

The regulation of Digital Trade

Key policies and international trends

Lillyana Daza Jaller

Simon Gaillard

Martín Molinuevo

Contents

- Contents..... 1
- 1. Introduction 2
- 2. Building the regulatory framework for digital markets 4
 - a) Regulating remote electronic transactions..... 5
 - i. Electronic documentation..... 5
 - ii. E-signature 8
 - b) Trust-building regulation 12
 - i. Consumer protection 13
 - ii. Intermediary liability..... 21
 - iii. Privacy and data protection..... 24
 - iv. Cybersecurity 28
 - c) Regulatory restrictions to digital trade..... 30
 - i. Ban of online sales 30
 - ii. Regulations on cross-border data flows 31
- 3. Concluding observations..... 38
- Bibliography 39
- Annexes..... 0
 - Annex 1:** Cross-country Comparisons of the Implementation of OECD Recommendation on Information Disclosure..... 0
 - Annex 2:** Cross-country Comparison on the Three Main Features of the Right of Withdrawal 1
 - Annex 3:** Cross-country Comparisons of the Implementation of OECD Recommendation on Data Privacy Principles 2

1. Introduction

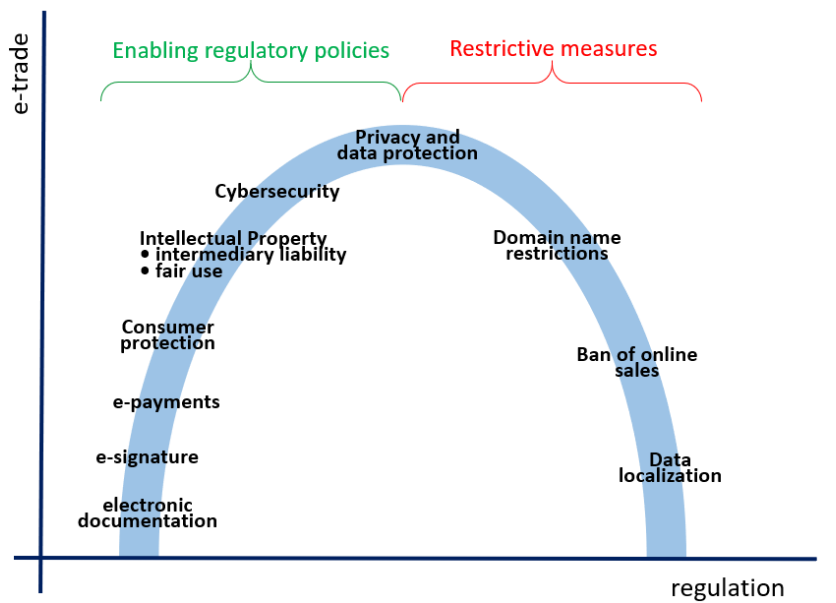
One day, people will wonder how global trade was even possible with before goods and services were bought and sold in global digital markets without regard or even knowledge of where sellers and buyers where located. We are not there yet --not by a long shot. For now, digital trade remains segmented mostly along national and regional boundaries, due largely to a combination of lack of consumer trust in online transactions and regulatory differences across borders, as well as the inherent challenges of moving goods internationally.

Regulation plays a central role in building the foundations of digital markets. It can provide the legal tools necessary for remote contracts, clarify the rights and obligations of the multiple actors involved in digital transactions, and establish a framework that promotes consumer trust in digital markets, even when the consumer does not know the merchant or when the merchant is in a different country.

However, regulation can also further segment digital trade, de facto restricting digital transactions to within national boundaries, or allowing for cross-border transactions with some partners to flourish, while limiting others. This can be the intended result of regulatory measures that limit cross-border data flows or online purchases or may be the undesired effect of regulatory differences across countries that leads businesses to offer different goods and services across boundaries.

Digital trade encompasses a broad variety of activities, ranging from renting a room in a foreign country through a mobile phone app, ordering a piece a jewelry online from an artisan across the world, obtaining satellite data on soil composition for mining, or a retailing firm replenishing its stock from a foreign vendor through automated, computer-to-computer, communication. All these activities entail a commercial transaction performed, normally remotely, through electronic means¹.

Figure 1: Domestic regulation can foster or hinder digital trade



The wide range of different goods and services that can be traded electronically, together with the novel nature of the technologies that allow for these transactions, make it so that there is no single, neatly defined, body of legislation or regulation that governs e-trade.

Instead, the regulation of digital markets is a patchwork of regulatory solutions from different policy areas. Broadly speaking, the regulation of e-trade entails elements of contract law, in particular

¹ Similarly to OECD (2011), we understand e-trade to refer to the sale of goods and services through digital networks, with the exclusion of orders made by telephone calls, facsimile or manually typed e-mail.

Regulation for Digital Markets

regarding electronic documentation and signatures, financial law in what relates to e-payments, consumer protection, intellectual property, cybersecurity, personal privacy, and data protection. A conducive regulatory framework in each of these policy areas is necessary for vibrant digital markets. However, specific restrictive measures within these areas may undermine e-trade, for example by unnecessarily curbing the types of goods that can be traded remotely, or by limiting the cross-border flows of data that underpin e-trade transactions.

Laws and regulations can hence either foster or hinder digital trade (Figure 1). Regulation can play three different roles for digital markets. First, it can provide essential regulatory tools for remote transactions, such as electronic documents and signatures, as well as electronic payments; secondly, it can improve the conditions for trust in digital markets, by ensuring that consumers are protected and that their information is safe and remains private, hence increasing reliance and bringing new actors to digital transactions. A strong regulatory framework on these pillars can be associated with the expansion of digital trade –represented on the upward part of the slope in Figure 1. Yet, third, regulations can also introduce restrictions that hamper the conditions for digital markets. Restricting the types of goods and services that can be bought online, limiting or increasing costs for the transfer of data—which is necessary for the transactions—, or creating burdensome conditions for online marketplaces, platforms, and services providers, ultimately limits the offer of goods and services in digital markets.

In what follows, this study reviews the main policy areas that build the regulatory framework for digital markets. The paper reviews domestic legislation and, where available, international guidelines with a view to highlighting the key policy and regulatory concerns in each area, and to identifying regulatory models implemented around the world that may offer guidance for recommendations for policymakers. The study is organized in two sections:

- The first section addresses measures that seek to facilitate electronic transactions and promote trust in digital markets. In particular, this section addresses regulation on e-documents and e-signatures, consumer protection, intermediary liability, privacy and data protection, and cybersecurity.
- The second section looks into common regulatory restrictions in digital markets, including the ban of online sales and regulations on cross-border data flows. Although these measures often pursue public policy objectives, they inherently entail restrictions to digital trade that need to be taken into account, and less restrictive alternatives could achieve such goals with fewer negative implications on digital trade.

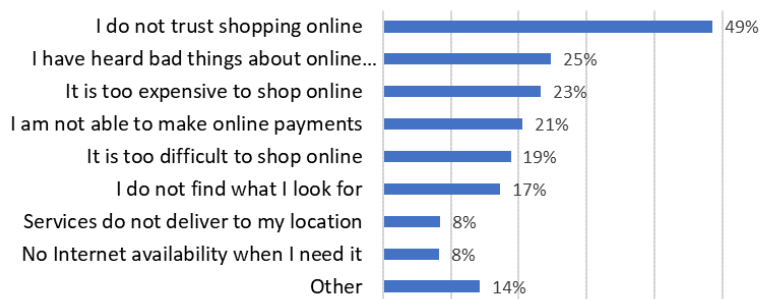
These different regulatory areas have in common that, taken together, they offer a set of basic rules that create tools for remote transactions (e-document and e-signature) or clarify conditions of digital transactions that enhance consumers' and businesses' trust (online consumer protection; data governance and cybersecurity). Importantly, there are a number of additional policies relevant to digital trade that are not covered in the current study: regulations related to competition policy, taxation, intellectual property, as well as the conditions for business licenses can also make or break a conducive framework for digital businesses.

2. Building the regulatory framework for digital markets

Online transactions remain a relatively new phenomenon, and one that has yet to gain the trust of most people. Lack of trust in online transactions remains in fact the main reason in middle- and high-income economies worldwide for not shopping online.

Basic regulations such as e-documents and e-signatures provide tools for e-commerce such as facilitating document recognition and expediting processes. Additionally, regulations to protect individual rights with regard to their private data can increase consumer trust on the internet. The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent economies from enjoying all the benefits of e-commerce. Finally, certain regulations can provide additional tools for law enforcement, allowing governments to be able to better protect their citizens' rights.

Figure 2. Lack of trust the top reason for not purchasing goods and services online



Source: 2017 CIGI-Ipsos Global Survey on Internet Security and Trust

Amongst the challenges faced by policymakers in the digital sphere is the very nascent nature of regulation regarding online activity. UNCTAD Global Cyberlaw Tracker maps countries that have adopted laws regarding electronic transactions, consumer protection, and data privacy. In particular, it recognizes that, out of 194 countries, 79 percent have adopted “e-transactions law”, 52 percent feature consumer protection laws, 58 percent, privacy laws, and 72 percent, cybercrime laws. Yet, despite these substantial figures, modern and comprehensive regulatory frameworks for digital markets remain elusive, found almost exclusively in developed countries. A closer examination of domestic legislation around the world, suggests that having an “e-commerce law” of similarly titled instruments is not necessarily indicative of the soundness of the country’s regulation on digital trade. Many countries’ regulation on privacy dates back to the 1980s, before the digital revolution, thus featuring inadequate provisions for the challenges of data privacy. Further, one country may include online transactions in their civil code’s strict rules regarding consumer protection, while another has a specific online consumer protection law in place which in fact has no teeth. Additionally, legislation with a tittle along the lines of “E-commerce Law” can include a broad range of provisions, from simply recognizing the use of e-documents, to providing a clear framework for companies and governments to protect individual rights of consumers in e-commerce. A sound assessment of the country’s framework requires thus a review of the content of a range of regulatory instruments and a specific evaluation of the solutions that they offer for digital markets.

a) Regulating remote electronic transactions

The legal recognition of electronic documents and signatures as adequate tools for remote transactions is a key step in building a thriving digital market. As communication technologies connect people and businesses around the world with increasing ease and convenience, businesses engaged in digital trade also expand their network of clients and suppliers across borders. Ensuring that electronic documents and signatures are fully recognized and can be enforced is therefore an essential regulatory step to allow for remote electronic contracts and transactions.

A strong and reliable framework for e-documents and e-signatures is particularly important for business-to-business (B2B) transactions. Transactions by final consumers, such as those on e-commerce platforms like Aliababa, Souq.com, or Jumia and app-based services like Airbnb, do not typically entail major documentation exchanges and can be concluded even without a specific regulatory framework for electronic transactions. However, for business relations that require a degree of customization of the products and services and that are provided over time, such as those that allow suppliers to connect to global value chains and/or services that require peripatetic delivery over extended contract periods, the ability to conclude a contract or amend its terms remotely in a secure and reliable manner is a key step towards engaging in business-to-business digital trade.

i. Electronic documentation

A strong framework for electronic transactions, providing for the legal recognition of electronic documents and signatures, is a key step in building a thriving digital market. As communication technologies connect people and businesses around the world with increasing ease and convenience, businesses engaged in digital trade also expand their network of clients and suppliers across borders. A conducive regulatory framework for digital trade should hence guarantee that contracts concluded remotely through electronic channels are valid and legally enforceable just as those concluded in person.

The requirement of paper invoices and handwritten contracts not only imposes a costly burden on businesses but also reduces the possibility to engage in remote transactions. Yet, some countries maintain to date such statutory requirements, hindering the ability of their firms to engage in digital trade. For instance, some internet platforms allow for the e-commerce transaction to be automatically registered in the recipient’s invoicing system. Firms in countries where invoices and contracts must be kept in paper copies, such as Russia, or Ukraine, are prevented from benefitting from these additional services (NTB, 2012).

Table 1: UNCITRAL recommended principles for electronic documentation

Legal recognition of data messages
Satisfaction of writing requirement
Admissibility & evidential weight
Contract formation & validity
Signature requirement satisfaction
Technological neutrality
Recognition of foreign e-signatures

Source: Authors, based on (UNCITRAL, 1996) and (UNCITRAL, 2001)

Principles

Three principles are widely regarded as the central elements of a modern and sound framework for electronic documents: non-discrimination, functional equivalence, and technological neutrality.

Regulation for Digital Markets

- The principle of **non-discrimination** ensures that a document would not be denied legal effect, validity, or enforceability solely on the grounds that it is in electronic form. This principle is the bare minimum that a regulation on electronic documentation should include. In digital trade, this means that a purely digital transaction, based on the offer of a product or service made online and its terms and conditions declared in digital form, are binding on the parties as if they were declared on a hard document or verbally. In other terms, it recognizes the common-sense condition that communications in digital form have the same legal effect as in other forms of expression.
- The **functional equivalence** principle seeks to ensure that statutory requirements for paper documents are also met by electronic communications that can effectively fulfill the same purpose. In particular, it sets out the specific requirements that electronic communications need to meet to fulfil the same purposes and functions that certain notions in the traditional paper-based system - for example, "writing," "original," "signed," and "record"- seek to achieve. For instance, where a law requires that a contract should be retained in its "original" form, according to the principle of functional equivalence an electronic communication must meet that requirement if there exists reliable assurance as to the integrity of the information it contains from the time it was first generated.
- The principle of **technological neutrality** mandates the adoption of provisions that do not differentiate between the types of technology used. In light of rapid technological advances, neutral rules aim at accommodating any future development without further legislative work. Regulations should hence avoid requiring the use of certain technologies to afford certain legal effects to electronic documents. For instance, a regulation that gives legal recognition only to electronic documents stored under certain cybersecurity measures, such as the E-Transaction Law adopted by Lebanon in 2018, may appear to promote good practices in the use of technology, but risks unnecessarily excluding other communications that are not typically encrypted, such as email or text messages.

