n°31 Janvier 2022
#31 January 2022

Lexing Insights

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

LE CADRE JURIDIQUE DES OUTILS DE CHIFFREMENT

LEGAL FRAMEWORK FOR ENCRYPTION TOOLS

LE CHIFFREMENT : UN OUTIL DE SECURISATION DES DONNEES

▪ D'abord réservée aux usages militaires et diplomatiques, la cryptologie fait partie intégrante de notre quotidien depuis l'avènement d'Internet. Cette science du secret, qui se divise en deux branches (cryptographie et cryptanalyse) est en effet aujourd'hui incontournable pour assurer la sécurité des systèmes d'information. Ainsi, le chiffrement, qui est un procédé cryptographique permettant de garantir la confidentialité d'une information, sert notamment, aux termes du RGPD, à atténuer les risques inhérents au traitement de données à caractère personnel.

▪ Les moyens de cryptologie peuvent faire l'objet de restrictions selon les pays. En France, conformément à la LCEN, l'usage d'outils de chiffrement est libre, mais leur importation et exportation sont soumis à déclaration ou à demande d'autorisation auprès de l'Anssi.

▪ Qu'est-ce que le chiffrement et pourquoi l'utiliser ? Quelles sont les conditions à respecter pour utiliser ou exporter/importer un logiciel de chiffrement ? Les fournisseurs de logiciels de chiffrement ont-ils l'obligation d'intégrer des *backdoors* ? Qu'est-ce qu'un bien à double usage ? Quelle est la position des autorités de protection des données à l'égard du chiffrement ?

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, Belgique, Chine, Espagne, France, Grèce, Luxembourg.

ENCRYPTION: A TOOL TO SECURE YOUR DATA

▪ *Initially used by military leaders and diplomats, cryptology has become an integral part of our daily lives since the advent of the Internet. This science of secret writing, which is divided into two types (cryptography and cryptanalysis), is today essential for the security of information systems. Under the terms of the GDPR, encryption, which is a cryptographic process that makes it possible to guarantee the confidentiality of information, is a way to mitigate the risks inherent in the processing of personal data.*

▪ *Cryptology tools may be subject to restrictions depending on the country. In France, in accordance with the LCEN Act, the use of encryption tools is free, but their import and export are subject to declaration with or authorization from the ANSSI.*

▪ *What is encryption and why use it? What are the requirements for using or exporting/importing encryption software? Are encryption software providers required to build backdoors? What is a dual-use item? What is the position of data protection authorities with regard to encryption?*

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

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

ANTHONY SITBON
Directeur du département Sécurité du cabinet
Lexing Alain Bensoussan-Avocats

Head of the Security department of Lexing Alain Bensoussan-Avocats

Cadre légal du chiffrement ou de la cryptographie en Afrique du Sud

▪ Le législateur sud-africain encadre le chiffrement et la cryptographie sans en interdire l'utilisation. Ainsi, les fournisseurs de services de chiffrement sont tenus de s'enregistrer auprès des autorités publiques, contrairement aux simples utilisateurs, qui sont dispensés de toute formalité. En outre, si à instar d'autres pays, tels que l'Australie, l'Afrique du Sud est dotée d'une loi anti-chiffrement, elle ne dispose pas de lois encadrant l'exportation des outils de chiffrement. Le présent article dresse un inventaire des lois sud-africaines pertinentes en la matière et décrit les modalités d'enregistrement à respecter par les fournisseurs.

Qu'est-ce que la cryptographie ?

▪ Wikipédia **(1)** définit la cryptographie comme « *la pratique et l'étude de la dissimulation d'informations* ». Le chiffrement d'un document ou d'une communication sert notamment à :

- établir son authenticité ;
- empêcher sa modification sans détection ;
- empêcher sa répudiation ; et
- empêcher son utilisation sans autorisation.

(1) https://en.wikipedia.org/wiki/Cryptography

Existe-t-il une loi sur la cryptographie ou le chiffrement en Afrique du Sud ?

▪ Historiquement, ce sont les militaires qui ont d'abord utilisé (et contrôlé) le matériel et les logiciels de chiffrement. De nos jours, les logiciels de chiffrement sont facilement disponibles sur Internet (souvent sous forme de logiciel gratuit (*freeware*) ou de logiciel à contribution (*shareware*)) et il est très difficile pour les gouvernements de décrypter un document ou une communication sans avoir accès à la clé privée de l'utilisateur.

▪ Plusieurs lois sud-africaines contiennent des dispositions relatives à la cryptographie, et notamment les lois suivantes :

- *Armaments Development and Production Act of 1968* (pour ce qui concerne les logiciels militaires) ;
- *Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002* (loi RICA) **(2)** ;
- *Electronic Communications and Transact*ions Act of2002 (loi ECT) **(3)**.

(2) http://www.internet.org.za/ricpci.html

(3) http://www.internet.org.za/ect_act.html

▪ C'est l'autorité indépendante des communications d'Afrique du Sud (ICASA) **(4)** qui est chargée de réglementer l'utilisation du chiffrement dans le secteur des télécommunications.

(4) http://www.icasa.org.za/

La loi sur le développement et la production d'armements de 1968

▪ Il n'existe aucun contrôle sur l'exportation, l'importation, le téléchargement et l'utilisation des logiciels de chiffrement « privés » en Afrique du Sud et il n'est pas nécessaire d'obtenir une autorisation pour les utiliser. Le terme « privé » fait référence à l'utilisation publique, par opposition à l'utilisation militaire, et le public est donc libre d'utiliser des logiciels de chiffrement.

▪ Le seul cas où une autorisation ou une licence serait nécessaire est celui où le logiciel est utilisé à des fins militaires ou provient d'un fournisseur militaire (c'est-à-dire une entité qui a développé la technologie spécifiquement pour la vendre aux gouvernements). Dans ce cas, la loi *Armaments Development and Production Act*

trouverait à s'appliquer, conformément aux dispositions du *General Armaments Control Schedule*.

La loi ECT : une loi sur le chiffrement

- Le **chapitre 5 de la loi ECT (5)** impose aux fournisseurs (et non aux utilisateurs) de services ou de produits de « cryptographie » d'enregistrer leurs noms et adresses, ainsi que les noms de leurs produits avec une brève description de ceux-ci, dans un **registre** tenu par le Département des communications et des technologies numériques (DoC) **(6) (7)**. A défaut, le fournisseur (local ou étranger) n'est pas autorisé à fournir ses produits ou services en Afrique du Sud et s'expose à des sanctions pénales (amende d'un montant non spécifié ou peine de prison d'une durée maximale de deux ans).
- Cet enregistrement a pour but de permet aux autorités chargées des enquêtes (telles que la police nationale sud-africaine, la SAPS) d'identifier les fournisseurs des technologies de chiffrement qu'elles pourraient être amenées à intercepter en vertu de la loi RICA (cf. ci-dessous). Le cas échéant, les autorités pourront ainsi se rapprocher de ces fournisseurs et obtenir leur aide pour déchiffrer les messages.
- Le chapitre 5 de la loi ECT (qui fait en quelque sorte office de loi sur la cryptographie) est considéré comme l'une des dispositions les plus controversées de cette loi. En effet, si de nombreux commentateurs comprennent la préoccupation du gouvernement quant aux conséquences que l'utilisation généralisée de la cryptographie pourrait avoir en limitant la capacité des services d'enquête à comprendre les données auxquelles ils ont légalement accès, ils font valoir que les dispositions dudit chapitre 5 ne sont pas conformes aux meilleures pratiques internationales et qu'elles ne répondent pas de manière efficace aux problèmes de sécurité.
- Beaucoup affirment également que ce chapitre n'est pas formulé de manière claire, qu'il pose plus de questions qu'il n'apporte de réponses et qu'il laisse beaucoup d'acteurs dans l'incertitude quant l'obligation ou non de s'enregistrer en tant que fournisseur de cryptographie **(8)**.

