LEXOLOGY®
Navigator

Digital Business

in Luxembourg

Table of contents

Law stated date

- Correct as of

Contributors

Luxembourg

NautaDutilh

NautaDutilh
Vincent Wellens
Vincent.Wellens@nautadutilh.com

NautaDutilh
Carmen Schellekens
Carmen.Schellekens@nautadutilh.com

Recent developments and future prospects

Trends and developments

Have there been any notable recent trends or developments concerning the conduct of online and digital business (both business to business and business to consumer) in your jurisdiction, including any regulatory changes or case law?

The Luxembourg government realised early on that the inescapable increase in importance of digital business goes hand in hand with new cybersecurity risks, and that a capacity to tackle such risks would make the Grand Duchy very attractive for digital business players. Accordingly, the Luxembourg government issued a National Cybersecurity Strategy in 2012. The strategy's latest version was published for the period 2018-2020.

Luxembourg has a rather liberal approach to e-commerce and continues to rely on the 'home state' principle under the EU e-Commerce Directive 2000/31 to attract such businesses that would be more strictly regulated in some other countries. Luxembourg does not currently regulate collaborative platform businesses specifically.

Future prospects

What are the future prospects for digital business in your jurisdiction, including any proposed or potential regulatory reforms and future technological/market developments?

Digital Lëtzebuerg, a programme intending to establish Luxembourg as a 'smart nation' – that is, one that is modern, open, highly connected and ready to cope with a digital society – was launched in 2014. This has so far paid off: in April 2015 Luxembourg was awarded the ninth overall ranking in the Global Information Technology Report published by the World Economic Forum. The Luxembourg government seeks to continue investing in this area and is particularly focused on further developing the digital economy, promoting e-government and encouraging the development of digital skills, as well as on strengthening and consolidating Luxembourg's position in the field of information and communication technology in the long term. In this context, the Luxembourg government has also issued a new National Cybersecurity Strategy for 2018-2020.

Legal framework

Legislation

What primary and secondary legislation governs the conduct of digital business in your jurisdiction?

- the Luxembourg e-Privacy Act, as modified;
- the Luxembourg Advertising Act;
- the Luxembourg Freedom of Expression in the Media Act, as modified.

Regulatory authorities

Which authorities regulate the conduct of digital business and what is the extent of their powers?

The main competent authority is the Ministry of Economy and, in particular, the Directorate of Digital Business and Information Security, whose principal aim is to create a modern and pragmatic environment that allows for actors active in the e-commerce field and trust service providers to evolve in a favourable climate. Accordingly, the directorate has the legislative powers to design and push forward the legislative framework in the areas of e-commerce, e-signature and e-archiving. Furthermore, the directorate has the competence to put in place means to assist companies along the way, such as via awareness campaigns and trainings.

Government policy and regulatory approach

How would you describe the government's policy and regulatory approach to digital business?

The Luxembourg government has taken a proactive approach towards digital business, including a favourable IP tax regime, which has attracted a number of key players including Amazon, eBay, iTunes, Skype and PayPal. The Luxembourg government focuses on further developing the digital economy, promoting e-government and encouraging the development of digital skills, and on strengthening and consolidating Luxembourg's long-term position in the ICT field. In that context, in 2014 Luxembourg launched Digital Lëtzebuerg, a programme intended to assert Luxembourg's position as a 'smart nation' (ie, a modern, open, highly connected nation ready to cope with a digital society). This is paying off: in April 2015 Luxembourg was awarded the ninth overall ranking in the Global Information Technology Report published by the World Economic Forum. The Luxembourg government has also realised that tackling cybersecurity risks at a national level gives it a competitive advantage as it makes Luxembourg more attractive for digital business players. Accordingly, the Luxembourg government has since 2012 issued a National Cybersecurity Strategy, the latest version of which is that for the period 2018-2020.