International practice

A key enabler for cross-border businesses, the regulation of electronic transactions is one of the few areas of digital regulation with dedicated international guidance and substantive regulatory experience around the world. In fact, regulation on electronic information and signatures can be traced back to the use of the telegraph in the 19th century. UNCITRAL Model Law on Electronic Commerce (MLEC) of 1996 is the international standard on regulation of electronic documents. The main objective of the MLEC is to facilitate remote transactions by establishing rules to allow the electronic equivalent of paper-based documents to be legally recognized, thereby removing obstacles encountered by the use of electronic means. The MLEC promotes the principles of non-discrimination, technological neutrality, and functional equivalence in the treatment of electronic documentation. The principle of non-discrimination is the cornerstone of the regulation, as it ensures that a document would not be denied legal effect, validity, or enforceability solely on the grounds that it is in electronic form.

Box 1 Summary of UNCITRAL's rules for electronic commerce

1. Legal recognition of data messages: information shall not be denied legal effect, validity, or enforceability solely because of its electronic nature. Data messages satisfy legal requirements for a writing, an original, and the retention of documents, records, or information; they are admissible evidence in legal proceedings

Regulation for Digital Markets

2. Signature: e-signatures satisfy legal requirements for a person's signature if the method used identifies the person and indicates approval of the information contained. The method must be appropriate for the purpose of the communication, in light of the circumstances
3. Formation and validity of contracts: a contract shall not be denied validity or enforceability on the sole ground that a data message was used for its formation
4. Recognition by parties of data messages: a declaration of will or other statement shall not be denied legal effect, validity, or enforceability solely because of its electronic nature
5. Attribution of data messages: a data message is that of the originator if it was sent by the originator itself
6. Acknowledgement of receipt: the addressee may acknowledge the receipt of data message through any communication or conduct unless the originator requests otherwise
7. Time and dispatch and receipt of data messages: dispatch takes place when the data message leaves the control of the originator
8. There is a chapter dedicated to actions related to contracts of carriage of goods

Source: **(UNCITRAL, 1996)**

The UNCITRAL MLEC has inspired legislation around the world. UNCITRAL recognizes that legislation based on or influenced by the Model Law has been adopted in 72 States and a total of 151 jurisdictions (UNCITRAL, 2019). In the United States, for example, the Uniform Electronic Transactions Act (UETA) is based primarily on MLEC and adopted by most states; it provides states with a framework law which gives legal validity and admissibility to electronic documents. The federal framework model law prohibits the denial of legal effect or enforceability of a record, signature, or contract on the basis of its electronic form. Where a law requires a record to be in writing, this requirement is satisfied by an electronic record. Where notarization is required, the electronic signature or record of the person authorized to sign the record is sufficient. The use of an electronic agent to enter into a contract is permitted. UETA includes a "mailbox" Rule, which clarifies when a message is considered dispatched and received. Finally, it gives negotiable instruments in the electronic form the status of "transferable records", meaning an e-document may be the authoritative copy of the record.

Canada's Uniform Electronic Commerce Act (UECA) of 1999, also designed to implement the principles of UNCITRAL MLEC, includes a section that gives the power to use electronic documents to create, collect, receive, store, transfer, distribute, or publish documents or information. The government may deem electronic communication to be acceptable where a specific type of communication is statutorily mandated.

Not all countries have incorporated all aspects of the UNCITRAL Model Law. In Middle East and North Africa (MENA), for example, all countries with the exception of Djibouti and Libya, have introduced regulations that follow MLEC principles in recognizing electronic documents as equivalent to paper-based documents.² Israel has done so by including provisions recognizing the general principal of non-discrimination of e-documentation in its legislation on electronic signature. The rest of the countries in the region have instead adopted a more developed framework on e-documents, reflecting in greater detail some of the principles of the UNITRAL MLEC . While a more detailed regulation offers advantages in terms of clarity of the regulation, both approaches do give legal recognition to electronic documents.

² No available data on existing regulation for Libya, Palestine, and Syria.

Regulation for Digital Markets

ii. E-signature

Digital activity involves engaging in remote –often international– contracts on a routine basis, to the point where users are not often aware of its international nature. The ability to conclude legally binding contracts remotely, without the face-to-face interaction of the parties is a central feature of global business. Digital technologies reduce distances by facilitating interaction and collaboration across borders; electronic signature complements that digital proximity by providing a mechanism which grants full legal recognition to any agreement that may be concluded, even at the distance.

Electronic signatures are essential for multiple facets of digital trade:

- **B2C digital trade:** A simple digital interaction like accepting the terms of use of a website or a mobile app (often without even reading the content) by clicking a box entails, in legal terms, the acceptance of a contract through an electronic signature. For the app developer or the supplier of the online service, a legal framework that recognizes such interaction as a legally binding commitment -in other terms, signing on the terms of the contract as a way of accepting them- brings needed certainty to the transaction. Lack of an electronic signature regulation in this context could mean that guests could disregard the conditions set out by homeowners when offering a residence through Airbnb because their electronic acceptance is not considered legally binding.
- **B2B digital trade:** Electronic signatures are particularly important to transactions between firms, especially in the context of a global or regional value chain. While e-commerce transactions by final consumers are typically individual purchases of discrete goods or services that can be satisfied with a simple click on a box, cross-border deals between firms often involve a business relation that extends in time and entails the production and delivery of customized goods or services, whose terms and specifications need to be clearly agreed to in advance. This type of business-to-business (B2B) interaction must be reflected on a distinct, specific contract between the client and supplier, sanctioned with the signature of the parties to accept the agreed terms. For these engagements, the parties may wish to back those digital documents with an electronic signature that provides certain guarantees against tampering or prying by third parties.
- **E-government:** Electronic signature is also essential to facilitate interactions between individuals and firms and the government. Allowing the submission of information through digital channels, for instance for business registration, tax statements, customs documentation, or in administrative or judicial procedures, promotes efficiency, facilitates service delivery, and ultimately reduces costs for government, businesses, and individuals. This type of remote interaction often involves sensitive information. Electronic signatures in this context must not only be secure but must also guarantee that the signature belongs to the individual concerned in that specific activity.

Principles

With the growth of e-commerce around the world, governments have enacted legal instruments to give recognition and legal validity to electronic and digital signatures. While the objective of all these regulations is recognizing some kind of electronic representation as a legally valid signature, three different regulatory models are currently in place (Frederick Fischer, 2001); (Blythe S. , 2011)).

Regulation for Digital Markets

- On one end of the spectrum, the **prescriptive approach** only recognizes one type of e-signature as legally valid –typically, secure digital signatures that have adopted specific encryption mechanism and have been issued following prescribed procedures. This approach was pioneered in the state of Utah, and later replicated in other states in the U.S. and countries around the world, including Bangladesh, Brazil, Malaysia, and Peru (Blythe S. , 2011); (Adobe, 2019)). Proponents of this approach claim that legal certainty is necessary to enhance public trust in e-signatures (Boss, 1999). This level of security can be required in many transactions, especially those involving sharing of information with government authorities, such as on taxation, customs declarations, or personal information. However, while secure digital signatures have the advantage of offering the maximum degree of security, the prescribed technology and procedures is unnecessarily costly and burdensome for many activities, in particular for contracts between private parties. Forcing users to employ secure digital signatures as the only recognized alternative is outweighed by the inconvenience related to the use of such technologies, which includes resorting to certification authorities, and paying a fee to obtain a certificate.
- A “minimalist” or “**permissive**” **approach**, on the contrary, allows parties to choose the technology they prefer, giving any selected technology equal legal validity. The minimalist approach is technology-neutral, which means it leaves the parties to adopt the technology of their choice (for instance, whether the signature is encrypted or not or the type of encryption adopted). The United States’ Electronic Signatures in Global and Commerce Act of 2000 (E-Sign) prohibits the denial of legal effect, validity, or enforceability of an electronic signature due to its nature, affording no presumptions to any specific technology. Supporters of this approach believe that the parties should be able to choose the technology that best suits their needs. However, others find that it does not provide sufficient legal certainty and it raises costs for the parties (Boss 2009). The United States, Canada, Australia, and New Zealand have adopted this approach (AssureSign, 2019). While it affords the greatest liberty to the parties in adopting any type of technology, thus reducing costs, the approach fails to acknowledge that certain technologies are indeed more secure than others and the greater security may be warranted under certain conditions.
- A hybrid or “**two-tiered**” **approach** is a mix between these two, recognizing all technologies as legally valid while giving certain presumptions only to secure digital signatures. Like the prescriptive approach, it describes the requirements of a secure digital signature, and includes rules of conduct regarding the rights and responsibilities of the parties, including the signatory, the certification service provider (CSP), and the relying party. A few countries have further developed this approach to offer greater liberty to private parties to adopt secure digital signatures through technologies of their own preference. While the prescriptive and hybrid models usually include rules of conduct regarding the rights and responsibilities of the parties, including the signatory, the certification service provider (CSP), and the relying party, this is usually absent from legislation adopting the minimalist approach.




International practice

At a minimum, a regulatory framework should recognize that electronic signatures are a legally valid form of accepting an obligation or terms of a document. Further, the framework should also ensure

Regulation for Digital Markets

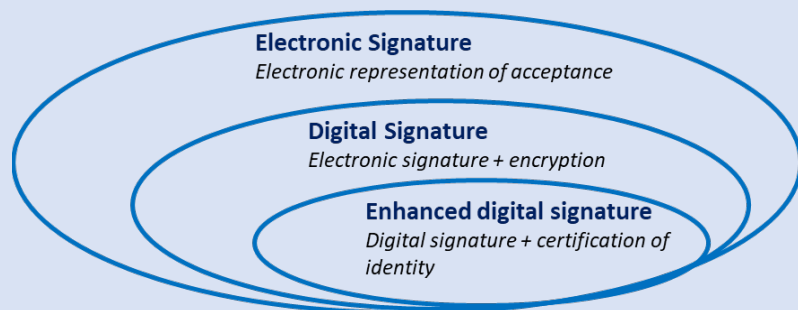
that, when an electronic signature meets certain requirements, it has full recognition of validity and enforceability, just like a handwritten signature.³ The UN Convention on the Use of Electronic Communications in International Contracts provides that e-signatures should satisfy a legal requirement for a signature so long as the e-signature meets certain requirements. The method used to identify the party's intent in respect of the information attached must be either as reliable as appropriate for the purpose of the electronic communication or proven to have fulfilled the requirements. The Convention's scope is limited to contracts between parties whose places of business are in different countries, and it excludes certain transactions, including contracts for family or household purposes and transactions on a regulated exchange.

Box 2: Electronic Signatures vs. Digital Signatures vs Enhanced Digital Signatures

Although the terms electronic signature and digital signature are sometimes used interchangeably, a digital signature is actually a type of electronic signature. An electronic signature is defined by Oxford Dictionaries as "symbols or other data in digital form attached to an electronically transmitted document as verification of the sender's intent to sign the document". In practice, an electronic signature is an electronic representation that the person has agreed to the content of the document, be that in the form of a typed name ("John Lennon"), an image of the person's handwritten signature (), or any other form electronic representation, such as an image () or icon () or simply the clicking of a box with a ✓.

Digital signature is defined as "a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate". Whereas an electronic signature can be created by simply clicking a mouse or tracing a handwritten signature with a finger, digital signatures involve the use of a code or algorithm to sign and validate the authenticity of a document. Unlike electronic signatures, digital signatures come under specific standards and a stringent verification process. A digital signature ensures the integrity of a message. This is achieved through a series of steps. First, the receiver's public key is used to encrypt a random key. This is combined with the encrypted message as well as the digital signature and the authenticated message is transmitted through an unsecured network. Upon receipt, the message is separated from the digital signature and the receiver's private key is used to decrypt it. A temporary digital fingerprint, hashed from the random key, validates the received fingerprint. If the message has not been corrupted during transmission, it is authenticated.

Digital signatures are most commonly created through a technology known as "Public Key Infrastructure" (PKI), which provides a cryptographic key pair that can be shared through a trusted authority. The use of the keys not only encrypts the message so that only the intended recipient can access it, but it also guarantees that the content of the message has not been violated or altered.



³ Handwritten signatures, in addition to being legally valid, are also enforceable as they create the presumption that they were indeed inserted by the designated person (a *rebuttable* presumption, which allows the interested person to show proof, for instance, that the signature had been forged). Electronic signatures can be recognized as legally valid but may or may not be given full enforceability depending on the technology and procedures in use. Typically, only "digital signatures" that use some type of encryption technology are given full enforceability—see Box 1 for further details. An electronic signature that is not fully enforceable would require that the person claiming its validity also provide evidence that such electronic signature was indeed inserted by the designated person.

Regulation for Digital Markets

The mere use of PKI, however, cannot guarantee that the person who sent the message is indeed the person who he/she claims to be. Indeed, one person could be sending secured messages using an alias. To prevent this, an “enhanced digital signature” (or “secure digital signature” in some countries) is a digital signature that belongs to a person whose identity has been verified by a relevant authority. An enhanced digital signature typically involves, in addition the use of a PKI : i) a certificate authority (CA)—typically an IT firm that offers electronic signature technologies, such as DocuSign or Adobe, and has been vetted to issue such certificate—who generates, stores, issues, renews, revokes, and verifies the digital certificates, and ii) a registration authority who verifies the identity of entities before their digital certificates are stored at the CA, which could be a public entity or a private one, depending on the regulation.

UNCITRAL Model Law on Electronic Signatures (MLES) of 2001 provides the standards required for an e-signature to be considered legally equivalent to hand-written signatures. It also lays out basic rules of conduct regarding the responsibilities and liabilities of the parties, including the signatory, the certification service provider (CSP), and the relying party. Any method of creating an electronic signature that satisfies certain requirements satisfies a legal requirement for a signature. If deemed sufficiently reliable, foreign certificates and electronic signatures are recognized regardless of the place of issuance of the certificate, creation or use of the signature, or place of business of the issuer or signatory.