La loi RICA : une loi anti-chiffrement

- Les enquêtes sur les infractions pénales sont souvent entravées par la découverte que des documents qui pourraient aider les enquêteurs ou être utilisés à titre de preuves sont chiffrés. Les forces de l'ordre essaient souvent de les décrypter en « cassant » la clé de chiffrement. S'ils peuvent parfois y arriver, au prix d'efforts et de dépenses considérables, il est probable que cela devienne de plus en plus difficile, voire impossible, à mesure que les technologies évoluent.
- La loi RICA contient des dispositions qui permettent aux services répressifs, de sécurité et de renseignement de lutter contre la criminalité et les menaces pour la sécurité nationale. Ce texte leur donne la possibilité de s'adresser à un juge pour obtenir une « **ordonnance de déchiffrement** » **(9)** enjoignant au détenteur d'une clé de chiffrement de divulguer ladite clé ou de fournir son assistance pour décrypter des informations chiffrées. Les services répressifs devraient (en théorie) être en mesure d'identifier le détenteur de la clé dès lors que ses coordonnées (en tant que fournisseur de logiciels de cryptologie) ont été inscrites dans le registre des fournisseurs de services de cryptographie du DoC visé ci-dessus **(10)** en vertu de la loi ECT. En pratique, cependant, le fournisseur ne sera pas en mesure, dans de nombreux cas, de fournir l'identité de l'utilisateur du logiciel de cryptologie.

(5) Michalsons, Guide to the ECT Act in South Africa | ECTAv

(6) https://www.dcdt.gov.za/

(7) En savoir plus sur les services d'enregistrement de Michalsons : Cryptography provider registration services | Get registered
Pour obtenir un devis de Michalsons pour vous enregistrer auprès du DoC en tant que fournisseur de cryptologie, vous pouvez remplir ce questionnaire en ligne : https://docs.google.com/forms/d/e/1FAIpQLSexlZdqgpAEFK7RIonyeoYyujXoyYD7EtbVpcp6x8B3zGPQBQ/viewform?formkey=dDNXR0FlZ0NSSGp2OVpLMU03Tzd4UUE6MA#gid=0

(8) Michalsons, Do you need to register as a Cryptography Provider?

(9) https://www.internet.org.za/ricpci.html#ch3_21_3

(10) https://www.dcdt.gov.za/

JOHN GILES

south-africa@lexing.network

Encryption law or cryptography law in South Africa

▪ *There is some encryption law or cryptography law in South Africa. None prohibit its use but cryptography providers or suppliers need to register with the Government. Users of crypto products don't need to register. South Africa has a kind of anti-encryption lawlike some other countries (for example Australia). South Africa doesn't have encryption export laws. In this article, we look at the relevant laws and help providers to get registered.*

What is cryptography?

▪ *Wikipedia* ***(1)*** *defines "cryptography" as "the practice and study of hiding information". Where a document or communication has been encrypted, the act of encrypting serves several purposes. To:*

- *establish its authenticity;*
- *prevent its undetected modification;*
- *prevent its repudiation and;*
- *prevent its unauthorized use.*

Is there cryptography law or encryption law in South Africa?

▪ *Historically, it has been the military who have used (and controlled) encryption hardware and software. Nowadays encryption software is readily available on the Internet (often as freeware or shareware) and it is very difficult for governments to decrypt the document or communication without access to the users private key.*

▪ *There are a few laws that deal with crypto in one way or another, including the:*

- *Armaments Development and Production Act of 1968 (for military software);*
- *Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002 (RICA)* ***(2)****;*
- *Electronic Communications and Transactions Act of 2002 (ECT Act)* ***(3)****.*

▪ *The Independent Communications Authority of South Africa (ICASA)* ***(4)*** *regulates the use of encryption over telecommunications facilities.*

Armaments Development and Production Act

▪ *There are no "domestic" controls on the export, import, downloading and use of encryption software in South Africa and one does not need a permit to use it. "Domestic" refers to the public's freedom to use encryption software (as distinct from military use).*

▪ *The only time a permit or licence is required is where the product is used for military purposes, or comes from a military supplier (an entity that has developed the technology specifically for sale to governments). This is in terms of the General Armaments Control Schedule of the Armaments Development and Production Act of 1968.*

(1) https://en.wikipedia.org/wiki/Cryptography

(2) http://www.internet.org.za/ricpci.html

(3) http://www.internet.org.za/ect_act.html

(4) http://www.icasa.org.za/

The ECT Act is partly an encryption law

▪ ***Chapter 5 of the ECT Act (5)*** *requires suppliers (not users) of "cryptography" services or products to register their names and addresses, the names of their products with a brief description in a* ***register*** *maintained by the Department of Communications and Digital Technologies* ***(6)*** ***(7)****. Unless the (local or foreign) supplier has registered, they cannot provide their services or products in South Africa. In addition, failure to record the particulars in the register is a criminal offence (an unspecified fine or imprisonment for a maximum period of two years).*

▪ *Registration will allow investigative authorities (such as the SAPS) to identify which organisation provided the encryption technologies intercepted by them in terms of RICA (see below). This will enable the investigative authorities to approach these service providers to assist with deciphering the encrypted messages.*

▪ *Chapter 5 (a kind of cryptography law) is regarded as being one of the most contentious chapters of the ECT Act. Whilst many commentators appreciate the Government's concern about the implications that the widespread use of cryptography may have for law enforcement in limiting the ability of the investigative authorities to understand lawfully accessed data, they argue that the provisions of the chapter do not accord with international best practice, nor do they meaningfully address security concerns.*

▪ *Many also contend that the chapter is not clear, poses more questions than anything else and leaves many uncertain whether to register as a cryptography provider or not* ***(8)****.*

Monitoring law (RICA) is a kind of anti-encryption law

▪ *Investigations into criminal offences are often hampered by the discovery that material that might otherwise assist the investigation, or be used in evidence, has been encrypted. Law enforcement agencies often try to "crack" the encryption key. Although this is occasionally possible after considerable effort and expense, it is likely to become increasingly difficult – if not impossible – as technology develops.*

▪ *RICA contains provisions that enable law enforcement, security and intelligence agencies to fight crime and threats to national security. In terms of the legislation, one has to apply to a Judge for a "****decryption direction****"* ***(9)*** *in terms of which the holder of an encryption key is directed to disclose that key or provide decryption assistance in respect of encrypted information. Law enforcement should (in theory) be able to identify the holder of the key if their details (as a supplier of crypto software) have been entered in the Department of Communications and Digital Technologies* ***(10)****'s register of crypto suppliers. This is the link with the crypto registration provisions in the ECT Act. In many instances in practice, however, the supplier will not be able to provide the identity of the user of the crypto software.*

(5) Michalsons, Guide to the ECT Act in South Africa | ECTAv

(6) https://www.dcdt.gov.za/

(7) Read more about Michalsons' cryptography provider registration services: Cryptography provider registration services | Get registered
To be provided with a Michalsons quote for you to register with the DoC as a crypto provider, please complete this online questionnaire https://docs.google.com/forms/d/e/1FAIpQLSexlZdggpAEFK7RIonyeoYyujXoyYD7EtbVpcp6x8B3zGPQBQ/viewform?formkey=dDNXR0FlZ0NSSGp2OVpLMU03Tzd4UUE6MA#gid=0

(8) Michalsons, Do you need to register as a Cryptography Provider?