Establishing digital businesses

Requirements

What regulatory and procedural requirements govern the establishment of digital businesses in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

Pursuant to Article 4 of the Luxembourg e-Commerce Act, as modified, which implements the EU e-Commerce Directive (2000/31/EC), the taking-up and pursuit of a digital business (ie, the performance of so-called 'information society services') may not be made subject to a prior authorisation. This is, however, without prejudice to any other authorisation or other procedural requirement that is not specifically and exclusively targeted at information society services. Hence, digital businesses offering a certain good or service are treated the same as a brick-and-mortar business offering the same good or service.

Electronic contracts and signatures

Electronic contract availability

Are electronic contracts legally valid in your jurisdiction? If so, what rules and restrictions govern their formation (including any mandatory or prohibited provisions and contract formats)?

Yes, Article 11(2) of the Luxembourg e-Archiving Act prescribes the principle of non-discrimination of electronic documents, meaning that such documents cannot be rejected by a judge solely on the grounds that they are in electronic form or do not comply with the authenticity and integrity/durability requirements set out in that act and its executing Grand Ducal regulations.

Electronic contracts will however have the same probative value as their written counterparts only when they meet the integrity and authenticity requirements set out in the e-Archiving Grand-Ducal Regulation of 25 July 2015. Furthermore, to the extent that a so-called 'certified dematerialisation' or 'e-archiving services supplier' (which has to comply with more advanced requirements as set out in the Grand-Ducal Regulation Implementing Article 4 of the Luxembourg e-Archiving Act) is being relied upon, there is the additional benefit of presumption of equivalence.

Lastly, the following requirements must be taken into account when concluding an electronic contract:

- in the context of both business-to-business (B2B) (Article 51 of the Luxembourg e-Commerce Act, as modified) and business-to-consumer (B2C) (Article L-222-3 of the Luxembourg Consumer Code, as modified): prior information requirements; and
- in the B2C context: the formal requirements as set out in Article L-222-4 of the Luxembourg Consumer Code and the prohibition to include any unfair clauses – that is, any clauses that create a mere imbalance between the parties to the detriment of the consumer.

Are there any limitations or restrictions on transactions that can be concluded through electronic contracts?

Yes, pursuant to Article 50 of the Luxembourg e-Commerce Act electronic contracts are excluded for:

- contracts that create/transfer real estate ownership (for now, this requires an authentic act with a wet-ink signature before the notary, but an imminent law proposal may change that in the near future);
- contracts requiring by law the involvement of courts, public authorities or professionals exercising public authority;
- contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession; and
- contracts governed by family law or by the law of succession.

Data retention

Do any data retention requirements apply to electronic contracts?

Yes, electronic contracts have the same probative value as their written counterpart only when they meet the integrity/durability and authenticity requirements set out in the e-Archiving Grand-Ducal Regulation of 25 July 2015.

The storage terms prescribed by Luxembourg law moreover apply mutatis mutandis to electronic contracts (eg, supporting documents to accounting documents must be stored for 10 years (Article 16 of the Luxembourg Commercial Code) and the general limitation period is 10 years (Article 189 of the Commercial Code).

Remedies

Are any special remedies available for the breach of electronic contracts?

No. On a general note, we must point out that for consumers, Articles L411-1 and following of the Luxembourg Consumer Code, as modified, provide however for an extrajudicial dispute settlement mechanism via the Consumer Mediator.

Electronic signatures

Are electronic signatures legally valid in your jurisdiction? If so, what rules and restrictions govern their use?

Yes, in accordance with Article 1322-1 of the Luxembourg Civil Code, as modified. Pursuant to Article 18(3) of the Luxembourg e-Commerce Act, as modified, no person may however be obliged to sign electronically, so that a co-contracting party is entitled to refuse to sign electronically.

Not all electronic signatures will however have the equivalent probative value of a hand-written signature. A differentiation has to be made between the (simple) electronic signature (eg, electronic copy of a handwritten signature on a document), the advanced electronic signature and the qualified electronic signature, whereby only the qualified electronic signature is regarded as the equivalent of a handwritten signature and, thus, has a binding probative force towards a judge that can be disallowed only via an exceptional and burdensome procedure of verification of signature.

A 'qualified electronic signature' is defined as an advanced electronic signature that is based on a qualified certificate and is created by a qualified electronic signature creation device.