Box 3: Summary of UNCITRAL’s standards for electronic signatures

1. Equal treatment of signature technologies: any method of creating an e-signature that meets the requirements of the applicable law has legal effect
2. Compliance with a requirement for a signature: e-signatures satisfy legal requirements for a person’s signature if the method used is appropriate for the purpose of the communication in light of the circumstances
3. Conduct of the signatory: rules of conduct including reasonable care to avoid unauthorized use of its signature creation data; timely notification of any substantial risk that the data may have been compromised; accuracy and completeness of all material representations by the signatory
4. Conduct of the CSP: rules of conduct including accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle; reasonably accessible means that enable a relying party to obtain necessary information
5. Trustworthiness: factors that determine whether systems, procedures, and human resources used by a CSP are trustworthy. These include financial and human resources; quality of hardware and software systems; procedures for processing of certificates and applications for certificates and retention of records; regulatory and extent of audit by an independent body
6. Conduct of the relying party: rules of conduct including verification of reliability of an e-signature and of the validity, suspension, or revocation of the certificate, where applicable
7. Recognition of foreign certificates and e-signatures: if foreign certificates and e-signatures are deemed reliable according to recognized international standards, they should be recognized

Source: **(UNCITRAL, 2001)**

Modelled after UNCITRAL’s MLES, the hybrid approach has become the preferred method of regulating electronic signatures around the world. In 1998, Singapore introduced the first law of this type, later amending it in 2010 to bring it in line with the UN Convention, and it has become the trend in modern electronic signature regulation, having been adopted by the EU, China, Hong Kong, Japan and South Korea, among many others (Blythe S. , 2011). This approach is preferable as it sets out the use of a specific technology (PKI) and procedures (Certification Services Providers) to ensure that secure digital signatures can indeed guarantee the identity of the signatory and integrity of the content. These specific procedures are required, for instance, for submitting documents to the government.

Regulation for Digital Markets

The procedure for obtaining the “certificate” can limit the use of digital signatures. A digital certificate is necessary for a digital signature because it provides the public key that can be used to validate the private key that is associated with a digital signature. Digital certificates make it possible for digital signatures to be used as a way to authenticate digital information. Digital certificates are typically issued by a certificate authority (CA), which is a trusted third-party entity that issues digital certificates for use by other parties. CAs can be government bodies or private entities, including commercial firms, officially recognized by the government. The smaller the number of certification authorities, the harder it may be to obtain a digital certificate and hence to be able to use a digital signature. Hence, when adopting either a prescriptive or hybrid approach that sets out requirements for a digital signature, the regulation should strive to create a vast network of certification authorities that can issue certificates, minimizing the burden for private parties.

The EU has further elaborated the two-tiered model by allowing for secure signatures backed by private certification authorities. With a view to increasing security while reducing costs of adoption, the EU Electronic Identification and Authentication Services Regulation (eIDAS) of 2016 creates a third category of signature, in between the electronic signature (with minimum requirements and weak legal recognition) and the digital signature (full legal recognition, but burdensome certification procedures). This new category allows private parties to adopt a digital signature that meets all the security requirements of the *secure* digital signature (called “qualified Electronic Signature”) but enjoys greater freedom on the selection of the certification authorities. A similar intermediate step was already present in Singapore’s ETA regulation, which allowed private parties to adopt other commercially available technology or procedures for a secure digital signature to the extent that it can provide security equivalent to the prescribed mechanism.

b) Trust-building regulation

Regulation plays an essential role in bolstering digital markets by promoting trust. As digital markets are still in their infancy, the top reason for not engaging in online purchases, at least in developed markets, remains the lack of trust in remote electronic transactions (Figure 2). Consumers typically have no face-to-face contact with vendors, leading to few “visual cues”, such as location, facilities, and personalized interaction, which helps consumers gauge the retailer or suppliers’ professionalism. In this environment, consumers are asked to disclose sensitive information and personal data either to a retailer, online intermediary, or digital platform. As a result, one important limiting factor in both developed and developing economies is the perception that cross-border online transactions and delivery are less secure, and remedies do not exist for when something goes wrong. (World Economic Forum, 2019).

Three sets of regulations are particularly relevant to promoting consumers’ trust in digital markets:

- An effective framework for *online consumer protection* helps consumers be better informed about the characteristics of the good or services at hand as well as the terms of the transaction, promoting a greater understanding of the conditions of the transaction;
- As consumers are required to provide sensitive personal and financial details, a strong *data governance* regime is essential to give individuals control over their own information;

Regulation for Digital Markets

- Similarly, a *cybersecurity* framework further improves trust by ensuring that firms meet certain minimum technical standards in the protection of their digital information and that illegal access to such data is duly prosecuted and, if needed, penalized.

i. Consumer protection

Online consumer protection is essential to support a global market for digital good and services. Distance shopping presents challenges, such as the inability to assess products in person before confirming a transaction. Online consumer protection laws aim to ensure “a level of protection not less than that afforded in offline commerce” (UNCTAD, 2017) (Bartley Johns, Hoppe, Molinuevo, Nghardsaysone, & Daza Jaller, 2017). To that end, *online* consumer protection builds on the principles and mechanisms of traditional consumer protection regimes, extending and adapting those protections to digital markets, in order to reduce some of the challenges of buying and selling online, such as the rights and obligations involving an electronic transaction, or the way to rescind it if necessary (OECD, 2000).

Principles

The main guiding principles for online consumer protection are recognized in two main international soft-law instruments:

- The UNCTAD Guidelines on Consumer Protection of 1985 (revised 1999 and updated in 2015) include recommendations directed to protecting online consumers and improving transparency in online transactions. The Guidelines also recommend cooperation among countries, including in terms of information exchange and enforcement activities.
- In 2016, the OECD revised its Recommendation on Consumer Protection for E-commerce of 1998, modernizing its approach to fair business practices, information disclosures, payment protections, unsafe products, dispute resolution, enforcement, and education (Box X). In addition, the OECD guidelines embrace further issues, such as non-monetary transactions, digital content products, active consumers, mobile devices, privacy and security risks, payment protection and product safety (UNCTAD, 2017) (see sub-section on Challenges below)

Box 4: General Principles for Consumer Protection for E-commerce from OECD Recommendation

Pre - Purchase

1. Transparent and effective protection: consumers who participate in e-commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce
2. Fair business, advertising and marketing practices: businesses engaged in e-commerce should pay due regard to the interests of consumers and act in accordance with fair business, advertising and marketing practices as well as the general principle of good faith
3. Online disclosures: online disclosures should be clear, accurate, easily accessible and conspicuous so that consumers have information sufficient to make an informed decision regarding a transaction. Online disclosures comprise the following areas of recommendations:
4. Information about the business: businesses engaged in e-commerce with consumers should make readily available information about themselves that is sufficient to allow, at a minimum: i) identification of the business; ii) prompt, easy and effective consumer

Regulation for Digital Markets

communication with the business; iii) appropriate and effective resolution of any disputes that may arise; iv) service of legal process in domestic and cross-border disputes; and v) location of the business

5. Information about the goods and services: businesses engaged in e-commerce with consumers should provide information describing the goods or services offered that is sufficient to enable consumers to make informed decisions regarding a transaction
6. Information about transaction: businesses engaged in e-commerce should provide information about the terms, conditions and costs associated with a transaction that is sufficient to enable consumers to make an informed decision regarding a transaction. Consumers should be able to easily access this information at any stage of the transaction

Purchase

7. Confirmation Process: businesses should ensure that the point at which consumers are asked to confirm a transaction, after which time payment is due or they are otherwise contractually bound, is clear and unambiguous, as should the steps needed to complete the transaction, especially for new payment mechanism

Post - Purchase

8. Dispute resolution and redress: consumers should be provided with meaningful access to fair, easy-to-use, transparent and effective mechanisms to resolve domestic and cross-border e-commerce disputes in a timely manner and obtain redress, as appropriate, without incurring unnecessary cost or burden. These should include out of court mechanisms, such as internal complaints handling and alternative dispute resolution. Subject to applicable law, the use of such out-of-court mechanisms should not prevent consumers from pursuing other forms of dispute resolution and redress. (See below sub-section on online dispute resolution and redress)
9. Privacy and security: businesses should protect consumer privacy by ensuring that their practices relating to the collection and use of consumer data are lawful, transparent and fair, enable consumer participation and choice, and provide reasonable security safeguards. (see section on data privacy)

Other

10. Education, awareness and digital competence: governments and stakeholders should work together to educate consumers, government officials and businesses about e-commerce to foster informed decision making. They should work towards increasing business and consumer awareness of the consumer protection framework that applies to their online activities, including their respective rights and obligations, at domestic and cross-border levels

International practice

Online consumer protection laws are scarce across the globe. According to UNCTAD, 97 countries have enacted such laws. 10 percent have draft legislation, 21 percent no legislation, and 12 percent no available data (UNCTAD, 2019). Given that e-commerce is set to double from 2017 (\$2.3 trillion) to 2020 (\$4.2 trillion) (eMarketer, 2019), laws and regulations need to catch up at a faster pace. For instance, many countries have consumer protection laws but do not grant specific rights to online consumers. In China, article 8 of the Law of the People's Republic of China on Protection Consumers' Rights and Interests states that "consumers are entitled to receive correct information on the commodities they buy and use or on the services they receive.", but this right concerns all types of consumers. The Indian Consumer Protection Act of 1986 protects online consumer rights since 2014, but remains ambiguous (Satyan, 2015). In the Philippines, Act No. 8792 grants online consumers the same legal status as offline

Regulation for Digital Markets

consumers (section 33, c), but falls short in detailing principles and rules. Conversely, some countries have granted specific rights to online consumers, thus following international standards, as exemplified by Uganda below.

These laws are, furthermore, fragmented at the national level. Consumer laws, information laws, contractual laws, etc. may encompass online consumer rights. Among the 97 jurisdictions listed by UNCTAD, some countries provide laws that partly entitle rights for online consumers. In Côte d'Ivoire, for example, the legislation is limited to consumers' rights in their relationships with Internet service providers (ISP).

One particular consideration is whether to establish specific regimes tailored to transactions through e-commerce platforms. Solutions on this area differ widely. For instance, China places extensive responsibilities on e-commerce platforms to the extent that platforms will be held liable if they fail to provide information on offending vendors, whereas the U.S. and EU place more responsibility on users (World Economic Forum, 2019).

According to international guidelines, detailed framework for online consumer protection should include digital-specific protections at all stages of the transaction. Consumer concerns include whether the information they enter online is safe and the conditions for the sale (pre-purchase), whether the goods purchased online will meet their expectations when they arrive (purchase), and whether they are entitled to any remedies if any problems arise during or after the transaction (post-purchase). These can be addressed through regulations addressing information disclosure requirements, the right to withdraw from a transaction, dispute resolution, and redress (Figure 3).



Pre-purchase provisions

Before an online purchase, a major challenge faced by consumers is the inadequacy of information disclosed by businesses. Information disclosure is key for consumers to assess the fairness of a transaction, including that of payment systems, the quality of a product, and the reliability of the seller. Misleading information on total prices, taxes and delivery may impede the use of e-commerce platform (UNCTAD, 2017).

Key focus on “pre-purchase” rules is to bridge information asymmetries between the seller and buyer, especially in the context of transaction where both parties may have little connection with each other. Guidance for the pre-purchase stage focuses hence on offering clear details about the goods and services, the business, and the conditions of transaction. Misleading information on total prices, taxes and delivery may impede the use of e-commerce platform (UNCTAD, 2017). According to the 2016 revised OECD guidelines for consumer protection in e-commerce, online disclosures should include information about the business, about the goods and services, and about the transaction (Figure X) (OECD, 2016). Informed decision making relies on knowledge about price and details about the product or service as well as the terms and conditions of sale, such as payment and delivery and post-purchase rights (OECD, 2018).

Regulation for Digital Markets

The information provided should allow consumers to identify, locate, and easily communicate with the business and to make educated decisions regarding the online transaction. Items of information particularly relevant in the context of digital trade transactions include:

- Identity and address of the merchant
- Product specifications and delivery conditions
- Payment process
- Procedures for complaint, and returns and cancellation (withdrawal)

These information disclosure requirements often include various country-specific elements. In France, for instance, a company engaged in e-commerce must disclose its tax identification number while, in Uganda, a seller must provide membership of any self-regulatory or accreditation body. In Tunisia, the disclosure of the identity, address and phone number of the merchant or the service provider is sufficient. Annex 2 shows the articles in each jurisdiction relating to OECD recommendations on information disclosure. It seems that the level of income does not positively correlate with the degree of stringency.

Purchase provisions

Provisions related to the purchase seek to ensure a transparent and effective conclusion of the transaction. Businesses should ensure that the point at which consumers are asked to confirm a transaction, after which time payment is due or they are otherwise contractually bound, is clear and unambiguous, as should the steps needed to complete the transaction, especially for new payment mechanism.

Post-purchase provisions

Post-purchase guidelines focus on offering consumers solutions in case the good or the service is not satisfactory. This is a central aspect of consumer protection in general and a central tenet for online transactions, where the distance, lack of knowledge of the vendor, and, importantly, the lack of the ability to physically inspect or test product, reduce trust in the transaction. In that context, clear and effective mechanism for canceling transactions, returning goods, and obtaining an adequate remedy (e.g. re-imbusement credit, etc.) are essential to boost trust in digital markets. Key post-purchase solutions include the right of withdrawal, online dispute resolution, and redress.

Right of withdrawal

The right of withdrawal allows consumers to cancel a contract after purchasing a product or services online. The right of withdrawal usually comprises three main features.

- The **information duty** binds businesses to provide the information on the existence of their right of withdrawal. Failing to comply with this requirement may trigger sanctions, such as an extension of the withdrawal period or a liability exemption.
- The **absence of reason** allows consumers to withdraw from contract without providing any reason. This feature is peculiar to online transactions.
- The **withdrawal period**, also known as cooling-off period, entitles the right of consumer to withdraw from contract within a specific timeframe.