(9) https://www.internet.org.za/ricpci.html#ch3_21_3

(10) https://www.dcdt.gov.za/

JOHN GILES

south-africa@lexing.network

Encadrement des logiciels de cryptographie

Contexte législatif

▪ Les premiers textes obligeant les opérateurs de télécoms belges à faire agréer leurs terminaux par l'Institut belge de postes et télécommunications (IBPT) en vue de s'assurer de la possibilité de mettre en œuvre les moyens d'écoute de l'époque étaient perdus dans les centaines de pages d'une indigeste loi-programme de 1994. Les textes récents sont un peu plus visibles, à défaut d'être toujours lisibles.

▪ La **loi du 13 juin 2005** relative aux communications électroniques définit la cryptographie comme « *l'ensemble des services mettant en œuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée* ». Conformément à l'article 48 de la même loi, l'usage de la cryptographie est libre en Belgique. La fourniture au public de services de cryptographie est soumise à une déclaration préalable auprès de l'IBPT.

▪ Malgré cette liberté, le gouvernement souhaite préserver les intérêts des enquêtes pénales et de ses services secrets. En ce sens, l'**article 88 quater du Code d'instruction criminelle** envisage d'ailleurs l'atteinte à l'intégrité des données dans le cadre d'une instruction. En effet, il n'est pas souhaitable que l'usage du chiffrement contrevienne à la poursuite des actes criminels tant au niveau national qu'européen **(1)**.

▪ Dans cette même perspective, la cryptographie présente des intérêts tant pour l'usage civil que militaire, étant considérée comme un système assurant la « sécurité de l'information ». À ce titre, elle est couverte par le Règlement instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage et du transit de **biens à double usage (2)**.

Controverse

▪ Un **projet de loi belge** fait l'objet d'une vive controverse actuellement, en ce qu'il obligerait les opérateurs à permettre le déchiffrage de ces données à la demande de certains utilisateurs tels que la police dans le but de faciliter les enquêtes. Il s'agit, ni plus ni moins, de forcer les opérateurs à installer des ***backdoors*** dans leurs logiciels de communication. Ces exigences compromettraient les systèmes cryptés de bout en bout ainsi que la sécurité des données des utilisateurs étant donné qu'il semble impossible de ne permettre cet accès qu'à certaines catégories de personnes **(3)**. L'**Autorité de Protection des données** a d'ailleurs émis un avis au sujet de l'obligation de rendre possibles les interceptions légales dans les systèmes de chiffrement, considérant que cela constituait une ingérence disproportionnée dans le droit au respect de la vie privée des personnes concernées **(4)**.

REFERENCES

(1) Gouvernance de l'internet — Stratégie du Conseil de l'Europe 2016-2019 — Démocratie, droits de l'homme et Etat de droit dans le monde numérique adoptée à la 1252e réunion des Délégués des Ministres le 30 mars 2016, p.12-13

(2) Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte) (abrogeant le règlement (CE) 428/2009 du 5 mai 2009)

(3) Bart Preneel, « Le gouvernement veut affaiblir la sécurité de nos communications », L'Echo, 11 octobre 2021.

(4) Autorité de Protection des données, Avis n° 108/2021 concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (CO-A-2021-099), du 28 juin 2021.

MARIE DEJAER

belgium@lexing.network

Regulation of cryptographic software

Legislative context

▪ *The first texts requiring Belgian telecom operators to have their terminals approved by the Belgian Institute of Posts and Telecommunications (BIPT) in order to ensure the possibility of implementing the eavesdropping methods of the time were lost in the hundreds of pages of an unpleasant programme law of 1994. The recent texts are a little more visible, if not always readable.*

▪ *The* ***law of 13 June 2005*** *on electronic communications defines cryptography as "*the set of services implementing the principles, means and methods of transforming data with the aim of concealing their semantic content, establishing their authenticity, preventing their modification from going unnoticed, preventing their repudiation and preventing their unauthorised use*". According to Article 48 of the same law, the use of cryptography is unrestricted in Belgium. The provision of cryptographic services to the public is subject to a prior declaration to BIPT.*

▪ *Despite this freedom, the government wishes to safeguard the interests of criminal investigations and its secret services. In this regard,* ***Article 88 quater of the Code of Criminal Investigation*** *provides for the infringement of data integrity in the context of an investigation. Indeed, it is not desirable that the use of encryption should contravene the prosecution of criminal acts at both national and European level* ***(1)****.*

▪ *In this same perspective, cryptography is of interest for both civilian and military use, being considered as a system ensuring "information security". As such, it is covered by the Regulation setting up a Union regime for the control of exports, transfers, brokering and transit of* ***dual-use items (2)****.*

Controversy

▪ *A* ***Belgian bill*** *is currently the subject of much controversy, in that it would compel operators to allow the decryption of this data at the request of certain users, such as the police, in order to facilitate investigations. This is nothing less than forcing operators to install* ***backdoors*** *in their communications software. These requirements would compromise end-to-end encrypted systems and the security of users' data as it seems impossible to allow access only to certain categories of people* ***(3)****. The* ***Data Protection Authority*** *has also issued an opinion on the requirement to enable lawful interception in encryption systems as a disproportionate interference with the right to privacy of data subjects* ***(4)****.*

REFERENCES

(1) Internet Governance - Council of Europe Strategy 2016-2019 - Democracy, human rights and the rule of law in the digital world adopted at the 1252th Committee of Ministers' Deputies meeting on 30 March 2016, p.11-12

(2) Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) (repealing Regulation (EC) 428/2009 of 5 May 2009)

(3) Bart Preneel, « Le gouvernement veut affaiblir la sécurité de nos communicationsv », L'Echo, 11 octobre 2021.

(4) Autorité de Protection des données, Avis n° 108/2021, regarding a draft legislation on the collection and retention of identification, traffic and location data in the electronic communications sector and their access by the authorities and a draft Royal Decree amending the Royal Decree of 19 September 2013 implementing Article 126 of the Law of 13 June 2005 on electronic communications (CO-A-2021-099) of 28 June 2021.