An electronic signature will in turn qualify as an advanced electronic signature where it:

- can be uniquely linked to the signatory;
- is capable of identifying the signatory;
- is created using means that the signatory can maintain under his or her sole control; and
- is linked to the data to which it related in such a manner that any subsequent change of the data is detectable.

It stems from the above that, where the signature is not a qualified electronic signature, it does not benefit from such presumption of equivalence and is not binding upon the judge who has a wider margin of discretion to appreciate whether to accept the signature or not. This margin of discretion is not unlimited. Indeed, Article 18(2) of the Luxembourg e-Commerce Act, as modified, provides for a principle of non-discrimination whereby an electronic signature may not be discarded by a judge simply due to being in electronic form or not satisfying the conditions of equivalence as set out by the law. This principle of non-discrimination means in practice that the burden lies with the person that contests the validity of an electronic signature (which is not a qualified electronic signature) and that it is upon the latter to prove that the electronic signature solution does not provide for sufficient guarantees in

terms of integrity and authenticity.

Furthermore, a non-qualified electronic signature can always constitute a "beginning of written proof", which must be then supported by other means of proof (eg, testimony, presumptions).

Electronic payments

Electronic payment systems

Are there any rules, restrictions or other relevant considerations regarding the use of electronic payment systems in your jurisdiction?

Yes, the provision of payment services is regulated by the Luxembourg Payment Services Act, as modified. Such services include:

the execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

The Luxembourg Payment Services Act, which implements the EU PSD1 (Payment Services, 2007/64/EC) and e-Money Directives, imposes numerous requirements in relation to:

- the payment service provider, which will need to meet a number of formal requirements (eg, obtaining a licence from the Ministry of Finance), administration and infrastructure requirements and legal form and shareholding requirements; and
- the performance of the payments services themselves, such as a large number of information requirements to be honoured towards the payment service user, but also a number of requirements incumbent on the payment service user, such as the principle of irrevocability (ie, the payment service user may not revoke a payment order once it has been received by the payer's payment service provider).

At EU level, a second payment services directive (PSD2, EU/2015/2366) has already been adopted, but is yet to be implemented in Luxembourg despite the deadline for implementation having lapsed on 13 January 2018. A PSD2 Draft Bill 7195, which will amend the Luxembourg Payment Services Act, is however pending.

Virtual currencies

Are there any rules or restrictions on the use of virtual currencies (eg, Bitcoin)?

There is no legal framework in Luxembourg specifically for virtual currencies. That said, the Luxembourg Financial Sector Regulator issued an official warning on 14 March 2018 in relation to virtual currencies in which it:

- stresses that any provision of financial sector services requires an authorisation by the Ministry of Finance; and
- invites persons considering exercising an activity associated with virtual currencies to submit their draft documentation to the regulator beforehand; the regulator will then determine whether such activity is regulated.

Data protection and cybersecurity

Collection, use and storage

What rules, restrictions and procedures govern the collection, use and storage of personal data in the course of digital business in your jurisdiction?

International data transfers

What rules and restrictions apply to the cross-border transfer of personal data collected in the course of digital business?

Cross-border transfers of personal data – that is, any transfers to countries outside the European Union/European Economic Area (EEA) – are regulated by Articles 44 to 50 of the GDPR, which applies directly in Luxembourg. Any such third-country transfers are subject to restrictions if they concern transfers to countries that the European Commission deems not to offer an adequate level of protection. Such transfers are thus prohibited unless adequate safeguards are provided, including:

- the use of the so-called 'standard contractual clauses' issued by the European Commission;
- the conclusion of intra-group binding corporate rules (which requires a prior authorization from the
-); or
- for recipients situated in the United States, the Privacy Shield certification (Article 46 of the GDPR).

A number of exceptions can also be relied upon to justify a third-country transfer, including, without limitation:

- the unambiguous explicit consent of the data subject;
- the transfer being necessary for the execution of a contract between the data subject and the data controller or the implementation of precontractual measures taken in response to the data subject's request;
- the conclusion or execution of a contract concluded in the interest of the data subject between the data controller and a third party; or
- the establishment, exercise or defence of legal claims (Article 49 of the GDPR).

