* ***(16)****, in charge of dealing with attacks against an information system located outside the Befti's remit;*
- *the Central Office for the Fight against Crime linked to Information and Communication Technologies (OCLCTIC)* ***(17)****, which has jurisdiction throughout France.*

▪ *Personal data breaches must be notified by the data controller to the national supervisory authority (in France, the CNIL)* ***(18)****.*

▪ ***Media plan.*** *An organization faced with an attack on its computer system that has led to a personal data breach will have to communicate on this incident internally and to all persons likely to ask information about it (journalists or clients) and must react very quickly to avoid the dissemination of any misleading or inaccurate information, any damage to its reputation, or a poor appreciation of the impact of such event on its business activity.*

▪ *Although the crackdown on attacks on information systems has been greatly reinforced both by Law 2014-1353 of 13 November 2014* ***(19)*** *introducing the offence of data retrieval in an automated data processing system and by the* Bluetouff *ruling* ***(20)*** *of the Court of Cassation of 20 May 2015, which establishes data theft, securing your information system is still the best way to fight against security breaches.*

https://www.prefecturedepolice.interieur.gouv.fr/Cybersecurite/Les-actions-PP/Les-brigades-de-police-judiciaire/La-BEFTI
and
https://t.co/GLLfZa62tR?amp=1

(16) http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite

(17) http://www.police-nationale.interieur.gouv.fr/Actualites/L-actu-police/Plateforme-Signalement-sur-Internet/Decouvrez-l-OCLCTIC

(18) www.cnil.fr

(19) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000029754374/

(20) https://www.alain-bensoussan.com/wp-content/uploads/2015/06/31182452.pdf
See also "Lexing Insights" # 7, "Unauthorized access to IT systems" (June 2014) and especially France's article (p.12), with focus on the "Bluetouff" case.

VIRGINIE BENSOUSSAN-BRULE

france
@lexing.network

Le cadre juridique grec de lutte contre la cybercriminalité

▪ L'arsenal juridique grec de lutte contre la cybercriminalité couvre la plupart des différentes formes de cybercriminalité, tels que le piratage, les attaques par déni de service (DoS), l'usurpation d'identité, l'utilisation de logiciels malveillants, ou encore l'hameçonnage (également connu sous le nom de « phishing »).

▪ Plus spécifiquement, le code pénal réprime la fraude et les abus informatiques, tels que l'accès frauduleux aux systèmes d'information, l'atteinte illégale à l'intégrité des systèmes ou l'atteinte illégale à l'intégrité des données.

▪ Les lois sur les télécommunications réglementent, quant à elles, l'interception illégale de transmissions non publiques de données à destination, en provenance ou à l'intérieur d'un système d'information. Les textes applicables en matière de vie privée en ligne interdisent également d'intercepter les communications (lors de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics), les données relatives au trafic et les données de localisation en dehors des cas autorisés par la loi (c'est-à-dire pour des raisons de sécurité nationale ou d'enquête sur certains crimes).

▪ Par ailleurs, la Grèce a ratifié la Convention sur la cybercriminalité du Conseil de l'Europe, également connue sous le nom de Convention de Budapest **(1)**. Cette convention fournit un cadre juridique pour la lutte contre les infractions commises via internet ou d'autres réseaux informatiques, et en particulier des infractions liées à la sécurité des réseaux. Elle organise également la coopération internationale et l'entraide des parties aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

(1) Loi 4411/2016

▪ En outre, la loi grecque 2121/1993 sur la propriété intellectuelle comprend des dispositions contre le contournement des MTP, c'est-à-dire les mesures techniques de protection qui empêchent ou limitent l'accès aux œuvres ou la copie de celles-ci. En effet, la fourniture d'un service destiné à permettre ou à faciliter le contournement des MTP est prohibée par la loi 2121/1993.

▪ Enfin, la loi 4624/2019 sur la protection des données à caractère personnel, qui a introduit dans le droit grec des mesures supplémentaires pour l'application du RGPD, inclut des sanctions pénales en cas notamment d'atteinte à un fichier de données à caractère personnel, ainsi qu'en cas de traitement illégal de données personnelles (par transmission, accès, etc.).

Cybersécurité

▪ Premier texte législatif européen sur la cybersécurité, la directive NIS (2) a été transposée par la Grèce dans son droit national par la loi 4577/2018. Ce texte a introduit des mesures visant à atteindre un niveau élevé de sécurité des réseaux et des systèmes d'information et s'applique aux opérateurs de services essentiels (c'est-à-dire les entités qui fournissent des services dans les secteurs de l'énergie, des transports, de la banque, de la santé, etc.) et aux fournisseurs de service numérique (places de marché en ligne, moteurs de recherche en ligne et services d'informatique en nuage).