MARIE DEJAER

belgium@lexing.network

JADE & FOUNTAIN PRC LAWYERS

Cadre légal pour l'importation/l'exportation et l'utilisation de la cryptographie en République populaire de Chine

▪ **L'arsenal législatif chinois** régissant l'importation, l'exportation et l'utilisation de la cryptographie a récemment été modifié par un plusieurs lois et règlements, nouvellement adoptés ou mis à jour, dont notamment :

- la loi sur la cryptographie (du 26 octobre 2019, entrée en vigueur le 1er janvier 2020) ;
- la loi sur le contrôle des exportations (du 17 octobre 2020, entrée en vigueur le 1er décembre 2020) ;
- le règlement sur la gestion de l'importation et de l'exportation de technologies (du 10 décembre 2001, modifié le 20 novembre 2020) ;
- l'avis concernant la publication de la liste des chiffrements commerciaux soumis à une licence d'importation, de la liste des chiffrements commerciaux soumis à un contrôle d'exportation et des mesures réglementaires connexes (du 26 novembre 2020, entré en vigueur le 1er janvier 2022) (ci-après dénommé « avis n°63 ») ;
- l'avis n°75 (entré en vigueur le 1er janvier 2022) publiée conjointement par le ministère du Commerce et l'administration nationale des douanes.

▪ En outre, un projet de « règlement sur la gestion des codes de chiffrement commerciaux » fait actuellement l'objet d'une consultation publique.

Cryptographie : définition et catégories

▪ En droit chinois, la « **cryptographie** » est définie comme « *la technologie, le produit et le service qui appliquent une méthode de transformation spécifique à des informations ou à autres éléments en vue d'assurer la protection par chiffrement ou la certification de la sécurité* ».

▪ La cryptographie se divise en **cryptographie principale**, **cryptographie générale** et **cryptographie commerciale**.

▪ La cryptographie principale et la cryptographie générale sont utilisées pour protéger les informations contenant un « secret d'Etat » (tel défini dans la loi sur les secrets d'Etat de la RPC).

▪ La cryptographie commerciale est, quant à elle, utilisée pour protéger les informations autres que les secrets d'État.

Importation/Exportation de la cryptographie

▪ La loi sur la cryptographie pose le principe selon lequel la recherche, la production, la vente, la prestation de services, **l'importation** ou **l'exportation** de cryptographie commerciale ne doit pas porter atteinte à la sécurité nationale, à l'intérêt public ou aux droits et intérêts légitimes de tiers **(1)**.

▪ Lorsque l'importation d'une cryptographie commerciale dotée d'une fonctionnalité de protection chiffrée touche à la sécurité nationale ou l'intérêt

(1) La cryptographie principale et la cryptographie générale sont considérées comme des secrets d'État, dont l'importation et l'exportation sont interdites par la loi.

public, il convient de solliciter une licence d'importation auprès du ministère du commerce et de l'administration nationale de la cryptographie.

▪ Parallèlement, des contrôles sont appliqués pour l'exportation de cryptographie commerciale concernant la sécurité nationale ou l'intérêt public, ou à l'égard de laquelle la Chine a une obligation internationale.

▪ La loi sur la cryptographie charge le ministère du commerce, en collaboration avec l'administration nationale de la cryptographie et l'administration générale des douanes, de publier et de mettre à jour **une liste** des cryptographies commerciales soumises à une licence d'importation et une liste des cryptographies commerciales soumises à un contrôle à l'exportation.

▪ Ces listes ont été publiées au moyen des avis n° 3 et n°75 visés ci-dessus.

▪ La cryptographie commerciale appliquée aux produits de consommation **(2)** n'est soumise ni à la licence d'importation ni au contrôle des exportations.

Utilisation de la cryptographie

▪ S'agissant de l'utilisation de la cryptographie principale ou de la cryptographie générale, toute information contenant un **secret d'État** transmise par des communications filaires ou sans fil ou un système d'information stockant ou traitant des secrets d'État doit être chiffrée et sécurisée ou faire l'objet d'une authentification de sécurité en utilisant la cryptographie principale ou la cryptographie générale.

▪ S'agissant de l'utilisation de la cryptographie commerciale, il existe un certain nombre de règles spéciales applicables aux cryptographies commerciales qui revêtent une certaine importance ou qui sont utilisées par un opérateur d'une « infrastructure d'information critique » **(3)** :

- lorsqu'un produit de cryptographie commerciale concerne la sécurité nationale, l'économie nationale et les moyens de subsistance de la population ou l'intérêt public et qu'il figure dans le « catalogue des équipements des réseaux critiques et des produits de cybersécurité », il ne peut être distribué ou fourni que s'il a été évalué et certifié par un organisme agréé, et
- un **opérateur d'infrastructures d'information critiques** doit obligatoirement utiliser la cryptographie commerciale pour sécuriser l'infrastructure d'information critique concernée et procéder à une évaluation de la sécurité de la cryptographie commerciale soit lui-même soit par l'intermédiaire d'un organisme externe d'évaluation et de certification lorsque la loi l'exige ;
- par ailleurs, lorsque les services fournis par un opérateur d'infrastructures d'information critiques sont susceptibles d'avoir un impact sur la sécurité nationale, un examen de la sécurité nationale par l'autorité nationale du cyberespace, en collaboration avec les autorités compétentes (dont l'administration nationale de la cryptographie), est requis.

(2) La « cryptographie commerciale pour les produits de consommation » désigne le produit ou la technologie ayant une fonctionnalité de chiffrement qui ne peut pas être modifiée sans moyens spéciaux et qui peuvent être achetés par le public par un canal de distribution normal sans contrainte et pour des raisons personnelles.

(3) L'expression « infrastructure d'information critique » est définie à l'article 31 de la loi sur la cybersécurité et désigne les infrastructures d'information qui, si elles sont détruites, rendues dysfonctionnelles ou font l'objet de fuites, sont susceptibles de mettre gravement en danger la sécurité nationale, le bien-être de la population et l'intérêt public.

JUN YANG

china@lexing.network

The import/export and use of cryptography in People's Republic of China

▪ *The* ***Chinese regulatory body*** *governing the import/export and use of cryptography has been refreshed by a number of new/updated laws and regulations released recently, to just quote the following:*

- *Cryptography Law (released on October 26, 2019 and effective on January 1, 2020)*
- *Export Control Law (released on October 17, 2020 and effective on December 1, 2020)*
- *Regulation on Administration of Import and Export of Technologies (released on December 10, 2001 and amended on November 20, 2020)*
- *Announcement on Issuing the List of Commercial Cryptography under Import Licensing, the List of Commercial Cryptography under Export Control and the Related Regulation Measures (released on November 26, 2020 and effective on January 1, 2022) (referred to hereinafter as "Announcement No. 63)*
- *Announcement No. 75 (effective on January 1, 2022) joint release by the Ministry of Commerce and the National Customs Administration.*

▪ *Besides, a draft of "Regulation on Administration of Commercial Cipher Codes" is being circulated for comments.*

Definition and classification of cryptography

▪ *The "****Cryptography****" is defined under Chinese law as "technology, product and service that effect encryption protection or security certification of information and the like by adopting the method for specific conversion."*

▪ *Cryptography is divided into* ***core cryptography****,* ***ordinary cryptography*** *and* ***commercial cryptography****.*

▪ *Core cryptography and ordinary cryptography shall be used to secure information containing "national secrecy" (separately defined by the PRC National Secrecy Law).*

▪ *Commercial cryptography shall be used to secure information other than state secrecy.*

Import/Export of cryptography

▪ *The Cryptograph Law poses the principle that the research, production, sale, service,* ***import*** *or* ***export*** *of commercial cryptography shall not be detrimental to national security, public interest or the lawful rights and interests of others* ***(1)****.*

▪ *Where the import of a commercial cryptography with encrypted protection functionality concerns national security or the public interest, the import license of the Ministry of Commerce and the State Cryptographic Administrative Office shall be solicited.*

(1) Core cryptography and ordinary cryptography are defined as state secrets under Chinese law and the law does not open the possibility for their import and export.