Consumer rights

What rights are afforded to consumers in relation to their personal data?

As data subjects, consumers are granted the following rights in relation to their personal data by virtue of Articles 12 to 23 of the GDPRv:

- the rights to information and access to personal data, the right to rectification and the right to object to direct marketing ; and
- under certain conditions, the right to erasure, the right to restriction of processing, the right to data portability, the right to object (other than to direct marketing), and the right not to be subject to automated individual decision-making, including profiling.

Cookies

How is the use of cookies regulated?

In accordance with Article 4(3)(e) of the Luxembourg e-Privacy Act, as modified, the general rule is that the use of cookies is permitted to the extent that consent was obtained from the subscriber or user after having been provided with clear and complete information. By way of exception, such consent and prior information is not required for cookies that are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
- strictly necessary to provide the requested service.

Examples are cookies for shopping carts or which store language preferences (provided the storage period is no more than the session or a couple of hours thereafter).

Consent need not be obtained through, for example, a pop-up box, but can also be obtained through some other positive act. For example, by continuing to browse after the appearance of an information bar indicating that to do so will result in cookies being placed, which cookies, the purpose thereof and by whom. The cookies may not be placed before a user has performed the requisite positive act (at the time of his/her first visit). As a general rule, a failure to amend default browser settings allowing cookies cannot be viewed as the expression of an informed, conscious choice by the internet user and will not readily be seen as consent. Where the default browser settings do not allow cookies, the Luxembourg e-Privacy Act, as modified, explicitly permits consent to be expressed by appropriate browser or other application settings.

Furthermore, it should be noted that to the extent personal data are being processed, the provisions of the GDPR will equally apply and impose additional obligations (eg, additional information obligation, third-country transfer restrictions, etc).

Lastly, for completeness's sake, reference is made to the pending EU e-Privacy Regulation, which requires an explicit consent for the use of cookies and provides for the additional exception ground of cookies being necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end user.

Data breach

What rules and standards govern digital operators' response to data breaches? Are they subject to any notification requirements in the event of a data breach? What precautionary measures should be taken to avoid data breaches?

Pursuant to Articles 33 and 34 of the GDPR, digital operators must, to the extent that they qualify as data controllers, notify:

- the competent supervisory authority without undue delay and in any case within 72 hours of having become aware the data breach, unless the risk of harm to the rights and freedoms of natural persons is unlikely; and
- the concerned data subjects without undue delay in the event of a likely high risk to the rights and freedoms of natural persons.

The information that needs to be included in such notices is explicitly set out in Articles 33 and 34.

So as to avoid any data breaches, digital operators must comply with their obligations under the GDPR and must specifically, to the extent that they qualify as data controllers:

- implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk as set out in Article 32 of the GDPR;
- comply with its data protection impact assessment and prior consultation with the competent supervisory authority obligations pursuant to Articles 35 and 36;
- implement data protection by design and by default procedures and techniques as required under Article 25; and
- ensure that they work only with reliable data processors with whom they conclude data processing agreements in accordance with Article 28(3) that offer, among others, guarantees that the latter will equally implement such appropriate security measures and will provide assistance to the data controller so that it can honour the remainder of its obligations under the GDPR.

Cybersecurity

What cybersecurity regulations and/or standards apply to the conduct of digital business?

In relation to providers of online search engines, online marketplaces and cloud computing services, the EU Directive on the Security of Network and Information Systems (NIS Directive, EU 2016/1148), which is yet to be transposed into Luxembourg law, sets out requirements in terms of security measures (for preventing risks, ensuring security of network and information systems and handlings incidents) and notification of serious incidents to the relevant national authorities.

Furthermore, provided that any digital business activity implies the processing of personal data, appropriate technical and organisational measures to ensure a level of security appropriate to the risk should be implemented (Article 32 of the GDPR). Such measures should, as appropriate, include:

- pseudonymisation and encryption;
- measures ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- measures ensuring the timely restoration of availability and access to personal data after an incident; and
- measures ensuring a process for regularly auditing the effectiveness of the security measures.