(2) Directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information

▪ S'agissant des fournisseurs de réseaux de communication publics ou de services de communications électroniques accessibles au public, il convient également de noter la décision 205/2013 de l'autorité hellénique pour la sécurité et la protection des communications (ADAE), telle que modifiée par la décision 99/2017 de l'ADAE (3) et l'acte conjoint 1/2013 de l'ADAE et de l'autorité hellénique de protection des données.

(3) « Règlement pour la sécurité et l'intégrité des réseaux et des services de communications électroniques »

▪ La décision 205/2013 définit les mesures techniques et organisationnelles qui doivent être mises en œuvre par ces fournisseurs afin de garantir la sécurité des données (analyse d'impact, continuité des activités, tests de pénétration, évaluations de la vulnérabilité, sécurité physique, sauvegardes, contrôles d'accès logique, pare-feu, VPN, systèmes de détection d'intrusion, gestion des incidents de sécurité, etc.).

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

Existing regulation

▪ *Greek legal framework covers most cybercrime activity, including hacking, Denial-of-Service (DoS) attacks, identity theft, use of malware, phishing, etc.*

▪ *More specifically, computer fraud and misuse laws (most importantly, penal code provisions) cover most cases of computer fraud, illegal access to information systems, illegal system interference and illegal data interference.*

▪ *There are also telecommunication laws in place which regulate illegal interception of non-public transmissions of data to, from or within an information system; furthermore, under applicable e-privacy laws, interception of communications (in connection with the provision of publicly available electronic communications services in public communications networks) and relevant traffic and location data is unlawful, unless otherwise provided by law (i.e. for reasons of national security and investigation of certain felonies).*

▪ *Notably, Greece has ratified the Convention on Cybercrime by the Council of Europe, also known as the Budapest Convention* ***(1)****. The said Convention regulates crimes committed via the Internet and other computer networks, dealing, among other issues, with violations of network security and also with matters of international co-operation and mutual assistance between the parties for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.*

(1) Law 4411/2016

▪ *Moreover, Greek Intellectual Property Law 2121/1993 includes provisions against illegal circumvention of technological protection measures (TPM) which prevent access to, or the copying of, works; the provision of a service the purpose of which is to enable or facilitate the circumvention of TPM is also prohibited under Greek Intellectual Property Law 2121/1993.*

▪ *Law 4624/2019, which has introduced supplemental measures for the application of the GDPR, includes certain criminal sanctions in cases of interference with personal data filing system; also in case of illegal processing of personal data, including, inter alia, illegal transmission and illegal access.*

Cybersecurity

▪ *Greece has, by virtue of Law 4577/2018, transposed NIS Directive* ***(2)****, the first piece of EU-wide legislation on cybersecurity. Law 4577/2018 has introduced measures with a view to achieving a high level of security of network and information systems and applies to Operators of Essential Services (i.e. entities in the sectors of energy, transport, banking, health, etc.) and to Digital Service*

(2) Directive (EU) 2016/1148 on security of network and information systems

Providers (i.e. online marketplaces, online search engines, and cloud computing services).

▪ *In the same context and with regard to providers of public communication networks or public electronic communication services relevant is also the Decision 205/2013 issued by the Hellenic Authority for Communication Security and Privacy (ADAE), as amended by ADAE Decision 99/2017* ***(3)*** *and the Joint Act 1/2013 issued by the ADAE and the Hellenic Data Protection Authority.*

▪ *Decision 205/2013 defines the technical and organizational measures that need to be implemented by the said providers in order to ensure data security (including, for instance, business impact analysis, business continuity, penetration tests, vulnerability assessments, physical security, backups, logical access controls, firewalls, VPNs, intrusion detection systems, security incident management, etc.).*

(3) "Regulation for the Safety and Integrity of Networks and Electronic Communications Services"

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

ROYAUME-UNI

PREISKEL & CO LLP

Dans cet article, nous nous interrogeons sur la légalité, au Royaume-Uni, de ce qui est communément appelé « piratage éthique » ou « piratage légal » et qui consiste notamment, pour une entreprise de cybersécurité, à identifier des vulnérabilités informatiques susceptibles de mettre le public en danger.