▪ *Meanwhile, the export control shall apply to the export of a commercial cryptography concerning national security or the public interest, or with respect to which China bears an international obligation.*

▪ *The Cryptograph Law provides that (a)* ***a list*** *of commercial cryptography under import licensing and (b) a list of commercial cryptography under export control shall be issued and updated by the Ministry of Commerce in collaboration with the State Cryptographic Administration Office and the General Administration of Customs.*

▪ *The Announcement 63 and Announcement 75 released such lists by substantiating the commercial cryptograph which shall be subject to export control or import license.*

▪ *Commercial cryptography applied to consumer products* ***(2)*** *is not subject to the import license and export control.*

Use of Cryptograph

▪ *Use of core cryptography or ordinary cryptography: any information containing* ***state secrecy*** *transmitted by wired or wireless communications or an information system storing or processing state secret information shall be encrypted and secured or be subject to security authentication by using core cryptography or ordinary cryptography.*

▪ *Use of commercial cryptograph: there are a number of special rules applicable to commercial cryptograph of significance or the use by an operator of a "critical information infrastructure"* ***(3)*** *is concerned:*

- *Where a commercial cryptographic product concerns national security, national economy and people's livelihood or the public interest and is listed in the "catalogue of critical network equipment and cyber-security products", it may not be distributed or supplied unless such product has been tested and certified by a qualified institution, and*
- *An* ***operator of critical information infrastructure*** *must use commercial cryptography to secure the critical information infrastructure concerned and conduct security assessment of commercial cryptography by itself or by an external testing and certification institution where the law so requires.*
- *Where the services procured by an operator of critical information infrastructure are likely to have an impact on national security, a national security review by the State cyberspace authority in conjunction with relevant authorities (including the state cryptographic administrative authority) is required.*

(2) The "commercial cryptograph for consumer products" refers to the product or technology having encryption functionality which may not be modified without special means and such products may be purchased by public through normal distribution channel without constraint and for personal.

(3) The term "critical information infrastructure" is defined in article 31 of the "Cyber Security Law" and this term refers to those information infrastructure, if destroyed, rendered dysfunctional or leaked, is likely to seriously endanger national security, people's welfare and public interest.

JUN YANG

china@
lexing.network

Cadre légal pour l'exportation/importation/utilisation des outils de chiffrement en Espagne

▪ Le chiffrement et les techniques cryptographiques constituent des **éléments de sécurité fondamentaux** dans la politique d'information d'une organisation et représentent une garantie supplémentaire afin de réduire le risque de traitement des données à caractère personnel.

▪ Ainsi, le règlement général sur la protection des données (règlement (UE) 2016/679) (**RGPD**), norme directement applicable en Espagne, aborde le chiffrement dans plusieurs dispositions, telles que le considérant 83 et les articles 6, paragraphe 4, point e), 32, paragraphe 1, point a), et 34, paragraphe 3, point a). En Espagne, la loi organique 3/2018 de protection des données, qui complète le RGPD, ne contient pas de nouvelles références au chiffrement.

▪ **L'Autorité de contrôle espagnole (AEPD)** considère que les systèmes de chiffrement ne peuvent pas être limités dans leur performances dans le but de permettre le contrôle des communications par les autorités policières ou judiciaires. La nécessité de lever le voile sur les communications pour enquêter sur les activités criminelles ne justifie pas l'incorporation de vulnérabilités secrètes dans les systèmes de chiffrement, telles que des clés ou des portes dérobées.

▪ En ce sens, l'utilisation en Espagne de la cryptographie fait l'objet de peu de contraintes légales. L'une des contraintes les plus importantes est celle contenue dans l'**article 43 de la Loi générale sur les télécommunications** qui, d'un côté reconnaît que les informations, de tout type, transmises par l'intermédiaire de réseaux de communications électroniques peuvent être protégées par des procédures de chiffrement et que le chiffrement est un instrument de sécurité de l'information, et d'un autre côté, établi l'obligation de fournir à un organe de l'administration générale de l'État ou à un organisme public les algorithmes ou toute procédure de chiffrement utilisée pour protéger la confidentialité des informations, ainsi que l'obligation de fournir gratuitement les dispositifs de chiffrement aux fins de leur contrôle conformément à la réglementation en vigueur.

▪ L'exportation des outils de chiffrement de l'Espagne vers d'autres pays de l'UE est largement libre. L'exportation vers des pays tiers peut nécessiter une autorisation générale communautaire d'exportation (AGCE) ou une licence nationale générale.

▪ L'Espagne a signé les principaux accords internationaux sur la cryptographie, dont le **CoCom**, qui permettait, jusqu'en 1994, d'assouplir des restrictions sur la cryptographie pour permettre l'exportation de logiciels de cryptographie, et depuis 1996, **l'arrangement de Wassenaar** sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage permettant aussi l'exportation de logiciels qui utilisent le chiffrement pour protéger la propriété intellectuelle (comme les systèmes de protection contre la copie).

MARC GALLARDO

spain
@lexing.network

Legal framework for the export/import/use of encryption tools in Spain

▪ *The use of encryption and cryptographic techniques is a* ***fundamental security element*** *in an organization's information policy and represents an additional safeguard to reduce the risk of processing personal data.*

▪ *In addition, the General Data Protection Regulation (Regulation (EU) 2016/679) ("****GDPR****"), a standard directly applicable in Spain, addresses encryption in several provisions, such as recital 83 and Articles 6(4)(e), 32(1)(a) and 34(3)(a). Organic Law 3/2018 on Data Protection, which complements the GDPR, does not contain new references to encryption.*

▪ *Thus, the* ***Spanish Authority (AEPD)*** *considers that encryption systems cannot have limits in their performance to allow the control of communications by the police or judicial authorities. The need to lift the veil on communications to investigate criminal activity does not justify the incorporation of secret vulnerabilities into encryption systems, such as keys or backdoors.*

▪ *In this sense, the use of cryptography in Spain has few legal constraints. One of the most important is that contained in* ***Article 43 of the General Telecommunications Law****, where, in addition to recognizing that any type of information transmitted through electronic communications networks can be protected by encryption procedures and that encryption is an instrument of information security, it is established that, among its conditions of use, when used to protect the confidentiality of information, the obligation to provide an organ of the general administration of the State or a public body with the algorithms or any encryption procedure used may be imposed, as well as the obligation to provide the encryption devices free of charge for the purpose of their control in accordance with the regulations in force.*

▪ *The export of encryption tools from Spain to other EU countries is largely free. Export to third countries may require a Community General Export Authorisation (DAGE) or a general national licence.*

▪ *Spain has signed the main international agreements on cryptography; namely the* ***COCOM*** *treaty until 1994, which allowed restrictions on cryptography to be eased to allow the export of cryptographic software, and since 1996 the* ***Wassenaar Arrangement*** *on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, which also allows for the export of software that uses encryption to protect intellectual property (such as protection systems against copying).*

MARC GALLARDO

spain
@lexing.network

Cadre légal pour l'exportation, l'importation et l'utilisation des outils de chiffrement en France

▪ En France, **l'usage d'outils de chiffrement** est entièrement laissé à la discrétion des entreprises qui souhaitent utiliser de tels outils.