Regulation for Digital Markets

The right of withdrawal has different characteristics across jurisdictions because of the variability of those features. For instance, EU regulation (art. 9, Directive 2011/83/EU) grants online consumers the right to withdraw from distance contracts within 14 days. A consumer can withdraw from contract if he does not like the product or has changed his mind. The consumer bears the direct cost of returning the goods, unless the trader agreed to bear it or failed to inform the consumer that he must bear them (art. 14, para. 1). Sichuan, a Chinese province, entitles the right of withdrawal with a cooling-off period of 7 days without giving a reason only if the consumer “made the decision against his own willingness and intention due to incomplete or inaccurate information provided by the operator” (article 10 of the Regulations of Sichuan on Protection of Consumer Rights and Interests). The absence of reason is, in this instance, conditional to the information duty. On average, the cooling-off period across provinces in China varies from 3 to 7 days (Metz & Purnhagen, 2012).

Online dispute resolution

In the event of a dispute between the parties to an online transaction, or the receipt of a defective or nonconforming product, legislation should provide tools for resolution. Traditional judicial mechanisms may not be adequate for dispute resolution when buyers and sellers located in different jurisdictions (UNCITRAL, Technical Notes on Online Dispute Resolution, 2017). Alternative dispute resolution (ADR) mechanisms, such as mediation, conciliation, and arbitration provide solutions to domestic and cross-border disputes (OECD, 2000). Additionally, online dispute resolution mechanisms (ODR), through a public or private platform, offer an inexpensive and speedy procedure to solve disputes between parties to an online transaction (Bartley Johns, Hoppe, Molinuevo, Nghardsaysone, & Daza Jaller, 2017). The OECD recommends implementing ADR mechanisms that do not impose a cost on customers that is disproportionate to the value of the claim at stake (OECD, 2007).

ODR can be described as a mechanism for resolving disputes using electronic communications and other information and communication technology “without the need for physical presence at a meeting or hearing” (UNCITRAL, 2017). E-commerce is a favorable field for the development of ODR given the low value of products sold and the increasing cross-border transactions (Cortés, 2010). ODR requires a technology-based intermediary (the ODR platform), that generates, sends, receives, stores, and exchanges communications to ensure data security. ODR may embrace three principal methods of ADR, namely arbitration, where a neutral third party makes a decision that is binding on the parties; mediation, in which a neutral third party aims at an agreement that is acceptable for the parties; and negotiations between the parties, which does not involve a third party.

Box 5: Advantages of ADR/ODR according to EU Commission

The EU Commission estimates that the overall cost of ineffective redress on the internet cost 0.4% of the EU's GDP in 2010 given that one out of five consumers was displeased with an online purchase. Alternative dispute resolution mechanisms are faster, cheaper and easier to use for consumers than going to court:

- Most disputes submitted to ADR are decided within 90 days.
- The majority of ADR procedures are free of charge for consumers or inexpensive to use (below €50).
- The ADR process is generally simpler compared to court proceedings.

Source: (EC, 2011)

ODR mechanisms, being digital in nature, are also suitable to address cross-border complaints. The e-consumer.gov website is one of the first examples of an international ODR platform focused on cross-border complaints. A partnership between 35 consumer protection agencies, e-consumer.gov helps

Regulation for Digital Markets

consumers and agencies combat international scams. It allows consumers make cross-border fraud complaints in several languages (English, French, German, Korean Japanese, Polish, Spanish, and Turkish) and across many industries (e-commerce, banking, tourism, lottery, etc.). It is also a secured platform hosted by the U.S. Federal Trade Commission for law enforcement to share and access consumer complaints. Under this international ODR platform, complaints are first brought to domestic consumer protection bodies and then they can be submitted to the international platform (ICPEN, n.d.).

Box 6: 2016 Revised OECD Principles on Dispute Resolution and Redress

Principle 43: Consumers should be provided with meaningful access to fair, easy-to-use, transparent and effective mechanisms to resolve domestic and cross-border e-commerce disputes in a timely manner and obtain redress, as appropriate, without incurring unnecessary cost or burden. These should include out-of-court mechanisms, such as internal complaint handling and alternative dispute resolution. Subject to applicable law, the use of such out-of-court mechanisms should not prevent consumers from pursuing other forms of dispute resolution and redress.

Principle 44: The development by businesses of internal complaint handling mechanisms, which enable consumers to informally resolve their complaints directly with businesses, at the earliest possible stage, without charge, should be encouraged.

Principle 45: Consumers should have access to ADR mechanisms, including ODR systems, to facilitate the resolution of claims over e-commerce transactions, with special attention to low value or cross-border transactions. Although such mechanisms may be financially supported in a variety of ways, they should be designed to provide dispute resolution on an objective, impartial, and consistent basis, with individual outcomes independent of influence by those providing financial or other support.

Source: **(OECD, 2016)**

Enforcement of ODR platforms is ensured by either public authorities, business associations, and/or consumer organizations:

- **Public dispute resolution providers**, such as the EU-wide platform for consumers and businesses, offer ODR solutions (European Commission, 2019). Given the multiplicity of languages and countries in the EU, the platform offers an example of an international ODR platform run by a public authority. Under that framework, national regulators are responsible for licensing private ODR mechanisms. Courts have also developed ODR processes, as evidenced by the Hangzhou Internet Court (Box 7).
- **Private dispute resolution providers** can settle their own ODR. The World Intellectual Property Organization, for instance, offers an arbitration and mediation center for domain name dispute resolution (WIPO, 2019). Square Trade is the preferred private ODR used by eBay (SquareTrade, 2019). It has been particularly successful due to the large number of similar and simple disputes easing the recognition of patterns of comparable disputes and their matching with proposed resolutions.

Regardless of the type of organization, there is binding enforcement of the ODR outcome. If parties cannot reach an agreement, one will most likely sue another at a traditional court even if it is deemed disproportionate to the values in dispute (Ortolani, 2016).

Box 7: Example of the Hangzhou Internet Court

Regulation for Digital Markets

The Court of Hangzhou in China, released in 2017, is an internet court for online shopping contract disputes, online shopping product liability disputes, online service contract disputes, loan contract disputes and online copyright disputes. The portal is in Mandarin and English. The method used is mediation. The process differs slightly from the general guidelines of UNCITRAL, as the parties engage directly in the facilitated settlement:

- 1) Filing: registration and name certification, as well as complaint completion. After the user is authorized, the system supports the investigation of e-commerce, transactions, logistics, micro-credit, intellectual property, and other information
- 2) Mediation: after the case is filed, the first pre-litigation mediation takes place. Within fifteen days, the mediator contacts the parties, through online, telephone, or video mediation
- 3) Final stage: if the mediation is unsuccessful, the case is formally submitted to the court, where it proceeds to the final decision — including the online payment of litigation costs

Source: **(Hangzhou Internet Court, 2019)**

UNCITRAL laid out general principles for ODR providers (UNCITRAL, Technical Notes on Online Dispute Resolution, 2017). Transparency, the first principle, ensures that any relationship between the ODR administrator and a vendor is disclosed, so that users are informed of potential conflicts of interest. Also, information should be available on the ODR administrator's website in a user-friendly and accessible manner. The second principle is independence. It invites the ODR administrator to adopt a code of ethics for its neutrals, in order to guide them as to conflicts of interest and other rules of conduct, and to adopt policies to mitigate conflicts of interest. Expertise is the third principle, which invites the ODR administrator to implement policies on the selection and training of neutrals so that they conform with the standards set by the administrator. Lastly, explicit and informed consent, the fourth principle, should give the basis for an ODR process.

Challenges ahead

The boom of cross border digital trade is bringing new challenges to consumer dispute resolution mechanisms. Engaging in legal actions is not practical given the multiplicity of jurisdictions and laws involved. Parties may be incentivized to use out-of-court mechanisms to dodge discordant legislations.

However, cross-border cooperation between national bodies is rather limited. E-consumer.gov offers multi-lingual services with adequate information on national law on consumer protection. In addition, consumer protection authorities do not have the authority to investigate in foreign jurisdictions if a citizen reports a problem with an international seller (Schmitz & Rule, 2017). The EU offers an interesting case of a regional centralized ODR system along with authorized national ODRs.

Also, online consumer protection regulations need to constantly evolve to adapt to new technologies, behaviors, processes, and markets. For instance, the development of mobile devices may reduce the effectiveness of information disclosure since information is provided in small font and/or in scrolling text boxes. With smaller screens, limited storage capacity and battery life, mobile devices have reduced capacities to offer adequate information disclosure about the business, the terms and conditions and payments (OECD, 2014).

The OECD points to seven key new developments that will shape the future of online consumer protection (OECD, 2016):

- **Non-monetary transactions:** consumers increasingly acquire “free” goods and services, such as email accounts, in exchange for their personal data. These transactions are now explicitly included in the scope of the Recommendation. Governments and stakeholders are called upon

Regulation for Digital Markets

to consider ways to provide redress to consumers experiencing a problem with such transactions

- **Digital content products:** transactions involving digital content often come with technical or contractual access or usage limitations and many consumers have difficulty understanding their rights and obligations. New language has been added to clarify that consumers should be provided with clear information about such limitations, as well as information on functionality and interoperability
- **Active consumers:** current e-commerce business models increasingly blur the boundaries between consumers and businesses, with consumers playing a participatory role in product promotion and development and entering into transactions with other consumers. The scope of the Recommendation has therefore been broadened and it now encompasses business activities that facilitate consumer-to-consumer transactions. A new provision is added to ensure that consumer endorsements are truthful and transparent
- **Mobile devices:** the growing use of mobile devices for e-commerce brings a number of technical challenges to making information disclosures effective (e.g. on small screens) and can constrain record keeping by consumers. Two new provisions are included to highlight the need to account for the technological limitations or special characteristics of the device used
- **Privacy and security risks:** consumer data is at the core of many e-commerce services and this elevates privacy and security risks. The Recommendation recalls the need to address these risks consistent with other OECD instruments and includes two new provisions highlighting specific protections of particular importance for B2C e-commerce
- **Payment protection:** recognizing that the level of payment protection can vary depending on the type of payment mechanism used, the Recommendation calls on governments and stakeholders to work together to develop minimum levels of consumer protection across payment mechanisms
- **Product safety:** in a number of countries, a range of unsafe products, which have been prohibited from sale or recalled from the offline retail market, are available in e-commerce. A new provision is added to ensure that unsafe products are not offered to consumers online and that businesses cooperate with the relevant authorities to address the problem

Redress

Finally, online consumers should be entitled to redress for the harm suffered as a consequence of goods or services that are defective or do not meet advertised quality criteria (OECD, Consumer Protection in E-commerce: OECD Recommendation, 2016). Redress refers to the compensation for economic harm. Redress can take the form of a monetary remedy (e.g. refund or price reduction) or a conduct remedy with a restorative element (e.g. exchange or repair) (OECD, 2007).

The costs of return usually fall under the customer's responsibility. However, certain conditions may transfer the cost to the business. For instance, when the business did not clearly indicate the costs of return during the purchase of the product. Other factors may be considered, such as the geographical scope and population. Regulations in mainland China do not offer free return to customers because of

Regulation for Digital Markets

the country's size. Conversely, Taiwan's regulations enforce free return due to its relatively small population and territory (Metz & Purnhagen, 2012).

ii. Intermediary liability

The internet's unparalleled ability to connect billions of individuals worldwide has boosted business models based on intermediation between vendors and consumers. E-commerce platforms like Alibaba, eBay, and Mercado Libre are based on offering consumers products from thousands of different providers rather than their own stock. "Gig economy" apps offer services such as rides, lodging, or delivery of food or groceries from firms and individuals. Other services rely on content such as video (YouTube, Vimeo), opinions and reviews of products or services (Yelp, Google), or information (blogs) developed by thousands of users, most of whom remain relatively unknown to the final consumer. The relationship between the intermediary (websites and apps) and the firms or individuals offering their own products or services is hence essential to the functioning of those digital transactions.

Intermediary liability rules are the set of provisions that distribute the liability between intermediaries (website and apps) and actual vendors or content developers when things go wrong. In other terms, intermediary liability is the responsibility that falls upon online intermediaries, such as search engines, application platforms, social networks, and broadband companies, for third-party content featured in, or products and services offered through, their website or apps (Gasser & Schulz, 2015). Just like intermediation is not a novel business model, intermediary liability rules are not new a legal concept – most such rules can be traced back to Roman law. Intermediary liability rules can in fact be broader rules that apply to online intermediaries. However, specific rules of digital intermediaries are more likely to adapt to the particular conditions of digital markets.

Principles

Rules on intermediary liability need to strike a balance between protecting consumer rights and supporting the expansion of digital markets, including through intermediary platforms. While the good, service, or content may be offered or developed by third parties, intermediary platforms benefit from it by building their businesses around it. Digital intermediaries manage the relationship with the customer, and they are often the largest, more sophisticated actor involved in the transaction. As such, regulations can impose on intermediaries (jointly with the third party) liability for fake or faulty products or services, or for offensive or illegal content, transacted through or featured in their services. On the other hand, intermediaries often don't have full knowledge of everything that is being offered by producers and content developers, who have greater control over it.

For digital intermediaries, responsibility may arise mainly from two types of conducts: the offering for sale of counterfeited products, or the publication of unlawful content, such as images or text, by their users. The offering of fake products would normally entail a violation of intellectual property rules (typically trademark protection). Unlawful content can instead run against intellectual property rules when the content is unduly featuring other people's work (a violation of copyright protection) by for instance reproducing music or video without the authors' permission, or it may violate criminal law provisions such as rules against libel, hate speech, or child pornography, the protection of individual privacy or classified information, or amount to *lèse-majesté* crimes.