▪ **Remarques préliminaires.** Deux remarques préliminaires :

- En l'espèce, le droit applicable se divise en deux branches : le droit pénal et le droit civil. Le droit pénal prévoit les comportements contraires à la loi (infractions) et les sanctions qui leur sont applicables. L'objectif d'une entreprise de cybersécurité sera d'éliminer tout risque d'action en responsabilité pénale. Le droit civil prévoit, quant à lui, les circonstances dans lesquelles une personne peut poursuivre ou être poursuivie en justice pour obtenir réparation d'un préjudice. L'objectif d'une entreprise de cybersécurité sera d'éviter autant que possible le risque d'action en responsabilité civile, et le cas échéant, si cette responsabilité ne peut être complètement éliminée, d'appliquer une approche fondée sur les risques.
- La loi ne prévoit pas de cadre spécifique pour le piratage éthique. En effet, il n'existe pas de loi qui s'y applique expressément. Il sera donc nécessaire d'y appliquer des lois qui n'envisageaient peut-être pas le piratage éthique au moment de leur promulgation et d'argumenter par analogie.

▪ Dans ce contexte, et au vu des éléments présentés ci-dessous, le piratage éthique à des fins commerciales peut être possible, mais cette activité comporte des risques juridiques très sérieux. Ces risques sont principalement l'engagement de poursuites judiciaires et le prononcé de condamnations (notamment à des peines d'emprisonnement) à l'encontre non seulement des pirates éthiques, mais également des dirigeants et des sociétés liées à ces derniers. En substance, ce type de piratage ne doit pas être réalisé à la légère.

▪ Le texte de référence au Royaume-Uni est la loi de 1990 sur l'utilisation abusive de l'informatique (Computer Misuse Act 1990, CMA), qui prévoit trois infractions pertinentes à cet égard :

- (a) l'accès non autorisé au matériel informatique ;
- (b) l'accès non autorisé avec l'intention de commettre ou de faciliter la commission d'autres infractions ;
- (c) les actes non autorisés commis intentionnellement ou par imprudence en vue de nuire au fonctionnement d'un ordinateur, etc.

▪ Ces infractions s'articulent autour de trois notions clés, que sont « ordinateur » **(1)**, « accès » **(2)** et « non autorisé » **(3)**.

▪ **Infractions plus graves.** Les infractions les plus graves requièrent du pirate l'intention (a) de commettre ou de faciliter la commission d'autres infractions ou (b) de compromettre, intentionnellement ou par imprudence, le fonctionnement d'un ordinateur ou d'autres dispositifs.

▪ Ainsi, un piratage informatique associé à une demande de paiement en échange d'explications sur les méthodes utilisées par le pirate pour mener à bien le piratage

REFERENCES

(1) « Ordinateur » : La loi CMA ne définit pas le terme « ordinateur ». Sa définition juridique usuelle est issue d'une affaire de la Chambre des Lords, dans laquelle un ordinateur a été décrit comme « un dispositif de stockage, de traitement et d'extraction d'informations ». Cette définition est large et peut inclure des dispositifs non électroniques et des systèmes électriques fermés (par exemple, un robot aspirateur équipé d'un microprocesseur). Selon nous, « ordinateur » s'entend de tout dispositif (électronique) capable de suivre un programme (ainsi que le programme lui-même). Cela étant, les infractions protègent généralement le matériel informatique en réseau, notamment en ce qui concerne l'accès, via un réseau public, à un réseau local/fermé.

(2) « Accès » : Ce terme désigne généralement l'accès aux programmes et aux données d'un ordinateur (plutôt que, par exemple, le démontage physique d'un ordinateur). Cet accès peut être commis par une personne interne ou une personne externe.
Selon nous, l'accès ne peut pas inclure le test d'un ordinateur afin d'évaluer son efficacité : il s'agirait dans ce cas de faire fonctionner un programme ou un ordinateur, et non d'accéder au matériel qu'il renferme.

(3) « Non autorisé » : La permission ou l'autorisation fait échec à l'infraction. L'infraction exige également que le contrevenant soit conscient, au moment de l'accès, de ne pas bénéficier

pourrait constituer l'infraction de chantage. Il s'agirait, en effet, d'un piratage visant à commettre ou à faciliter la commission d'autres infractions.

d'une autorisation. L'autorisation doit par conséquent être donnée préalablement à l'accès.