In this context, it is commendable to adhere to the ISO 27K norms.

Is cybersecurity insurance available and commonly purchased?

Yes, cybersecurity insurance is available, but the number of providers is still limited – although no official data exists as to how commonly it is purchased. The Luxembourg authorities encourage insurance companies to create more specific products in the area of cyber insurance, such as probe services and products (intrusion detection systems).

Encryption

Are there regulations or restrictions on the use of encryption?

Yes. Article 3 of the Luxembourg e-Commerce Act, as modified, states that the use of encryption techniques is free. Encryption of personal data is one of the security measures mentioned in the GDPR to be implemented by both data

controllers and processors taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Furthermore, encryption is prescribed by certain Luxembourg financial regulations as a security technique to be used by financial service providers (eg, CSSF Circular 17/654 on IT outsourcing relying on a cloud computing infrastructure).

Government interception/retention

What rules and procedures govern the authorities' interception of communications and access to consumer data?

Article 4(3)(b) of the Luxembourg e-Privacy Act, as modified, provides for an exception to the general prohibition of any kind of interception or surveillance of communications without the consent of the user for the following authorities/bodies: judicial authorities acting within the powers attributed to them by law and those legal inquiry authorities competent for safeguarding the security of the state, the defence, the public interest and for the prevention, investigation, establishment and prosecution of criminal offences.

Access to consumer data by the authorities qualifies as processing of personal data by such authorities, which is allowed only to the extent that one of the legal bases mentioned in the GDPR can be relied upon. This is the case where the processing is necessary for:

- compliance with a legal obligation;
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- the purposes of a legitimate interest (accepted for anti-money laundering processing).

The legal basis for the first two cases requires a specific provision in union law or member state law. Moreover, any such processing must be compliant with all obligations under and principles enshrined in the GDPR.

Advertising and marketing

Regulation

What rules govern digital advertising and marketing in your jurisdiction?

In a business-to-consumer (B2C) and business-to-business (B2B) context, Chapter IV (Commercial Communications) of the Luxembourg e-Commerce Act, as modified, imposes an obligation of transparency in relation to commercial communications and sets out restrictions on unsolicited commercial communications.

In a B2C and B2B context, Chapter II of the Luxembourg Advertising Act prohibits misleading advertising and restricts comparative advertising.

In a B2C context, Articles L.224-4 and 5 (advertising in relation to consumer credits) and Articles L.226-5 and 6 (advertising in relation to mortgages) of the Luxembourg Consumer Code, as modified, apply.

Are there any specific regulations governing the use of targeted advertising?

To the extent that such targeted advertising qualifies as an unsolicited commercial communication, whereby 'commercial communication' is defined broadly as "any form of communication designed to promote directly or indirectly the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession", the following rules set out in Article 48 of the Luxembourg e-Commerce Act, as modified, must be respected:

- General rule: opt-in (explicit, specific prior consent needed), with right to withdraw consent afterwards (to be included in each communication), free of charge (using at least the same communication means);
- Exceptions:
    - o existing clients: opt-out (no consent needed, with a right to request to no longer receive the emails); if
    - o the electronic contact data was acquired in the context of the sale of a product or service;
    - o information is sent about similar products or services offered by the seller; and
    - o at the time the contact data was acquired, the customer was clearly and expressly offered the opportunity to object easily and free of charge; and

o a similar opportunity to object (free of charge) is offered in each communication sent, and using at least the same communication means; and

• No prior consent if message sent to a business, using an impersonal address (eg, info@xxx.com).

Furthermore, the sending of targeted advertising implies the processing of personal data, leading to the applicability of the EU General Data Protection Regulation (2016/679) (GDPR), which provides for additional rights for data subjects that form the subject of 'direct marketing', which includes targeted advertising.

Restrictions

Are there any restrictions or limitations on goods and services that can be advertised, marketed and sold online?

Yes. Pursuant to Article 50 of the Luxembourg e-Commerce Act the following types of contract may not be concluded electronically:

• contracts that create/transfer real estate ownership (for now, this requires the passing of an authentic act with a wet-ink signature before the notary, although an imminent law proposal may change that in the near future);
• contracts requiring by law the involvement of courts, public authorities or professionals exercising public authority;
• contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession; and
• contracts governed by family law or by the law of succession.