Typically, rules on online intermediary liability have two components: one attributing responsibility to the intermediary and another reducing its liability by removing the violation ("safe harbor"). For

Regulation for Digital Markets

example, the intermediary would be held liable if it had knowledge that the product being offered was fake but could be exonerated from responsibility if it took steps to remove the product from its listings upon obtaining knowledge of the violation. Rules on responsibility pivot between no responsibility, actual knowledge of the infringement (the platform knew the content was unlawful), duty of knowledge (the platforms should have known that the content was unlawful), or absolute responsibility (the platform is responsible in all conditions). Safe harbor provisions typically involve notice and stay-down procedures, which require that upon receipt of a notice regarding infringing content, the intermediary search and remove all copies of the infringing content and ensure it is not uploaded again (Gasser & Schulz, 2015).

Views on the extent of liability that should be imposed on intermediaries varies greatly between the content industry and the internet industry. Most intermediaries do not have the time or resources to investigate each notification they receive from copyright a holder. As a result, they tend to remove the content upon notice. The American Association of Publishers (AAP) advocates for sanctions imposed on intermediaries for failing to ensure the protection of copyrighted material (USITC, 2017). Content industry representatives claim that the lack of such responsibility leads to an increase in online piracy and decreased revenue for content industries (USITC, 2017). On the other hand, internet industry representatives argue that an increase in intermediary liability is likely to increase costs and limit intermediaries' ability to combat piracy (USITC, 2017). Content industries usually advocate for notice and stay-down provisions, as it has been shown that requiring that intermediaries block websites is ineffective, as the infringing content can be moved by hosts (European Parliament, 2015).

International practice

Rules on liability for digital intermediaries are nascent and still evolving, and a global trend on the topic remains elusive. Even within countries, views on the extent of liability that should be imposed on intermediaries varies greatly between the content industry and the internet industry. Much of this tension is seen in the United States, home to some of the largest internet firms as well as content developers, which has traditionally resulted in strong protections to digital intermediaries, as well as far-reaching disciplines on intellectual property (Holland, et al., 2014). Content industry representatives claim that the lack of intermediary responsibility leads to an increase in online piracy and decreased revenue for content industries, which has led the American Association of Publishers (AAP) to advocate for sanctions imposed on intermediaries for failing to ensure the protection of copyrighted material (USITC, 2017). On the other hand, internet industry representatives argue that an increase in intermediary liability is likely to increase costs and limit intermediaries' ability to combat piracy (USITC, 2017). The U.S. Digital Millennium Copyright Act (DMCA) creates a safe harbor for intermediaries under certain circumstances, including if they unknowingly display, transmit, or store infringing content. Section 230(c) of the Communications Decency Act shields intermediaries from liability for most third-party content. However, when it comes to copyright infringement, they must meet certain conditions, including a notice and takedown requirement.

The EU released a draft directive in 2016, which requires that intermediaries routinely check that they do not host infringing content. In June 2017, Germany passed a law imposing fines of up to €50 million upon online intermediaries who do not remove illegal content within twenty-four hours of notice. Russia's Federal Law No. 187 provides intermediaries with safe harbor protections based on a legal test which determines whether they knew or should have known about infringing content. Content owners

Regulation for Digital Markets

are not required to notify intermediaries about infringing content, and instead may go directly to the courts to request an injunction to block the content.

Seeking to protect online freedom of expression, an international coalition released the Manila Principles for Intermediary Liability (Box 8). The Principles provide governments with standards for censorship and takedown laws which respect the users' rights while promoting innovation.

Box 8: Intermediary Liability guidelines

The Manila Principles for Intermediary Liability were developed to protect online freedom of expression and to provide governments with standards for censorship and takedown laws that respect the users' rights. The effort involved civil society groups from around the world, led by the Electronic Frontier Foundation (EFF, USA), the Centre for Internet and Society (CIS, India), Article 19 (UK), KICTANET (Kenya), Derechos Digitales (Chile), Asociación por los Derechos Civiles (ADC, Argentina) and Open Net (South Korea).

The proposed principles are:

1. *Intermediaries should not be liable for third party content: intermediaries should be exempt from liability for third party content where they did not modify the content; they must not be required to routinely monitor content on their network or platform;*
2. *An order by a judicial authority must be required for content restriction: an order from an independent and impartial judicial authority must be required for content restriction;*
3. *Requests for restrictions of content must be clear, be unambiguous, and follow due process: where an intermediary receives a restriction request before a court order is issued, they need not evaluate the legality of the content; the request must include its legal basis; sanctions should be imposed for bad faith restriction requests;*
4. *Laws and content restrictions orders and practices must comply with necessity and proportionality tests: restrictions should be specific to the content at issue, if applicable, limited in geographical scope; and not extend beyond its duration;*
5. *Laws and content restriction policies and practices must respect due process: parties must be provided the right to be heard and to appeal against restriction orders;*
6. *Transparency and accountability must be built into laws and content restriction policies and practices: applicable rules and transparency reports must be published online in a timely manner.*

Source: (EFF, 2019)

At the international level, some principles on intermediary liability were included in recent trade agreements. The recent Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTTP) and the United States, Mexico, and Canada Agreement (USMCA) set limits to intermediary liability by internet service providers in their intellectual property chapter. Internet service providers are not liable for copyright infringements "that they do not control, initiate, direct, and that take place through systems or networks controlled or operated by them or on their behalf". However, they must remove or disable access to copyright infringing content on their networks upon obtaining knowledge of its existence.

Intermediary liability rules relating to criminal or civil infringement laws are being modernized for the digital environment. The proliferation of fake news in recent years has led countries to seek to reduce the amount of misinformation that citizens can find online. However, this raises concerns about content filtering, freedom of speech, and media manipulation. Singapore, who has been often criticized for its heavy control of the media (Leung, 2019), recently introduced the Protection from Online Falsehoods and Manipulation to hold social media sites liable for third-party content published on their platforms. Noncompliant platforms are subject to fines and imprisonment if they do not remove the

Regulation for Digital Markets

“misinformation” or publish “corrections” next to it. Industry groups fear that this new type of law allows governments to decide what is true or false, endangering the freedom of expression and speech. Following a terrorist attack in a mosque in New Zealand, which was streamed live on Facebook, Australia passed a bill requiring social media platforms to promptly remove abhorrent violent user content shared on their sites. The acts covered by the new law include murder, torture, rape, and kidnapping. Other countries around the world, including France and Germany, are also tackling these issues through legislation.

iii. Privacy and data protection

Consumers are increasingly aware of the value of their personal data. Lack of trust on the way personal data is managed leads consumers away from electronic transactions, limiting the growth of digital markets. At the same time, burdensome regulations on the use and transfer of individual data can build substantial costs for businesses, especially small and medium enterprises. The goal is hence to allow data transfers in a manner that supports the expansion of digital markets, while increasing consumer trust that their private information remains secure and under their control.

Data privacy legal frameworks consist of entitling rights for all or certain types of individuals (also called data subjects) regarding the collection, usage, storage, and disposal of their personal data. They also create obligations for controllers and processors while enacting derogations in certain circumstances (state security, public safety, etc.). Security processes for data controllers (either public or private) ensure the appropriate processing of personal data.

Box 9: How much is personal data worth?

To raise public awareness, the OECD quantified the market price of certain personal data. Using different methodologies, the institution shed light on the revenues made by Facebook and Experian per user. Those companies earn USD 4 to 7 per year per user.

Looking at the market prices for a specific period, the OECD found that companies earn:

- USD 0.5 for a street address,
- USD 2 for a date birth,
- USD 8 for a social security number,
- USD 3 for a driver’s license,
- USD 35 for a military record.

Source: (OECD, **Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, 2013**)

Principles

Several international instruments have been focused on setting out the key principles of data privacy regulation. Asia-Pacific Economic Cooperation (APEC) Privacy Framework of 2015 promotes a flexible approach to privacy protection, with a focus on avoiding the creation of unnecessary barriers to information flows. The Convention “108+” by the Council of Europe is an international human rights treaty focused on data protection, setting out principles that are compatible with the requirements of the European regulation. In 2013, OECD members updated their Guidelines on the Protection of Privacy adopted in 1980 to account for the new reality of digital data flows. The OECD Guidelines declare digital risk an economic risk and they aim to protect privacy and individual liberties with respect to personal data process in the public or private sector. They include eight basic principles for data protection:

Regulation for Digital Markets

- **Collection limitation principle:** limits the collection of personal data and suggests lawful and fair means for collection, as well as consent of the data subject where appropriate
- **Data quality principle:** calls for relevancy of the personal data to the purposes for which they are to be used. Additionally, it calls for data accuracy, completion, and maintenance
- **Purpose specification principle:** data controllers should specify the purpose for which the data are collected no later than at the time of data collection. Subsequent use of the data should be limited to those purposes and the data subject should be notified of any change of purpose
- **Use limitation principle:** limits the use of the data for purposes other than those specified, with the consent of the data subject or by the authority of law
- **Security safeguards principle:** calls for reasonable protection of the data from risks such as loss or unauthorized access, destruction, use, modification, or disclosure of the data
- **Openness principle:** suggests a general policy of openness regarding developments, practices, and policies with respect to personal data
- **Individual participation principle:** the data subject should have the right to request data from a data controller or a confirmation of whether the data controller has personal data relating to the individual. If the data controller has such data, it should be provided to the data subject within a reasonable time, in a reasonable manner and in a form that is readily intelligible to the data subject
- **Accountability principle:** the data controller should be held accountable for abiding with principles of the Guidelines

Box 10: The influence of EU legislation across the world. Example of Argentina.

Argentina was the first country in Latin America to be recognized by the EU for having adequate protection of personal data. Argentina's Personal Data Protection Act of 2000, based on the EU Data Protection Directive, includes general principles related to data protection.

It addresses the legal means of data collection, including the requirement of free, express, and informed consent of the data subject prior to collection. Data collected must be true, accurate, relevant, and it must be updated as necessary. Data may not be used for a purpose that is different or incompatible with that which motivated the collection and the data subject must be provided with express and clear information regarding the purpose for collection. The data must be stored in a manner that allows for the data subject's exercise of the right to access the information. Additionally, the data controller must implement technical and organizational measures necessary to guarantee the security and confidentiality of the personal data.

However, the law includes several exceptions to the general rule that personal information could not be transferred to countries with inadequate levels of data protection and the lack of independence of the supervising authority from the rest of the government. A draft bill updates the old law in certain areas, including the removal of legal entities from the definition of data subjects; the elimination of the duty to register databases; new rules on international transfers of personal data; and an introduction to sections on child consent. Additionally, it proposes the independence of the supervising authority in charge of compliance with data protection from the rest of the government.

Source: (Article 29 Data Protection Working Party, 2002)

Regulation for Digital Markets

International practice

Countries have unevenly embraced data privacy legal frameworks. The 1970s and 1980s saw a surge in personal data protection regulation, with several European countries enacting laws and several international organizations, such as the OECD, enacting instruments addressing the issue. But at the time, regulation arose for large government-owned datasets. Since the 1990s, digital communications led to the collection of massive data from private companies, which led to a new generation of legal frameworks to strengthen personal data protection and consumers' trust. However, while some countries have strived to modernize their privacy frameworks to reflect the challenges of the new digital technologies, many countries lag behind and still rely on broad privacy principles set out in their constitution or elaborated in older privacy laws.

Despite these different approaches, a common objective of data privacy is granting rights to individuals for the protection of personal information (or "personally identifiable information -PII"). However, the definition of PII as well as the grounds under which it may be collected, processed, or shared, remain highly idiosyncratic to each jurisdiction.

Europe has been at the forefront of the most comprehensive (and costly) legislation on data protection. It had a significant impact on other countries' legislation (see box 11). The United States developed a less stringent and comprehensive framework which mostly relies on industry-related best practices. Canada and Latin American countries developed privacy frameworks in the 1990s and 2000s partly in the form of habeas data. Asia and Oceania have seen their most developed countries adopting data privacy laws (Australia, New Zealand, Hong Kong, South Korea) while others remain lagging. The Middle East and Africa have the least developed data privacy legal frameworks (Bygrave, 2014).

Box 11: Data privacy in the United States and the European Union

Two legislative frameworks which are particularly different with regards to data privacy rules in the context of e-commerce help illustrate the diverse approaches in this arena. The EU General Data Protection Regulation (GDPR) grants the data subject a set of legal rights which provide control over data that describes him or her, consolidating data privacy and protection as a fundamental human right. The laws of United States, instead, tend to treat personal data as a property of the individual that can be transferred to others, ultimately granting ownership of such data to the data collector and processors, along with the power to use it and transfer it with certain limitations.

The European Union has a notice requirement as well as a consent requirement. This means that anyone with access to the data must obtain consent from the data subject before using the data and must inform the data subject how the data will be used. Consent must be obtained in some circumstances. In the United States, anyone with unrestricted access to the data owns it and may use it with certain exception. One exception is where the data subject gives restricted access to the data, such as when a user, when agreeing to share data, is afforded a right to later opt-out. Additionally, use may be statutorily prohibited, forbidding companies that do not meet certain requirements from using the data. Finally, if the data was accessed by unlawful means, it may not be used.

The United States has no comprehensive federal data protection policy and instead relies on self-regulation by companies and the enactment of laws as they are deemed necessary. Certain types of information, such as health information and information pertaining to children is subject to stricter rules. The Assault of Non-Solicited Pornography and Marketing Act of 2003 regulates commercial email at the federal level.

Regulation for Digital Markets

A comprehensive legal framework for data governance should provide detailed rules on all the principles recognized in the OECD Guidelines (see above). Annex 1 provides a cross-country comparison of regulation embodying these principles, as enacted in three low- and middle- income countries. Importantly, each of these principles can be implemented in different ways, depending on the priorities of the policymaker. For example, consent to data collection and transfers can be expressed on an opt-in or opt-out basis, which can lead to greater or fewer data collected by firms; an adequate framework must ensure that the rules for consent are clear one way or the other, but a choice of one option or the other depends on the policy concern of each authority.