▪ **Etendue du risque.** On ne pas peut échapper à la responsabilité pénale en sous-traitant à un tiers la réalisation d'actes de piratage. En effet, le droit pénal est d'application large et le donneur d'ordre, qui se pense à l'abri, peut tout à fait se voir accusé de complicité. Le droit pénal assimile le complice à un auteur : le complice sera donc puni comme auteur de l'infraction. Pour les entreprises, il n'existe donc pas de manière simple d'aménager sa responsabilité en matière de piratage. Prenons l'exemple d'un cas analogue : le scandale des écoutes téléphoniques qui a eu lieu au Royaume-Uni. Dans cette affaire, des accusations ont été portées contre des cadres supérieurs et des dirigeants de l'organisme concerné, quand bien même les piratages téléphoniques litigieux avaient été effectués par du personnel extérieur à cet organisme.

▪ Ne pas oublier que sont concernées aussi bien les personnes physiques que les personnes morales. Une entreprise peut dès lors être faire l'objet d'une condamnation pénale.

▪ **Seuil de tolérance bas et absence d'intention délictueuse.** L'affaire Daniel Cuthbert **(4)** montre à quel point le seuil de déclenchement de la responsabilité peut être bas, puisque le moindre accès non autorisé (même avec une intention innocente) peut aboutir à une condamnation.

(4) https://www.theregister.co.uk/2005/10/06/tsunami_hacker_convicted/

▪ **Moyen de défense.** L'intérêt général ne peut être invoqué comme moyen de défense. Le ministère public peut refuser d'engager des poursuites dans l'intérêt public, mais cela reste exceptionnel.

▪ **Conseils pratiques généraux.** En bref, pour éviter toute accusation de piratage, aussi bien à l'encontre d'une personne physique que d'une personne morale, les pirates éthiques sont invités à s'assurer :

- a) que l'accès ne se fait pas à un « ordinateur » ;
- b) que l'accès est autorisé ; et/ou
- c) qu'il n'y ait pas d'« accès » à du matériel informatique qui ne soit pas la propriété du pirate.

▪ **Conseils pratiques concernant l'accès aux ordinateurs.** Selon nous, l'accès à une unité fermée qui possède un petit processeur ne donnerait probablement pas lieu à infraction, car seul le processeur peut être couvert par la définition d'« ordinateur ». Si une personne ne fait que « tester » une unité, cette action pourrait, sous réserve bien entendu d'une analyse plus approfondie, ne pas être qualifiée d'« accès » au sens de la loi. A notre avis, utiliser un appareil conformément à sa destination ne peut constituer une infraction.

▪ **Conseils pratiques concernant l'autorisation.** La meilleure manière procéder est d'obtenir une autorisation avant d'accéder à un matériel appartenant à une autre personne, ce qui est d'ailleurs généralement le cas des pirates informatiques éthiques (les fameux « white hat »). Si vous accédez à une unité fermée vous appartenant intégralement (par exemple, vous démontez son propre robot aspirateur), vous ne sera probablement pas susceptible de tomber sous le coup d'une infraction. En effet, une personne propriétaire d'un objet peut « s'auto-autoriser » un tel accès.

DANIEL PREISKEL

uk@lexing.network

In this article, we consider whether it is lawful for a cybersecurity company to conduct what is commonly known as "Ethical Hacking" to expose IT vulnerabilities that could put the public at risk.

▪ ***Preliminary points.*** *We need to make two preliminary points.*

- *First, one must note there are two types of applicable law: the criminal law and the civil law. The criminal law provides for offences and punishments, and the aim should be for a cybersecurity company to eliminate any exposure to criminal liability. The civil law instead provides for the circumstances where a party may sue or be sued, and the aim should be to manage exposure to liability, on a risk-based approach if it cannot be eliminated completely.*
- *Second, the law does not offer an exact fit for ethical hacking. There is no law which expressly applies. We thereby have to have apply laws which may not have envisaged ethical hacking when the law was enacted and argue by analogy.*

▪ *On the basis of our reasoning below, we would say that ethical hacking on a commercial basis may be possible, but there are also very serious legal risks. These risks include the prosecution and convictions of not only those who commit the hacks but also directors and related companies, and possible imprisonment of directors. In essence, hacking should not be done lightly.*

▪ *The starting point is the Computer Misuse Act 1990 (CMA), where there are three relevant offences:*

- *(a) unauthorised access to computer material (the section 1 offence);*
- *(b) unauthorised access with intent to commit or facilitate commission of further offences;*
- *(c) unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.*

▪ *These offences require an understanding of three key terms. These are, in logical order: computer* ***(1)****, access* ***(2)****, and unauthorised* ***(3)****.*

▪ ***More serious offences.*** *The more serious offences require that person to have further intent: (a) to commit or facilitate commission of further offences or (b) to impair, or with recklessness as to impairing, operation of computer, etc.*

▪ *For example, a computer hack tied to a demand for payment for showing how it was done could amount to an offence of blackmail. That would be a hack to commit or facilitate commission of further offences.*