▪ En revanche, selon l'article 30 de la LCEN, les sociétés qui souhaitent procéder à la « ***fourniture, l'importation, le transfert intracommunautaire et l'exportation d'un moyen de cryptologie*** *sont soumis, sauf exception, à déclaration ou à demande d'autorisation* ».

▪ Ces démarches incombent au fournisseur du moyen de cryptologie et sont à accomplir auprès de **l'Agence nationale de sécurité des systèmes d'information (Anssi)**.

▪ Si une société décide de s'affranchir de ces démarches effectuées auprès de l'Anssi, sa solution peut faire l'objet d'une **demande de retrait** du marché français.

▪ Conformément à l'article 29 de la loi LCEN, on entend par prestation de cryptologie « *toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie* ».

▪ Un moyen de cryptologie concerne tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.

▪ Au niveau européen, le **règlement eIDAS n°910/2014 du 23 juillet 2014** est le premier règlement qui est venu imposer des mesures de chiffrement pour tous les prestataires de service de confiance de type signatures électroniques, prestataire d'identité numérique, lettre recommandée électronique…

▪ De la même façon, le **RGPD** impose que des mesures de sécurité soient mises en œuvre pour la gestion de données à caractère personnel et le chiffrement est la première des mesures examinées.

▪ Le RGPD est mis en œuvre depuis mai 2018 et la première **décision de la CNIL** sanctionnant un défaut de chiffrement est intervenue le 17 décembre 2020 **(1)**, décision dans laquelle 2 médecins ont été sanctionnés car ces derniers n'avaient « *pas pris soin de chiffrer les données contenues dans leurs outils professionnels respectifs* ». L'un a, par ailleurs, estimé que le chiffrement provoquait un ralentissement dans l'exécution des applications (dossier médical, outil de visualisation des images…).

▪ La CNIL a donc rappelé que l'absence de chiffrement permettrait à toute personne, s'introduisant de manière indue sur le réseau auquel l'ordinateur est

(1) https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins

raccordé, d'accéder aux données contenues dans le disque dur de l'ordinateur de manière lisible et en clair.

▪ A cet égard, la CNIL recommande l'usage de certains moyens de chiffrement des postes nomades et supports de stockage mobiles (clés USB, les disques durs externes ou les ordinateurs portables) tels que le chiffrement du disque dur dans sa totalité lorsque cette fonction est proposée par le système d'exploitation.

▪ Une autre décision importante est intervenue en France dans l'utilisation des outils proposés par les GAFAM. Le Conseil d'Etat a, en effet, considéré le 12 mars 2021 **(2)** que le site internet https://www.doctolib.fr/ était autorisé à héberger ses données de santé sur un cloud géré par Amazon, société dont le siège est situé aux USA, car les données étaient chiffrées sur les serveurs d'AWS et que doctolib gérait lui-même les clés de chiffrement, rendant ainsi illisible les données même pour Amazon lui-même et par conséquent pour toutes les autorités qui s'adresseraient à Amazon.

(2) https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043261200

▪ La 2e condition exigée par le CE est que AWS s'engage à transmettre à ses clients toutes les demandes des autorités étrangères.

Les outils existants

▪ Les entreprises utilisent aujourd'hui, deux principaux types de chiffrement de données : le chiffrement asymétrique, et le chiffrement symétrique. Ces deux types diffèrent dans la façon dont les données sont déchiffrées.

▪ Dans le cas du chiffrement symétrique, la même clé de chiffrement est utilisée pour le chiffrement et le déchiffrement du message ou du fichier.

▪ Dans le cas du chiffrement de données asymétrique, deux clés sont utilisées : une clé publique, et une clé privée. La clé publique peut être partagée avec n'importe qui, mais la clé privée doit impérativement être protégée.

ANTHONY SITBON

france
@lexing.network

Legal framework for exportation, importation and use of encryption tools in France

- *In France,* ***the use of encryption tools*** *is entirely left to the discretion of companies wishing to use such tools.*

- *However, according to Article 30 of the Confidence for Digital Economy Act (LCEN), companies wishing to "*supply, import, transfer from or to another Member State of the European Community and export cryptology means are subject, except in exceptional cases, to a declaration or an authorisation request*".*

- *These steps are the responsibility of the supplier of the cryptology means and must be done with the* ***National Cybersecurity Agency (Anssi)****.*

- *If a company decides to ignore these steps, its solution may be subject to a* ***request for withdrawal*** *from the French market.*

- *According to Article 29 of the LCEN, a cryptology service means "*any operation consisting of the implementation, for others, of cryptology means*".*

- *"Cryptology means" means any hardware or software designed or modified to transform data, whether information or signals, using secret conventions or to perform the reverse operation with or without secret conventions. The main purpose of these cryptology means is to guarantee the security of storage or transmission of data, by allowing to ensure their confidentiality, their authentication or the control of their integrity.*

- *At the European level, the* ***eIDAS Regulation No. 910/2014 of 23 July 2014*** *is the first regulation that came to impose encryption measures for all providers of trust services such as electronic signature, digital identity, electronic registered delivery.*

- *Similarly, the* ***GDPR*** *requires that security measures, including encryption, be implemented for the management of personal data.*

- *The GDPR has been implemented since May 2018 and the first* ***CNIL decision*** *sanctioning a failure to encrypt occurred on 17 December 2020* ***(1)****. In this decision, 2 doctors were sanctioned because they had "*not encrypt the data contained in their respective business tools*". One of them stated that encryption caused a slowdown in the execution of applications (such as medical file, image viewing tool).*

- *The CNIL pointed out that the absence of encryption would allow any person, unlawfully entering the network to which the computer was connected, to access the data contained on the computer's hard disk in a legible and clear manner.*

- *The CNIL generally recommends the use of certain encryption methods for mobile workstations and mobile storage media (USB sticks, external hard drives or laptops), such as the encryption of the hard drive in its entirety when the operating system offers such a functionality.*

- *Another important decision was issued in France regarding the use of tools offered by Big Tech. On 12 March 2021* ***(2)****, the French* ***Council of State*** *ruled that*

(1) https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins

(2) https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043261200

the website https://www.doctolib.fr/ was authorized to host its health data on a cloud managed by Amazon, a company headquartered in the USA because the data was encrypted on AWS' servers and doctolib itself managed the encryption keys, thereby making the data unreadable even for Amazon and consequently for all the authorities that would contact Amazon.