Implementing agencies

A key aspect of data protection is who monitors and enforces the implementation of the regulation. The establishment of a capable and effective implementing agency is central to ensuring adequate implementation of the regulation and to providing individuals with a policing entity to which resort in case of violations.

Most countries who have adopted a comprehensive framework on data protection have buttressed it with a data protection agency (DPA). Certain countries, such as France, have a DPA since the 1970s, when large state-owned datasets were the main concern of the public. While most DPAs are independent agencies, some countries have embodied them with ministries or policy-making bodies (Makulilo, 2016).

The U.S. does not have a DPA *per se*. Under the EU-US Privacy Shield framework, private companies importing data from the EU must self-certify to the Federal Trade Commission (FTC) that they comply with EU laws, but there is no notification requirement for companies in most cases. The FTC has the most actionable enforcement powers, based on the Federal Trade Commission Act, which tasks the Agency with protecting consumers against unfair or deceptive commercial practices. Sector-specific regulations also exist, as in the health sector, where Health Insurance Portability and Accountability Act of 1996 (HIPAA) is enforced by the Office of Civil Rights within the Department of Health and Human Services. Furthermore, state-wide regulations, enforced by the state's Attorney General, may be more stringent. The California Consumer Privacy Act (CCPA), scheduled to become effective on January 1, 2020, grants California residents additional protections with regard to their personal data. Under the new law, companies are subject to penalties of up to \$7500 USD per intentional violation. Violations include not providing a link on their website to allow customers to opt-out of having their personal data sold to third parties. In the case of data breach incidents, the law provides for a private right of action under which each customer may receive up to \$750 dollars per incident.

Countries who have established DPAs typically give them the following tasks:

- **Raise awareness:** DPAs inform citizens about their rights regarding the processing of their personal data. In 2013, the French DPA, CNIL, received almost 125,000 telephone requests for advice or further information
- **Assist data subjects:** DPAs assist citizens, or data subjects, to enforce their right for information disclosure, data access or deletion, if applicable
- **Advise and support data controllers:** the German DPA advises and supports data protection officials and data controllers in their tasks, according to section 38 of the German Federal Data

Regulation for Digital Markets

Protection Act. The French DPA delivers certifications for products or procedures that deal with data protection (CNIL, The CNIL's Missions, 2019).

- **Supervise data controllers:** depending on their activities and size, data controllers must notify or obtain authorization prior to processing data (see below). In Senegal, data controllers must fill a 6-page notification or a 10-page application for authorization (CDP, 2019). Conversely, in Australia, the Office of the Australian Information Commissioner registers binding codes of practice from supervised industries
- **Regulate:** DPAs enact regulations to ensure that privacy acts are enforced on a daily basis by stakeholders
- **Inspect and sanction:** DPAs can perform inspections and impose fines on data controllers. The Federal Institute for Access to Public Information and Data Protection, the Mexican DPA, can also resolve disputes between data subjects and controllers

Data protection agencies can be costly to man an equip, straining government budgets. A European DPA typically employs up to 200 civil servants with high qualifications. The French DPA, CNIL, employs 71 percent of highly qualified civil servants (A class) (CNIL, Rapport d'activité, 2015). 38 percent of staff members are lawyers and 22 percent legal assistants, while 12 percent are engineers and auditors (CNIL, Statut et organisation de la CNIL, 2019). In addition, the cost of a DPA will greatly depend on the size of the jurisdiction's data market, the scope of the privacy act, and the revenue scheme adopted. The annual budget of the UK information Commissioner's Office was GBP 25m in 2017 (USD 33m) whereas the French government spends €17m (USD 20m) per year on the CNIL.

DPAs may be financed directly from the state budget (such as France), by an annual fee collected from data controllers when notifying the DPA prior to processing personal data, and/or by sanctions imposed on data controllers. Depending on the size, the annual turnover, and the type of organization, DPAs may collect different fees. In the UK, fees of the 400,000 supervised data controllers account for almost all the revenue of ICO (ICO, 2019). They are categorized as follows:

- GBP 35 for most data controllers,
- GBP 500 for:
 - a turnover of GBP 25.9m and more than 249 members of staff;
 - a public authority with more than 249 members of staff.
- GBP 35 for charities, small occupational pension schemes, and organizations that have been in existence for less than one month regardless of their size and turnover.

iv. Cybersecurity

While less visible to individual consumers, cybersecurity regulation is an essential component for promoting trust in digital markets. Major data breaches, like Yahoo's 2013 incident which affected 3 billion user accounts, not only compromise people's privacy, but can have a chilling effect for digital markets as consumers see that their information is vulnerable. In 2015, the OECD declared digital risk an economic risk (OECD, 2015). If personal data is not securely processed it is more prone to breaches.

Regulation for Digital Markets

Principles

Promoting security in digital markets is an essential component of data regulation. To that end, in addition to ensuring the rights of data subjects, data privacy regulation should render data controllers and processors liable for data processing. A data controller makes decisions over the purposes and means of the data processing, while data processors are responsible for processing data on behalf of controllers. Although businesses may see data security as an unnecessary up-front cost, a data breach can be more expensive in the end, in terms of the actual loss in addition to the costs to remedy the loss. One study estimated that cybercrime, including consumer data breaches, costs the global economy about 600 billion USD per year (McAfee & CSIS, 2018).

Security requirements consist of organizational and technical measures as well human resources. These may include mandatory encryption of personal data, implementation of rigorous internal policies, or the appointment of a data manager. Assessment of the risk to a data subject’s privacy helps determine the adequate safeguards that need to be implemented (OECD, 2013). Countries without adequate data protection regulations risk being avoided by companies due to the lack of certainty about compliance and data handling (NTB, 2015). Additionally, these countries are missing out on the benefits of the Internet, such as innovation and economic growth (WEF, 2016).

International guidelines

Data security is a concept grounded in principles of various international guidelines. Article 7 of Convention 108 of the Council of Europe stipulates that “appropriate security measures” for protecting personal data “against accidental or unauthorized destruction of accidental loss as well as against unauthorized access, alteration or dissemination” must be taken. In spite of being linked to data privacy, cybersecurity has increasingly become an autonomous topic due to the proliferation of data use and data breaches. The EU General Data Protection Regulation (GDPR), which went into effect in 2018, introduces detailed provisions to protect the personal data and privacy of EU citizens, including cybersecurity requirements (Table 2).

Table 2: EU GDPR cybersecurity requirements

Security of processing	Controllers and processors must ensure a level of security appropriate to the risk through measures such as data pseudonymization and encryption
Breach notification	In case of a personal data breach, controllers must notify the supervisory authority within 72 hours of becoming aware of the breach. In cases where the breach is likely to result in a high risk to the individual rights, the controller must notify the data subject of the breach without undue delay
Impact assessment	Where data processing is likely to result in high risk to individual rights, the controller must conduct an impact assessment prior to processing, including the foreseen measures to address the risks
Designation of data protection officer	Controllers and processors must designate a data protection officer under certain circumstances, including if the bulk of the processing activities require regular and systematic monitoring of data subjects on a large scale, or if it consists of processing of sensitive data on a large scale

c) Regulatory restrictions to digital trade

Regulation can also impose limitations that may hinder digital trade. Restrictions to digital trade, just like any economic activity, may be warranted for safeguarding public policy goals, such as protecting children, promoting public health, or protecting individual privacy. Other limitations may be aimed at overcoming or preventing market failures, such as bridging information gaps, or preventing anti-competitive practices. Oftentimes, however, the pursuit of public policy goals or the prevention of market failures can lead to overly restrictive measures that unnecessarily disrupt digital trade -thus losing business opportunities that could help boost economic growth.

A conducive regulatory framework for digital trade must hence not only provide for sound regulatory pillars to digital markets, as discussed earlier, but must also ensure that restrictions to digital trade, while effective to achieve the desired policy goals, are not unnecessarily cumbersome to digital firms.

This section reviews some of the most common restrictions to digital trade and attempts to identify emerging good regulatory practices. In particular, the section addresses restrictions related to bans on online sales and limitations on cross-border data flows.

i. Ban of online sales

Some governments prohibit or limit the online sale of certain goods or services. Like retailing services in general, the distribution of certain goods, such as chemical products like fertilizers or explosives, or guns and ammunition, drugs and medicines, or tobacco and alcohol products may be limited for reasons of public health and safety. The sale of such products is typically governed in brick-and-mortar retail by establishing certain conditions (minimum age, medical prescription, or specific permits requirements) and checking and often recording the identity of the buyer during the transaction. E-commerce brings particular challenges to such sales, as the digital nature of the transactions limits the ability of sellers to verify compliance with these conditions.

Online sales bans are largely accepted for transactions that require verifying the buyer's identity. The EU in particular, in its quest to ensure the free movement of goods within the single market, has repeatedly faced this matter. For instance, despite a 2007 ruling by the European Court of Justice (ECJ) declaring that a ban on private imports of alcohol is an unjustified restriction trade within the EU, and the EU declining proposals to ban online sales of alcohol, the Swedish government has proposed a law which bans the online purchase of alcohol from another EU country, claiming public health as a policy concern (Gunnilstam, 2017). The ECJ has, in other occasions, admitted the validity of online sales bans in cases where the identity of the seller must be verified as a condition for the sale. In Germany, the ECJ revoked a ban on the online sale of over-the-counter (OTC) pharmaceuticals in 2003 (Deutscher Apothekerverband, 2003). This was found to be a discriminatory measure, since German pharmacies could sell the products at their physical stores, while foreign pharmacies only had the internet as an avenue into the German market. Although the Court accepted that OTC pharmaceuticals could be sold online, it agreed with Germany's public health argument regarding the need to verify a doctor's prescription before issuing medicine to customers, accepting the ban on the online sale of prescription pharmaceuticals in Germany. Similarly, although the ECJ noted that a ban on online gambling maintained by the Netherlands was a restriction to trade, it ultimately agreed with the Dutch government that the need to combat fraud and criminal activity justified such a barrier (Ladbrokes Betting and Ladbrokes International, 2010).

Regulation for Digital Markets

Some alternatives to online sales bans focus on verifying the buyer's identity by a registered establishment at the time of delivery of the product. Under U.S. federal law, a person wishing to purchase a gun over the internet from a seller outside the state must have it shipped to a dealer within the state and retrieve it in person after demonstrating the minimum age and passing a background check (18 U.S.C. § 922(a)(3)). This regime does not apply to the purchase of ammunition, as a buyer may purchase ammunition from a seller online anywhere in the country and have it shipped directly to his or her home. However, states that set a minimum age to purchase ammunition, such as Massachusetts and the District of Columbia, require ammunition sales be completed face-to-face.

From a digital trade perspective, however, it remains essential that such measures be applied on a non-discriminatory basis to all sellers –foreign and domestic. It would hardly be justifiable on a legitimate public policy basis that a ban on online sales affects only foreign sellers. Similarly, when a mechanism is established to allow domestic vendors to sell controlled goods online –such as requiring that the identity verification is done at the time of delivery–, foreign online sellers should be afforded a similar regime to the extent feasible.

Online sales bans may fade out as technology improves and facilitates the identity verification. It can be expected that as technologies like face or fingerprint recognition evolve, and solutions like secure digital signature become mainstream, online sales of regulated goods will be gradually allowed, at least by vendors who meet certain qualification criteria.

ii. Regulations on cross-border data flows

Data flows are the bloodstream of digital trade. Data exchanges not only channel the information that results in digital transaction (buyers' and sellers' details, price, contractual terms, payment order, etc.), but when it comes to trade in services, they embody the actual object of the transaction (the professional advice; the customer care; the images, video, or sounds; the app-based intermediation services that are being trade, etc.). Digital data is also becoming increasingly important to other activities, by providing information that boosts the capacity and efficiency of other economic activities (the real time monitoring of manufacturing robots; patients clinical data; etc.) –see Box 12. Cloud computing allows users to store, manage, and process data remotely, which is highly beneficial to users who can choose to pay only for the quantity and time needed (Koske, Bitetti, Wanner, & Sutherland, 2014). As such, regimes open to the flow of information across borders are essential for digital trade to flourish.

Box 12: The need for data transfers in GVCs

Data is crucial for firms in the manufacturing sector for several different reasons:

1. Exercise control and coordination: firms must be able to move data across different locations to be able to control and coordinate production in different geographical locations, work with subcontractors and suppliers, and handle internal issues
2. Pre-production research and development: communication with external partners located around the world is necessary to conduct R&D and testing in the pre-production phase
3. Ensure supply chain management: firms need to share information across different entities to manage input flows and the necessary capital
4. Manage production: the production and assembly of products is handled by robotics; data transfers are necessary to control this process
5. Run and monitor sold goods: firms rely on data transfers in the post-sales phase to handle maintenance, repairs, and spare parts

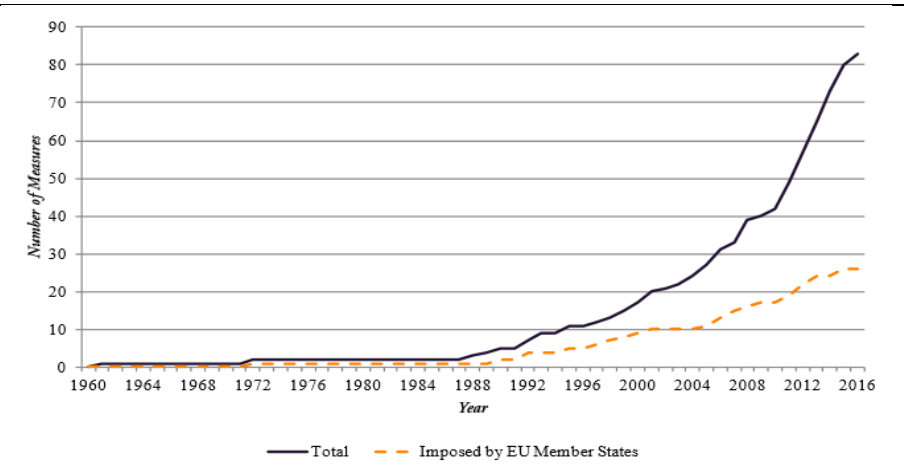
Regulation for Digital Markets

Source: (NTB, 2015)

Yet, public policy may prevent some data from being freely shared around the world. Governments prefer that some information remain physically located within their boundaries for national security interests, or for ensuring regulatory oversight over such information, or, often, as a way of promoting domestic business related to the servicing of such data. These data regulations lead to productivity losses, which in turn result in lower returns on investment (OECD, 2016). These losses need to be weighed against the public policy concerns in order to find a reasonable solution that protects the citizens' rights while enabling cross-border trade.