The following acts, among others, are also forbidden:

• marketing and sale of all signs and symbols that might provoke a rebellion or any trouble to the public order (Article 274-1 of the Luxembourg Criminal Code, as modified);
• advertisement of weapons; and
• in the context of the protection of minors (under 16 years of age), advertisement of indecent objects or activities that are considered to be troubling to their imagination (eg, violence, sexual content, etc) (Article 385bis of the Luxembourg Criminal Code, as modified).

Lastly, the marketing and sale of the following goods, among others, is subject to limitations (prior authorisation) or can even be prohibited in relation to minors: alcohol, tobacco and medicinal products.

Spam messages

What rules and restrictions govern the sending of spam messages?

The following rules set out in Article 48 of the Luxembourg e-Commerce Act, as modified, must be respected:

• General rule: opt-in (explicit, specific prior consent needed), with right to withdraw consent afterwards (to be included in each communication), free of charge (using at least the same communication means).
• Exceptions:

• Existing clients: opt-out (no consent needed, with a right to request to no longer receive the emails); if
• the electronic contact data was acquired in the context of the sale of a product or service;
• information is sent about similar products or services offered by the seller; and
• at the time the contact data was acquired, the customer was clearly and expressly offered the opportunity to object easily and free of charge; and
• a similar opportunity to object (free of charge) is offered in each communication sent, and using at least the same communication means.
• No prior consent if message sent to a business, using an impersonal address (eg, info@xxx.com).

Furthermore, the sending of spam messages implies the processing of personal data, leading to the applicability of the GDPR, which provides for additional rights for data subjects that receive direct marketing, whereby spam messages are likely to form such direct marketing. 'Direct marketing' is defined by the Council of Europe as:

all activities which make it possible to offer goods or services or to transmit any other messages to a segment of

the population by post, telephone or other direct means aimed at informing or soliciting a response from the data subject as well as any service ancillary thereto.

This may cover spam messages.

Digital content and IP issues

Required notices

Are websites and any other digital content required to display certain legal notices or other information in your jurisdiction?

Yes, pursuant to Article 5 of the Luxembourg e-Commerce Act, as modified, the provider of the information society service must render easily, directly and permanently accessible to the recipient of the service and competent authorities, the following information:

- its name, geographic address and contact details, including its email address, which will allow it to be contacted rapidly and communicated with in a direct and effective manner;
- as the case may be, its Luxembourg trade register number, value-added tax number and the authorisation it holds for exercising its activities, as well as the particulars of the relevant authority having granted such authorisation; and
- as concerns regulated professions:

- any professional body or similar institution with which the service provider is registered;
- the professional title and the member state where it has been granted; and
- a reference to the applicable professional rules in the member state of establishment and the means to access them.

Where the concerned information society service(s) refer(s) to prices or terms of sale/service delivery, these are to be indicated clearly and unambiguously. Whether the prices are inclusive of any taxes and additional costs must be stated clearly.

Lastly, in a business-to-consumer context more information needs to be provided pursuant to the Luxembourg Consumer Code, as modified, and this both in general (Articles L. 111-1 and 112-1 to 8 of the Luxembourg Consumer Code) and in the event of an actual contract closure.

Liability for content

What rules govern liability for online or other digital content that is defamatory or infringes another party's IP rights?

Such actions can be subject to both civil and criminal liability in accordance with the principles of general tort law set out in Article 1382 of the Luxembourg Civil Code, as modified, and/or the regulations of the concerned IP rights that are being infringed (respectively, Articles 443 to 452 of the Luxembourg Criminal Code, as modified, on defamation).

How can liability be excluded or limited?

Under Luxembourg law, limitation or exclusion of liability clauses are valid to the extent that they:

- do not erode the effects of the contract or do not tarnish one of its essential obligations (meaning that they do not deprive the contract of its essence);
- do not exclude an obligation of mandatory Luxembourg law (eg, the warranty of the seller for hidden defects); and
- do not exclude and/or limit liability for death or bodily harm or for wilful intent or personal fraud.