- *The Council of State also took into account the fact that AWS committed to transmit to its customers all disclosure requests from foreign authorities.*

Existing tools

- *Today, companies use two main types of data encryption: asymmetric encryption and symmetric encryption. These two types differ in the way the data is decrypted.*
- *In the case of symmetric encryption, the same encryption key is used to encrypt and decrypt the message or file.*
- *In the case of asymmetric data encryption, two keys are used: a public key and a private key. The public key can be shared with anyone, but the private key must be protected.*

ANTHONY SITBON

france
@lexing.network

Cadre légal pour l'exportation, l'importation et l'utilisation des outils de chiffrement en Grèce

▪ Le **règlement (UE) n° 2021/821** institue un régime de l'Union de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage. Ce règlement fournit une liste exhaustive des biens à double usage, y compris les logiciels et les technologies, susceptibles d'avoir une utilisation tant civile que militaire et dont l'exportation est soumise à une autorisation préalable. Son annexe I comprend (sous la **catégorie 5A002**) les systèmes, équipements et composants assurant la « sécurité de l'information » :

a. conçus ou modifiés pour utiliser la « cryptographie pour la confidentialité des données » ayant un « algorithme de sécurité décrit », la capacité cryptographique étant utilisable, ayant été activée ou pouvant être activée par tout moyen autre que l'« activation cryptographique » sécurisée, c'est-à-dire :
- les biens dont la fonction principale est la « sécurité de l'information » ;
- les systèmes, équipements ou composants de communication numérique ou de réseau non visés à l'Annexe I ;
- les calculateurs, autres biens dont la fonction principale est le stockage ou le traitement de l'information et leurs composants, non visé à l'Annexe I ;
- les biens, non visés à l'Annexe I, pour lesquels la « cryptographie pour la confidentialité des données » ayant un « algorithme de sécurité décrit » répond à toutes les conditions suivantes :
  - elle est à l'appui d'une fonction non primaire du bien ; et
  - elle est réalisée par un équipement ou un « logiciel » intégré qui serait, en tant que tel, visé à la catégorie 5, partie 2.

b. consistant dans un « jeton d'activation cryptographique » ;
c. conçus ou modifiés pour utiliser ou accomplir la « cryptographie quantique » ;
d. conçus ou modifiés pour employer des techniques cryptographiques pour générer des codes de découpage en canaux, des codes de brouillage ou des codes d'identification de réseau pour des systèmes de modulation à bande ultralarge et présentant une largeur de bande supérieure à 500 MHz ou une « bande passante fractionnelle » de 20 % ou plus
e. conçus ou modifiés pour employer des techniques cryptographiques pour générer le code d'étalement pour le « spectre étalé », autres que ceux mentionnés à l'alinéa 5A002.d., y compris le code de saut pour les systèmes à « sauts de fréquence ».

▪ En Grèce, **l'article 8, paragraphe 7, du décret présidentiel 47/2005** (procédure de « levée du secret des communications ») dispose que les « *fournisseurs de services de communication et les fournisseurs de réseaux de communication* » « *qui utilisent des méthodes de codage, de compression ou de chiffrement* » doivent, sur ordre de l'autorité compétente, « *fournir les informations demandées sous forme décodée* ». Cet article n'exige pas spécifiquement la fourniture des clés de chiffrement en tant que telles, mais la fourniture des informations sous « *forme décodée* ». Toutefois, il est théoriquement possible pour l'autorité compétente de demander la divulgation des clés de chiffrement si cela est jugé nécessaire pour les besoins d'une enquête sur un crime grave ou pour une question de sécurité nationale.

REFERENCES

(1) Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte) (abrogeant le règlement (CE) 428/2009 du 5 mai 2009)

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

Legal framework for exportation, importation and use of encryption tools

▪ ***Regulation (EU) No 2021/821*** *sets out a Union regime for the control of exports, transfer, brokering and transit of dual-use items. This Regulation provides a comprehensive list of dual-use items, including software and technology, which can be used for both civil and military purposes, for the export of which a prior authorisation is required. Annex I includes (under* ***Category 5A002****) following information security systems, equipment and components:*

a. Designed or modified to use "cryptography for data confidentiality" having a "described security algorithm", where that cryptographic capability is usable, has been activated, or can be activated by any means other than secure "cryptographic activation", meaning:

- *items having "information security" as a primary function;*
- *digital communication or networking systems, equipment, or components, not explicitly described under this Annex;*
- *computers or other items having information storage or processing as a primary function, and components therefor, not explicitly described under this Annex;*
- *items, not specified under this Annex, where the "cryptography for data confidentiality" having a "described security algorithm" meets all the following:*
  - *it supports a non-primary function of the item; and*
  - *it is performed by incorporated equipment or "software" that would, as a standalone item, be specified in Category 5 – Part 2.*

b. Being a "cryptographic activation token";
c. Designed or modified to use or perform "quantum cryptography";
d. Designed or modified to use cryptographic techniques to generate channelising codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having a bandwidth exceeding 500 MHz; or a "fractional bandwidth" of 20 % or more;
e. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, other than those specified in 5A002.d, including the hopping code for "frequency hopping" systems".

▪ *In Greece,* ***article 8(7) of the Presidential Decree (PD) 47/2005*** *(procedure for the 'lifting of secrecy of communications') dictates that "providers of communication services and providers of communication networks" "which use encoding, compression or encryption methods" must - upon relevant order by the competent authority – "provide the requested information in decoded form". Article 8(7) does not specifically require provision of the encryption keys as such but provision of information in "decoded form". However, it is theoretically possible the competent authority to request disclosure of encryption keys if this is deemed necessary for the needs of the investigation of a serious crime or for a national security matter.*

REFERENCES

(1) Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) (repealing Regulation (EC) 428/2009 of 5 May 2009)

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

Les biens à double usage

▪ Les biens à double usage sont des produits, technologies et logiciels susceptibles d'avoir une utilisation tant civile que militaire. Ils incluent notamment tous les biens qui peuvent à la fois être utilisés à des fins non explosives et intervenir de quelque manière que ce soit dans la fabrication d'armes nucléaires ou d'autres dispositifs nucléaires explosifs.

Technologies à double usage

▪ Afin de promouvoir la sécurité de l'Union européenne, des **contrôles** et des mesures restrictives s'appliquent de manière uniforme et cohérente quant à leur exportation, importation, transit, courtage, assistance technique et transfert intangible de technologie.

▪ Les accords internationaux sur le contrôle des biens à double usage, notamment l'arrangement de Wassenaar, le régime de contrôle de la technologie des missiles, le groupe des fournisseurs nucléaires et la convention sur les armes chimiques, répertorient ces biens en dix catégories, allant des matières, installations et équipements nucléaires à l'électronique, en passant par les capteurs et lasers, les calculateurs, ou encore les télécommunications et la « sécurité de l'information ».

▪ L'opérateur doit déterminer si son produit est susceptible d'être classé comme « bien à double usage » et, à cette fin, il doit comparer les caractéristiques techniques de ce produit avec les critères contenus, pour chaque bien listé, dans l'annexe I du règlement (EU) 2021/821 **(1)**.

▪ Les autorités douanières luxembourgeoises ne sont pas tenues d'accepter le code tarifaire choisi par l'opérateur. Il est conseillé à l'opérateur, pour obtenir la garantie d'un classement tarifaire valable dans toute l'UE, d'introduire une demande de renseignement tarifaire contraignant auprès de l'administration compétente.

Le transfert intangible de technologie relatif à des biens à double usage est soumis à autorisation préalable

▪ Sauf lorsque le transfert immatériel de technologie ne porte sur des connaissances qui sont du domaine public ou qui relèvent de la recherche scientifique fondamentale, tout opérateur qui procède à un transfert intangible de technologie relatif à des biens à double usage, y inclus lorsqu'un tel transfert contribue ou est susceptible de contribuer à la prolifération — c'est-à-dire la transmission par voie digitale ou orale de documents quel qu'en soit le support ; la gestion ou la maintenance à distance de réseaux informatiques ; le suivi de cours magistraux ou de formations sous quelque forme que ce soit ; les activités d'études ou de recherche scientifique ; la transmission de savoir-faire, de connaissances pratiques, techniques ou scientifiques et d'informations sous quelque forme que ce soit — doit introduire une **demande d'autorisation individuelle ou globale préalable**.