Regulations regarding data localization and the restrictions on data flows have been on the rise around the world (Figure 3), and the way in which they are imposed vary throughout countries. Companies across different sectors depend on data transfers to be able to participate in global value chains (GVCs) (Box 12). In a survey carried out among U.S. industry representatives, data localization was the most cited measure restricting digital trade (USITC, 2017).

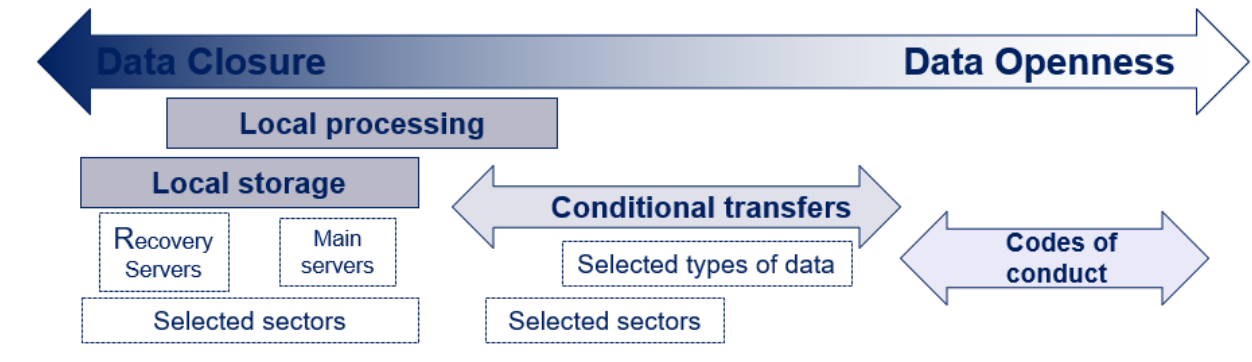
Figure 3: Data localization measures implemented globally and intra-European Union



Source: (ECIPE, 2016)

Data governance regimes seldom provide for full openness or closure to cross-border data flows. Governments aim to protect sensitive information through limitations on the transfers of data. These measures can be found in almost every region of the world. Regulations on cross-border data flows can broadly take two forms: i) requirements for storage or processing of data within their territory, typically referred to as server or data localization requirements, and ii) data transfer conditioned to certain requirements in the destination country (Figure 4) (Casalini & López González, 2019).

Figure 4: Types of limitations on cross-border data flows



Data localization requirements

Data localization requirements compel the storage or processing of data within the country where the service is provided. Some governments require the storage of a copy of the data within national borders, while others ban the processing or transfer of data outside country borders. For instance, many states of the United States require that any contractors to public contracts locate their servers within the state itself. Some countries, like Saudi Arabia, also follow this practice. Data localization requirements can be narrowed down to a specific sector. China and Indonesia maintain broad localization requirements, while Korea and Vietnam, for example, impose data localization requirements on financial services and internet services providers, respectively. Most data localization measures are found in the accounting and financial sector, as well as the health sector (Bauer, Matthias et al, 2016).

While the geographical location of the data may sometimes respond to public policy concerns, for instance with data sensitive to national security, often this requirement results in unnecessary costs to the taxpayers. Further, the localization of servers within a given country is hardly an effective cybersecurity measure in and of itself, as the data may be better protected distributed in servers around the world than in one single location, or within one single country. This can particularly troubling when requiring the localization of both the main data servers as well as the “recovery” centers used for backup.

Box 13. Law enforcement and data localization requirements

One of the policy goals often prompting data localization requirements is the need to ensure the access to data by law enforcement (Chander & Le, Data Nationalism, 2015). Whereas other rules on data governance, such as those on privacy protection, are desirable as a tool to increase trust in the digital markets, disciplines on data governance and its relationship with law enforcement provide courts with effective regulatory tools to carry out their law enforcement duty in the era of digital communications, while ensuring that online services are not unnecessarily burdened in that process. The tension arises when law enforcement agencies need to access data stored in a foreign jurisdiction and the agencies lack specific tools to compel the online provider to produce the data. In that case, courts may fail to obtain the necessary information –potentially leaving a case unresolved as a result- or may resort to draconian measures that unnecessarily burden services providers and impact consumers –hence hampering the global digital market.

How can cross-border data flows hamper law enforcement – and vice versa?

Some recent high-profile cases illustrate the challenge that global data flows can bring to law enforcement: United States vs. Microsoft Corp demonstrated the linkages between cross-border data flows and the ability of courts to investigate and legitimately prosecute unlawful conduct (Matsakis, 2018). There, U.S. federal prosecutors investigating a drug trafficking case in 2013 served a warrant to Microsoft Co. to provide an

Regulation for Digital Markets

individual's emails. Microsoft handed data stored on U.S. servers and the person's address book but didn't deliver the actual content of the individual's emails, arguing that they were stored in a Microsoft data center in Dublin, Ireland, and the warrant by U.S. authorities did not have extraterritorial application. U.S. prosecutors argued that, because the facts of the case took place in the United States and Microsoft is a U.S.-based company, producing a copy of such information would not entail extraterritorial effects of the warrant, but a mere compliance with a warrant by a U.S. court.⁴ The case was taken to the Supreme Court but ended without a ruling due to the passage of the new Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") in 2018. This law allows federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of where the data are stored in the U.S. or on foreign soil.

The circumstances of this case raise substantial questions related to the regulation of cross-border data flows and law enforcement procedures. With no data localization requirements in the U.S., companies like Microsoft, which has over 100 data centers in 40 countries, could potentially move data swiftly for business purposes and thus hamper law enforcement (Barnes, 2017). If firms are free to transfer and store data in any physical location of their choosing, how can law enforcement agencies obtain access to such information? How can policymakers ensure that data regarding offenses occurring within their jurisdiction, by their nationals, stored by a domestic company remains reachable?

Courts from developing countries have faced similar challenges in retrieving data from foreign jurisdictions, resorting at times to heavy-handed measures to overcome them. Brazilian courts have come, in multiple occasions, to stand-offs with online services who refused to produce data. An early case in 2006 entailed an order from a federal judge issued to Orkut, a social media platform owned by Google and one of Brazil's most popular websites at the time, to provide details on over twenty Brazilian nationals alleged to be using the social platform for spreading child pornography and selling drugs. After an initial refusal by Orkut on the argument that the information was not stored in Brazil, but in Google's servers in the U.S. –for which the judge imposed a fine of USD 23,000 a day-, Google agreed to cooperate with the judge's request and hand over the information (Nakashima, 2006) (Morphy, 2006). Eventually, Orkut went further in the cooperation with Brazilian authorities, granting the federal police direct access to Orkut's accounts and the ability to monitor and even to delete users accounts in real time, without the need for a judicial order (Pagnan, 2006). A similar case occurred in 2016, in a judicial attempt to retrieve data from encrypted end-to-end chat mobile app, Facebook-owned WhatsApp. Faced with non-compliance, the judge first ordered the arrest of Facebook's executive vice-president, who was released one day later by order of the Court of Appeals, who deemed the arrest arbitrary and unjustified (G1 Sao Paulo, 2016). The judge then blocked WhatsApp services in Brazil for 72 hours, but the appeals court overturned the order only hours later (BBC, 2016). Another case involving WhatsApp entailed the freezing of Facebook's bank accounts in Brazil for over 6 million USD in fines, as a result of months of noncompliance with a court order issued in an investigation of an alleged international cocaine smuggling ring (Commuter).

What are the existing tools for cooperation in law enforcement in the digital age?

Mutual Legal Assistance Treaties (MLATs) are to date the main tool for international cooperation in law enforcement. MLATs are traditionally aim to fulfill criminal and public investigation procedures like obtaining testimony of witnesses located abroad, executing search warrants in foreign jurisdictions, or obtaining records of financial institutions abroad.

However, MLATs are poorly suited to address the challenges of the digital age. MLATs can be cumbersome and time-consuming, not only due to the rigorous legal requirements that they entail, but also due to the limited

⁴ Given the confidentiality of the procedures, the nationality of the individual remains undisclosed, as well as whether the emails were generated within the United States, and the reasons why the account content was physically stored in Ireland. This latter fact may relate to the individual having indicated Ireland as its country of citizenship or residency, or simply to a business decision by Microsoft. On the facts of the case, see Harvard Law Review, "Microsoft Corp. v. United States", 130 Harv. L. Rev. 769, December 6m 2016, <https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/> and Lawreview, "Microsoft Corp. v. United States", 102 Minnesota Law Review 6, February 23 2017, <http://www.minnesotalawreview.org/2017/02/microsoft-corp-v-united-states/>

Regulation for Digital Markets

resources often available for this kind of international cooperation (Force Hill, 2015). They are designed for courts to reach assets, companies, and people, that are less mobile than the fleeting storage of bytes. Furthermore, if data controllers are free to move personal data around at will and could disregard injunctions to produce required information by legitimate authorities, nothing prevents businesses from storing data in specific jurisdictions that are unresponsive to judicial cooperation, effectively providing a safe haven from legal prosecution. Unscrupulous firms could build a business model around such practices.

What other solutions can help law enforcement while fostering seamless cross-border data flows?

Policy makers who wish to support global trade and investment flows with an open cross-border data regime should be able to do so without sacrificing their domestic law enforcement capacity. Data localization requirements, while potentially effective to ensure access to data by law enforcement, entail costs that can hamper businesses. Innovative regulatory solutions should reconcile these policy objectives.

- Legislation may grant domestic courts the ability to request their citizens and firms to produce data regardless of their physical location, overcoming the need for data localization requirements. The recently approved CLOUD Act distinguishes between data from Americans and non-Americans held abroad on servers of American companies.⁵ It allows for the retrieval of data by American citizens held abroad thus bypassing MLATs, making it mandatory for firms to comply with such court order. On the other hand, the CLOUD Act permits foreign governments that have entered into executive agreements with the U.S. government to obtain information from U.S.-based internet companies.
- Other solutions may focus on strengthening cooperation between law enforcement agencies and/or national data protection authorities. Stronger cooperation could focus on expedited consideration and implementation of the request from foreign authorities, while ensuring that privacy concerns of citizens and residents remain well protected. Such regulatory agency cooperation is hardly a novelty. Competition authorities, across the Atlantic and with many other countries, have established strong collaboration frameworks in cases related to transnational anti-competitive behaviors. Specific to cybercrime, “24/7 Networks” seek to ensure points of contact in law enforcement agencies in different countries that can respond in real time and jointly to cyberattacks and other cyber-crimes.⁶
- Trade agreements could support international rules on the interplay between data flows and law enforcement. By recognizing that court orders may, under certain conditions, reach online firms that are not established in the court’s jurisdiction, they could help prevent burdensome punitive measures on cross-border providers that unnecessarily disrupt the broader digital market. To that end, a softly worded provision, similar to existing provisions on e-commerce cooperation in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) or the EU – Canada Comprehensive Economic and Trade Agreement (CETA), could promote greater collaboration between the parties in this field, or even serve as legal grounds for courts to request data from non-established firms.
- Finally, guidelines in the form of rules of conduct for firms responsible for data storage and processing could also provide a valuable instrument to support domestic law enforcement efforts. Firms established in the country or firms located abroad who offer services in that country would need to comply with such rules to facilitate law enforcement, much like the Privacy Shield between the U.S. and EU provide a framework for compliance with privacy regulations.

The interaction between cross-border data flows and law enforcement offers an example of the challenges that new technologies can bring to policy making. New forms of information sharing and its sheer volume,

⁵ Several countries have already in similar procedures. See Maxwell, Winston and C. Wolf, “A Global Reality: Governmental Access to Data in the Cloud”, Hogan Lovell White Paper, 2012, <https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20%2818%20July%2012%29.pdf> for a review the legislation of ten high-income countries on this matter.

⁶ On MLATs, 24/7 Networks, and other forms of international cooperation specific to cybercrime, see World Bank and United Nations. 2017. *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

Regulation for Digital Markets

unthinkable only one generation ago, are creating formidable opportunities for business, spurring economic growth. These interactions, however, can affect sensitive public policies, such as the need to protect privacy, establish a conducive environment for trade and investment, or ensure safety and security. These policy-making challenges are only at their initial phases, and warrant careful, balanced, and innovative regulatory responses.

Source: (Molinuevo & Gaillard, 2018)

Requirements for local processing establish that the data must be processed within the boundaries of the country concerned. Russia's Personal Data Act requires that the personal data of Russian citizens be used by local data operators and be stored in the country. While this can be more effective to the purposes of generating employment than mere localization, it also introduces a critical dependence on the local IT expertise. In countries with limited human resources capacity, local processing requirements could entail severe risks to quality of services or even to cybersecurity.

Data localization requirements introduce costs for firms who are forced to have multiple data storage locations, and can close the market for those who cannot afford those expenses (Bauer, Matthias et al, 2016). These costs can ultimately be passed on to consumers as well as the country imposing the restriction. Additionally, keeping the data static negatively impacts its resilience, making it more vulnerable to attacks (Klein, 2015). Countries imposing data localization requirements often do so with the goal of creating jobs in the valuable IT sector. However, the employment and capacity transfers benefits are often marginal. In 2011, Apple built a \$1 billion data center in Maiden, North Carolina, bringing merely fifty full-time support jobs (Rosenwald, 2011). More broadly, a review of a number of data localization regulations around the world showed that alternative measures could to achieve the purported policy goals while allowing for cross-border data transfers (Chander & Le, 2015).