Which parties can be held liable for defamatory or infringing content? Can contingent liability be extended to internet service providers (ISPs)?

Pursuant to Article 21 of the Luxembourg Freedom of Expression in the Media Act, as modified, the criminal and civil responsibility for any fault committed via the media, such as defamatory or infringing content published online,

lies in principle with the contributor, and in the event that such contributor is unknown, with the editor and, in the event that such editor is unknown, with the broadcaster. Such liability is however not absolute and both the Luxembourg Freedom of Expression in the Media Act, as modified, itself and Article 443 of the Luxembourg Criminal Code, as modified, foresee certain limitations.

The definition of 'broadcaster' contained in Article 3(2) of the Luxembourg Freedom of Expression in the Media Act, as modified, is very broad and includes any information society service providers, such as ISPs. Furthermore, the notion of 'broadcaster' specifically includes online intermediaries that perform "mere conduit", "caching" or "hosting" services in accordance with Articles 60 to 62 of the Luxembourg e-Commerce Act, as modified. Nevertheless, the latter online intermediaries cannot be held liable if the strict conditions mentioned in the law are met.

Content takedowns

What rules and procedures govern content takedowns? Can ISPs remove defamatory or infringing content without permission?

Within the context of a criminal procedure, content takedowns may be requested and granted in accordance with Articles 75 and 76 of the Luxembourg Freedom of Expression in the Media Act, as modified. ISPs are nonetheless free to remove defamatory or infringing content without permission, provided that they safeguard freedom of expression too, in order to avoid any claims in response. Online intermediaries providing hosting services should act expeditiously to remove or disable access to the information in question in order to benefit from the exclusion of liability foreseen in Article 62 of the Luxembourg e-Commerce Act, as modified, upon obtaining actual knowledge or awareness of illegal activities.

Domain names

What rules, restrictions and procedures govern the licensing of domain names?

The top domain name '.lu' is managed by DNS Luxembourg, which accredits registrars from which a registration of a '.lu' domain name can be obtained. More information can be found at https://www.dns.lu/en/.

Domain name registrations must respect the principles set out by the Internet Corporation for Assigned Names and Numbers (ICANN), meaning that, among other things, they should not be identical or confusingly similar to trademarks or service marks in which another person has rights.

How are domain name disputes resolved in your jurisdiction?

Domain name disputes are typically resolved via:

- the
- set up by ICANN, whereby the claimant must prove that:

  - o the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which it has rights;
  - o the respondent has no rights or legitimate interests in respect of the domain name that is the subject of the complaint; and
  - o the domain name was registered and is being used in bad faith; or

- ordinary court proceedings, meaning before a district court at first instance, where the following grounds are typically invoked:

  - o trademark infringement if the domain name is also a registered trademark;
  - o domain name grabbing constituting a fault pursuant to general tort law (Article 1382 of the Luxembourg Civil Code); or
  - o trade name protection and possibly copyright protection of the trade name.

For '.lu' domain names, there is also an additional procedure that allows to freeze the transfer of '.lu' domain names if a valid court action has been brought against the '.lu' domain name holder.

IP protection measures

What special measures and safeguards should rights holders consider in protecting

their online/digital content?

Rights holders should ensure that:

• their rights are acknowledged, either by advertsing the intellectual property's protected status of the content, or making sure that it is mentioned (eg, copyright symbol and explicit clause in the disclaimer). It may also be worthwhile making use of the i-depot procedure of the Benelux Office for Intellectual Property and logging relevant ideas, especially in relation to unregistered IP rights such as copyright, in order to be able to prove later on that they created, devised or designed it; and

• sufficient security measures are in place in connection with the website or online space in which the content is available.

Tax issues

Online sales

How are online sales taxed?

Profits derived from a digital business activity should be subject to taxation in Luxembourg based on ordinary tax rules – that is, the company carrying out the online sales activity is subject to Luxembourg corporate income taxation if it is resident in Luxembourg or if it has a Luxembourg permanent establishment to which the sales can be attributed. In this respect, an IT server could, in principle and depending on how essential and significant the activities performed through the servers are, constitute a permanent establishment to the extent that it is at the free disposal of the company for reaching out to its consumers and it is physically located in a fixed place in the relevant jurisdiction (in this case, Luxembourg).