▪ ***Extent of exposure.*** *One cannot easily "contract out" of criminal offences by contracting with a third person to do the hacking. The criminal law has a wide net and the offences of "aiding and abetting" offences can catch people who think they have distanced themselves. The application of standard principles of criminal law*

(1) Computer": The CMA does not define "computer". The working legal definition is instead from a House of Lords case, where a computer was defined as "a device for storing, processing and retrieving information.". As you will appreciate that is a wide definition and could include non-electronic devices, and closed electrical systems (such as, say, a robot vacuum cleaner which happens to have a small chip-processor).
In our view, the definition of "computer" should be taken to mean any (electronic) device capable of following a program (as well as the program itself). That said, the offences usually protect networked computer material, especially in respect of access via a public network into a local/closed network.

(2) "Access": This usually means accessing the programs and data of a computer (rather than, say, taking a computer apart physically). This can be both an external party or an internal party accessing a system.
In our view this cannot include testing a computer so as to assess its efficacy. That would be running a program or computer, not accessing material within it.

(3) "Unauthorised": Permission or authorisation defeats the offence. The offence also requires the defendant to be aware at the time that they are unauthorised. The authorisation thereby has to be prior authorisation.

mean that anyone aiding or conspiring can also commit the offence. There is no easy corporate way of structuring things – in the analogous phone hacking cases, charges were brought against senior managers and executives even though the hacks were done by external operatives.

- *A person can mean a company, and so a company can end up with a criminal conviction.*
- ***Low threshold and lack of wrongful intention.*** *How low that threshold can be can be shown with the example of Daniel Cuthbert* ***(4)*** *where only the slightest unauthorised access (with innocent intent) resulted in a conviction.*
- ***No public interest defence.*** *There is no public interest defence. The Crown Prosecution Service may decline to prosecute in the public interest, but that is exceptional and cannot be relied upon.*
- ***General practical advice.*** *In simple terms, the way to ensure a person or company is not caught by the offence is to ensure:*
  - *(a) that the access is not to a "computer";*
  - *(b) that the access is authorised; and/or*
  - *(c) there is no "accessing" any computer material which is not owned by the hacker.*
- ***Practical advice – computer and accessing.*** *So we would view accessing (say) any closed unit which happens to have a small chip-processor would presumably not be an offence, as only the chip-processor may be within the definition of "computer". If a person was merely "testing" a unit, it may well be that would not be seen as "accessing" it for the purposes of the law, but we would want to know more about this before proceeding. But using a device for how it was intended cannot be an offence in our view.*
- ***Practical advice – authorization.*** *The safest way to proceed is to get authorisation before accessing something belonging to another. That is, of course, what "white hat" and "ethical" hackers usually do. Accessing any closed unit owned entirely by the person accessing it is likely to be outside the offence. This is because a person can "authorise" itself if it owns an item. For example taking one's own robot vacuum cleaner apart.*

(4) *https://www.theregister.co.uk/2005/10/06/tsunami_hacker_convicted/*

DANIEL PREISKEL

uk@lexing.network

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne *Germany*	Beiten Burkhardt	Andreas Lober	+49 69 756095-0	germany@lexing.network
Australie *Australia*	Gadens	Dudley Kneller	+61 438 363 443	australia@lexing.network
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Jean-François De Rico	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Costa Rica *Costa Rica*	Lexing Costa Rica	Gabriel Lizama	+506 2253-1726	costa-rica@lexing.network
Côte d'Ivoire *Ivory Coast*	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
États-Unis *USA*	DataMinding Legal Services	Françoise Gilbert	+1 650-804-1235	usa@lexing.network
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Guinée *Guinea*	BAO & Fils	Mody Oumar Barry	+ 224 623 68 78 79	guinea@lexing.network
Hongrie *Hungary*	OPL - Orbán & Perlaki	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde *India*	Poovayya and Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Israël *Israel*	Appelfeld & Co	Ilanit Appelfeld	+ 972 3 60 98 099	israel@lexing.network
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Maroc *Morocco*	Elkhatib Lawfirm	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Arve Føyen	+47 21 93 10 00	norway@lexing.network
Nouvelle-Calédonie *New Caledonia*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	nc@lexing.network
République tchèque *Czech Republic*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	czechrepublic@lexing.network
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Sénégal *Senegal*	SCP Faye & Diallo	Mamadou Seye	:(+221) 33 823 60 60	senegal@lexing.network
Slovaquie *Slovakia*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	slovakia@lexing.network
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network

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/