(1) Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte) (abrogeant le règlement (CE) 428/2009 du 5 mai 2009)

▪ Les pièces justificatives à joindre à la demande d'autorisation individuelle ou globale sont les suivantes : une lettre explicative détaillée de l'opération ; un contrat de vente ; un descriptif des moyens mis en œuvre ou à mettre en œuvre pour assurer la sécurité des informations, tant au niveau du fournisseur du savoir-faire qu'à celui de la relation entre fournisseur et bénéficiaire du savoir-faire ; une présentation détaillée de l'opération de transfert envisagée, de son contenu et de tous les acteurs impliqués ; un document d'identification des risques associés à l'opération de transfert ; une présentation détaillée des moyens organisationnels, humains et techniques mis en œuvre pour parer aux risques ; un extrait récent du registre du commerce luxembourgeois.

▪ La demande d'autorisation est traitée dans un délai de 60 jours ouvrables, à partir du jour où le dossier est complet, ce délai pouvant être prolongé pour une durée maximum de 30 jours.

▪ En l'absence de réponse dans ce délai, la demande d'autorisation est considérée comme accordée pour **1 an pour les autorisations individuelles**, renouvelable pour une période de 6 mois, et pour **3 ans pour les autorisations globales**, renouvelable pour une période de 18 mois.

▪ Une fois cette autorisation obtenue, l'opérateur doit respecter les conditions spéciales qui y sont contenues et tenir un registre détaillé et complet des opérations effectuées en application de l'autorisation.

▪ En cas de refus d'autorisation, un recours peut être introduit contre la décision administrative.

Sanctions

▪ Encourent une **peine de réclusion de 5 à 10 ans** et/ou une **amende de 25.000 à 1.000.000 euros**, les personnes qui effectuent un transfert intangible de technologie pour des biens à double usage sans disposer de l'autorisation requise ou sans respecter l'interdiction applicable à l'opération.

▪ Encourent une **peine d'emprisonnement de 6 mois à 5 ans** et/ou une **amende de 7.500 à 75.000 euros**, les personnes qui :

- ne tiennent pas ou qui ne conservent pas durant la période de 10 ans (courant à partir de la fin de l'année civile au cours de laquelle l'opération a eu lieu) les registres ;
- ne présentent pas les registres sur première demande des ministres ;
- omettent, de manière répétée ou significative, de renseigner une ou plusieurs des informations obligatoires du registre ;
- fournissent des informations qui s'avèrent fausses ou incomplètes dans le cadre d'une demande d'autorisation ;
- ne tiennent pas les engagements pris dans les déclarations d'utilisation et demandes d'autorisation remises aux ministres ;
- ne transmettent pas les informations dans les délais et selon les modalités indiquées.

EMMANUELLE RAGOT

luxembourg@lexing.network

Dual-use items

▪ *Dual-use items are goods, technology and software that can be used for both civil and military purposes and include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.*

Dual use technologies

▪ *In order among other objectives, to promote the security of the EU,* ***controls*** *and restrictive measures apply in a uniform and coherent way in relation to their export, import, transit, brokering, technical assistance and intangible transfer of technology too.*

▪ *International agreements on the control of dual-use items, comprising the Wassenaar Arrangement, the Missile Technology Control Regime, The Nuclear Suppliers Group, the Chemical Weapons Convention classify them in 10 categories from Nuclear materials, facilities and equipment, electronics, sensors and lasers to computers, Telecommunications and "information security" etc.*

▪ *The operator must determine whether his product is likely to be classified as a "dual-use item" and must compare the technical characteristics of the product with the criteria contained, for each item listed, in Annex I to Regulation (EU) 2021/821* ***(1)****.*

▪ *Customs authorities in Luxembourg are not required to accept the tariff code selected by the operator. It is advisable for the operator to be guaranteed of a tariff classification valid throughout the EU to lodge a binding tariff information request with the relevant Administration.*

Intangible transfer of technology related to dual-use-items is subject to a prior authorization

▪ *Except where the intangible transfer of technology implies knowledge in the public domain, basic scientific research, the operator operating an intangible transfer of technology related to dual-use items including where such a transfer contributes or is likely to contribute to proliferation including i.e. transmission, digitally or orally, of documents irrespective of the medium; management or remote maintenance of computer networks; monitoring of magisterial courses or training in any form whatsoever; study or scientific research activities; and transmission of knowledge, practical, technical or scientific knowledge and information in any form whatsoever shall* ***submit a prior individual or global authorization****.*

▪ *The supporting documents to be attached are the following: a detailed explanatory letter of the operation, sales agreement, description of the means implemented or to be implemented to guarantee the security of information, at the level of the provider of knowledge and at the level of the relation between the provider and the beneficiary of the knowledge, detailed presentation of the intended transfer, of its content and all concerned actors; document related to the*

(1) Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) (repealing Regulation (EC) 428/2009 of 5 May 2009)

identification of risks associated to the transfer, detailed presentation of organizational, human and technical measures implemented to face risks, recent extract of the Luxembourg Trade Register.

▪ *The application for authorisation shall be processed within 60 working days of the day on which the file is complete with a possible extension of 30 days.*

▪ *In the absence of a reply within this period, the application for authorisation shall be considered as granted for* ***1 year*** *for* ***individual authorisations****, renewable for a period of 6 months for* ***3 years*** *for* ***global authorisations****, renewable for a period of 18 months.*

▪ *Once provided to the operator, compliance with special conditions contained in the authorization shall be effective and a detailed and complete registers of operations carried out pursuant to the authorization shall be kept.*

▪ *A legal action may be lodged against the negative administrative decision.*

Sanctions

▪ *An* ***imprisonment of 5 to 10 years*** *and/or a* ***fine of an amount of EUR 25,000 to EUR 1,000,000****, may be applied to anyone who is operating an intangible transfer of technology related to dual-use items without the required authorisation or without respecting the prohibition applicable to the operation.*

▪ *May be punished by an* ***imprisonment of 6 months to 5 years*** *and/or a* ***fine of EUR 7,500 to EUR 75,000****, anyone who:*

- *fails to keep the registers or does not keep them during the period of 10 years (starting with the end of the calendar ear during which the operation took place);*
- *fails to present the registers at the first request of the ministers;*
- *omits, repeatedly or significantly, to fill in one or more of the mandatory information in the registers;*
- *provides, in the context of an application for authorisation, information that is false or incomplete;*
- *does not fulfil the commitments made in the declarations of use and applications for authorisation submitted to the ministers;*
- *fails to provide information within the time limits and in the manner set out.*

EMMANUELLE RAGOT

luxembourg@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
Brésil	Montgomery & Associados	Neil Montgomery	+55 11 4096-4000	brazil@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Pascal Archambault	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@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*	Mulligan, Banham & Findley	Janice F. Mulligan	+1 619.238.8700	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
Hongrie *Hungary*	OPL - Orbán & Perlaki	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde *India*	Poovayya & Co	Siddhartha George	+91 80 4115 6777	india@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
Luxembourg *Luxembourg*	Emmanuelle Ragot Lawyers & Associates	Emmanuelle Ragot	+ 352 661 84 4250	luxembourg@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	Øyvind Eidissen Ransedokken	+47 21 93 10 00	norway@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/