Other taxes

What other tax liabilities arise in respect of the conduct of digital business in your jurisdiction?

The conduct of a digital business activity could be subject to Luxembourg indirect tax. The value-added tax (VAT) regime applicable to online sales depends on several factors:

• what is offered by the company carrying the digital business (ie, products or services);
• the nature of the buyer (VAT registered or not);
• the location of the parties to the sale; and
• the overrun of specific thresholds.

For instance, if a company non-resident in Luxembourg reaches a turnover of €100,000 in relation to the sale of products to Luxembourg individual consumers, such company should be registered in Luxembourg for VAT purposes and should be liable to Luxembourg VAT.

Jurisdiction, governing law and dispute resolution

Jurisdiction and governing law

How do the courts determine jurisdiction and governing law in relation to online/digital transactions and disputes?

The rules set out in the EU Rome I, Rome II and Brussels 1bis Regulations (593/2008, 864/2007 and 1215/2012, respectively) apply.

If the dispute takes places in a contractual context:

• in the event of a choice of law and jurisdiction clause, the courts will respect the chosen jurisdiction and governing law. In a business-to-consumer (B2C) context, such choice is however limited in the following way:

o governing law: the chosen law cannot deprive the Luxembourg resident consumer of the protection afforded to him/her by provisions that cannot be derogated from by agreement under Luxembourg law, especially when it comes to Luxembourg provisions on unfair terms in consumers contracts, which are stricter than those in other EU

member states;

o jurisdiction: Luxembourg resident consumers may always bring proceedings against the trader in the courts of the country of his/her habitual residence; moreover proceedings against a Luxembourg resident consumer may also only be brought by the trader in such country's courts and any jurisdiction choice deviating from the above is only valid after a dispute has arisen;

• if there is no choice of law and jurisdiction clause, the following rules will apply:

o governing law:

in a business-to-business (B2B) context: for sale of goods, the law of the country where the seller has its habitual residence; for provision of services, the law of the country where the service provider has his habitual residence; and
in a B2C context: the law of the country where the consumer has his/her habitual residence provided that the professional pursues its activities in such country or by any means directs such activities to such country (among others);

o jurisdiction:

in a B2B context: the courts of the member state in which the person that is being sued is domiciled or in the courts of the member state of the place of performance of the obligation in question; and
in a B2C context: the consumer may be brought only before the courts of the member state where he/she is domiciled; the consumer may choose between his/her domicile or that of the trader.

If the dispute takes place in a non-contractual context:

• governing law: in principle the law of the member state where the damage occurs, but for IP infringements, it is the law of the member state for which protection is claimed; and
• jurisdiction: the courts of the member state in which the person that is being sued is domiciled or in the courts of the member state where the harmful event occurs or may occur.

Courts

Are there any specialist courts in your jurisdiction which deal with online/digital issues and disputes?

No, online/digital issues and disputes are dealt with by the ordinary courts, meaning at first instance by a district court, certain chambers of which deal exclusively with commercial matters.

Alternative dispute resolution

What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

The following ADR mechanisms are available and are increasingly relied upon for online/digital disputes:

• The national service of the Consumer Mediator: This free-of-charge ADR mechanism is available for disputes in relation to sales contracts or service contracts and can be initiated by both consumers residing in Luxembourg or in another member state faced with a dispute against a Luxembourg trader, and Luxembourg traders.
• The Centre for Civil and Commercial Mediation: This mediation service is open to all types of dispute, whereby the remuneration of the mediator (fixed hourly rate) and the costs of the mediation are in principle carried equally by both parties.
• The EU Online Dispute Resolution Platform: This platform can be used by both traders and consumers for the resolution, by an independent dispute resolution body, of disputes in relation to goods/services purchased/sold online.

Law stated date

Correct as of

Please state the date of which the law stated here is accurate.

1 June 2018.