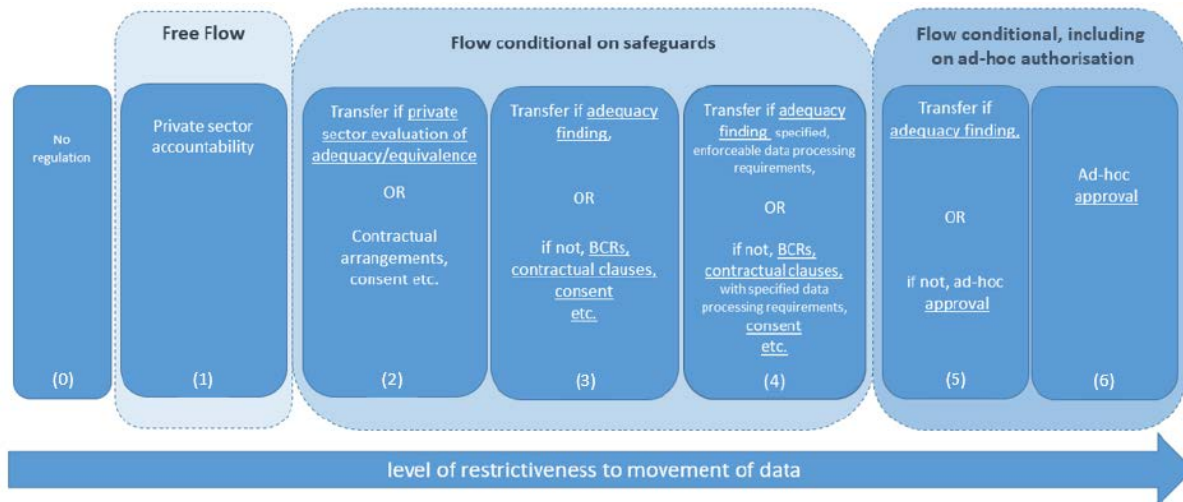
Conditional data flows

Conditional data flows allow for cross-border transfers of data, but only after certain particular regulatory requirements are met. Conditions typically relate to express consent by the data subject or to the treatment of data by the country where it is being transferred. Conditional data transfers can apply to certain types of data, such as personally identifiable information, or to data relating to specific sectors, such as health data.

Conditional transfers tend to reflect more open data regimes than localization requirements, but much depends on the implementation of the regime. The broader the scope of types of data included, and the harsher the regulatory conditions for transfer, the more closed the data regime will be. Ultimately, a conditional data transfer regime could be so strict that no transfers are allowed –being equivalent in practice to a data localization requirement.

Figure 5. Taxonomy of conditional data flows

Regulation for Digital Markets



Source: (Casalini & López González, 2019)

The EU data privacy regime features the most prominent example of conditional transfers. Under the GDPR, personal data can only be transferred to countries (or part thereof) who have established a data privacy regime that offers an “adequate” level of protection for personal data –and the European Commission has officially recognized as much in an Adequacy Decision. The issuance of an Adequacy Decisions entails a review by the European Commission of an exhaustive and detailed set of requirements relating to the regulatory framework of the country, in categories such as

- the rule of law and legal protections for human rights and fundamental freedoms;
- access to transferred data by public authorities;
- existence and effective functioning of DPAs; and
- international commitments and other obligations in relation to the protection of personal data.

A key aspect of regulation setting out conditions for cross-border data flows is who may assess whether the conditions for transfers are met (Figure 5). Essentially, the decision on whether data may be transferred may rest on the firms transferring the data, or on a public entity -typically the data protection agency. In the first case, cross-border data transfer is only permitted where the data exporter, on the basis of its assessment, considers that the context of the transfer ensures an equivalent or adequate level of data protection in the recipient country. However, and more frequently, the determination of adequacy or equivalence can be determined by the data protection authority, certifying that the data protection system of another country is suitable for the transfer. This determination can take the form of a unilateral recognition, or it can take the form of a mutual recognition of data protection measures (Casalini & López González, 2019).

Regulations setting out conditions for data transfer must also provide alternative solutions for transfers to countries that do not meet such regulatory standards. The GDPR, for example, allows transfers to countries who may not offer “adequate” protection if the receiving firm is contractually bound to certain data protection obligations. The GDPR offers pre-approved contractual clauses and allows the parties to draft custom clauses and have them approved by the local DPAs; also, firms may receive data if subject to legally binding corporate rules (BCRs) that hold them responsible for data protection.

Regulation for Digital Markets

Conditional data transfers offer a middle ground between strict data localization requirements and full openness to cross-border data. In so doing, they grant policy makers the ability to set out certain safeguards on the use of data, notably for the protection of individual privacy, while allowing for data to cross borders where needed. As such, conditional data flows appear as a more suitable tool than data localization or processing requirements. Regulations on conditional flows in themselves offer a wide range of solutions, in terms of scope as well as procedures for regulatory compliance, that allow for greater flexibility and lower costs to business or greater public oversight and data protection. Importantly, as shown in the case of the GDPR, regulators can also adopt multiple channels for the protection of cross-border data, relying on private firms' liability (through contractual clauses) where the broader regulatory regime does not meet the desired standards for data protection.

3. Concluding observations

The regulation of digital markets, like any economic and social regulation, entails the balancing of policy goals, often between economic freedoms and other public policy interests. Just like in the offline world, measures meant to safeguard public health will ban the sale of certain goods (e.g. toys containing toxic chemicals), or do it under certain conditions (e.g. tobacco, medicines), thus inherently limiting trade. Other limitations may be motivated by other legitimate policy concerns, such as protecting citizens' privacy, limiting access to sensitive or offensive material like child pornography or hate speech, or preventing cybercrime. In the online world, the regulation must also consider the additional challenges that remote, often international, transactions bring about. The sale of controlled substances, such as alcohol or tobacco products, or chemical products, may be banned or require additional conditions in digital markets, where the identity of the buyer can more easily be concealed. Ultimately, the exact balance between the freedom to trade online with the level of security or protections remains an idiosyncratic decision of each policymaker to be made on a case-by-case basis.

A cursory review of some of the key policy pillars of digital trade suggests that regulatory solutions are still evolving, and consensus on "best regulatory practices" remains elusive. This is particularly the case for the newer issues, such as online consumer protection, intermediary liability, data protection, and cybersecurity. The regulation of remote transactions, instead, such as electronic documentation and electronic signature has benefitted from greater international guidance, but newer regulations have also introduced innovations to facilitate the adoption of such solutions while ensuring the security of the transactions.

The review demonstrates that digital markets, especially at a global level, introduce important policy challenges that demand thorough and sound regulatory solutions. Regulations are necessary to provide the legal tools for remote transactions, such as electronic document and signatures, balancing the security of such tools with enough flexibility and incentives to promote mainstream adoption. Additional regulations addressed at boosting trust in digital markets tackle key questions regarding citizens' and users' rights, such as consumer protection and data privacy, as well as central rules to the functioning of digital platforms, such as intermediary liability rules. Policymakers and regulators, both at the national and international level, must work towards sound regulatory solutions in line with their public policy interests, their governments' implementing capacity, and harmonized with its international partners in a way that boosts access to global markets and expands the benefits of digital trade.

Bibliography

- 15 U.S.Code § 6801, Protection of nonpublic personal information.
- 18 U.S.C. § 922(a)(3).
- Adobe. (2019, June). *Global Guide to Electronic Signature Law*. Retrieved from <https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf>
- Ahmed, U., & Anupam, C. (2015). Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows. *E15Initiative*.
- Albright Stonebridge Group. (2015). *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*.
- Article 29 Data Protection Working Party. (2002). *Opinion 4/2002 on the level of protection of personal data in Argentina*. Brussels: European Commission.
- AssureSign. (2019, June). *E-Sign Laws Across Borders*. Retrieved from AssureSign: <https://www.assuresign.com/e-sign-laws-across-borders/>
- Barnes, R. (2017, October 16). *Supreme Court to consider major digital privacy case on Microsoft email storage*. Retrieved from Washington Post: https://www.washingtonpost.com/politics/courts_law/supreme-court-to-consider-major-digital-privacy-case-on-microsoft-email-storage/2017/10/16/b1e74936-b278-11e7-be94-fabb0f1e9ffb_story.html?utm_term=.85a60c2da3d0
- Bartley Johns, M., Hoppe, M., Molinuevo, M., Nghardsaysone, K., & Daza Jaller, L. (2017). *Taking Advantage of E-Commerce: Legal, Regulatory and Trade Facilitation Priorities for Lao PDR*. Washington, DC: World Bank Group.
- Bauer, Matthias et al. (2014). The Cost of Data Localisation: Friendly Fire on Economic Recovery. *ECIPE Occasional Paper No 3/2014*.
- Bauer, Matthias et al. (2015, June). Data Localisation in Russia: A Self-imposed Sanction. *ECIPE Policy Brief*.
- Bauer, Matthias et al. (2016). Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States. *ECIPE Policy Brief*.
- BBC. (2016, July 20). *WhatsApp in Brazil back in action after suspension*. Retrieved from BBC News: <https://www.bbc.com/news/world-latin-america-36836674>
- Blythe, S. (2011). *E-Commerce Law Around the World - Volume 1*. USA: Xlibris Corp.
- Blythe, S. E. (2012). *An E-Commerce Law for the World: The Model Electronic Transactions Act*.

Regulation for Digital Markets

- Boss, A. H. (1999). *The Internet and the Law: Searching for SEcurity in the Law of Electronic Commerce*. 23 *NOVA L.REV.*
- Boss, A. H. (2009). The Evolution of Commercial Law Norms: Lessons to be Learned from Electronic Commerce. 34:3 *Brooklyn Journal of International Law*, 673.
- Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press.
- Casalini, F., & López González, J. L. (2019). *Trade and Cross-*. Paris: OECD. Retrieved from <http://dx.doi.org/10.1787/b2023a47-en>
- CDP. (2019). *Liste des formulaires*. Retrieved from <http://www.cdp.sn/liste-des-formulaires>
- Chander, A., & Le, U. P. (2014). Breaking the Web: Data Localization vs. the Global Internet. *US Davis Legal Studies Research Paper Series*.
- Chander, A., & Le, U. P. (2015, March 13). Data Nationalism. *Emory Law Journal*, 64(3).
- CNIL. (2015). *Rapport d'activité*. Paris: Commission nationale de l'Informatique et des Libertés.
- CNIL. (2019). *Statut et organisation de la CNIL*. Retrieved from <https://www.cnil.fr/fr/le-fonctionnement>
- CNIL. (2019). *The CNIL's Missions*. Retrieved from <https://www.cnil.fr/en/cnils-missions>
- Commuter. (n.d.). *Brazil court blocks Facebook funds over WhatsApp*. Retrieved from Commuter: <https://worldcommuter.com/brazil-court-blocks-facebook-funds-whatsapp-dispute-report/>.
- Cortés, P. (2010). *Online Dispute Resolution for Consumers in the European Union*. London: Routledge, Taylor & Francis Group.
- Deutscher Apothekerverband, C-322/01 (European Court of Justice December 11, 2003).
- Digital Signature Act § 61 , Malay. (1997).
- EC. (2011, November 28). *Alternative Dispute Resolution and Online Dispute Resolution for EU consumers: Questions and Answers*. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_11_840
- ECIPE. (2016). *Digital Trade Estimates*.
- EFF. (2019). *Manila Principles on Intermediary Liability*. Retrieved from <https://www.manilaprinciples.org/>
- Electronic Transactions Act, Sing. (1998).
- European Commission. (2019). *Online Dispute Resolution*. Retrieved from <https://ec.europa.eu/consumers/odr/main/?event=main.home2.show>
- European Parliament. (2015). *Review of EU Copyright Framework*.
- Force Hill, J. (2015, January 28). Problematic Alternatives: MLAT Reform for the Digital Age. *Harvard National Security Journal*.

Regulation for Digital Markets

- Frederick Fischer, S. (2001). Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation. *7 B.U.J.SCI & TECH. L.*, 229.
- G1 Sao Paulo. (2016, July 19). *WhatsApp: Justiça do RJ manda bloquear aplicativo em todo o Brasil*. Retrieved from O Globo: <http://g1.globo.com/sao-paulo/noticia/2016/03/felizes-diz-facebook-sobre-soltura-de-vice-presidente-presos-em-sp.html>
- Gasser, U., & Schulz, W. (2015). Governance of Online Intermediaries: Observations from a Series of National Case Studies. *Berkman Center Research Publication No. 2015-5*.
- Gunnilstam, J. (2017, January 17). *Sweden is trying to restrict the free movement of goods within the EU*. Retrieved from ECOMONY: Reporting from the E-commerce Economy: <http://www.ecomony.com/Swedish-Government-to-Outlaw-Online-Alcohol,9431.html>
- Hangzhou Internet Court. (2019). *The litigation platform of Hangzhou Internet Court*. Retrieved from <https://www.netcourt.gov.cn/portal/main/en/index.htm>
- Holland, A., Bavitz, C., Hermes, J., Sellars, A., Budish, R., Lambert, M., & Decoster, N. (2014). *Intermediary Liability in the United States*. Retrieved from Global Network of Internet and Society Research Centers (NoC): <https://publixphere.net/i/noc/instance/noc.html>
- ICO. (2019). *Data protection fee*. Retrieved from <https://ico.org.uk/for-organisations/register/>
- ICPEN. (n.d.). *International Consumer Protection and Enforcement Network*. Retrieved from <https://www.icpen.org/resolve-dispute>
- Klein, S. (2015, November 23). *The Data Is in the Details: Cross-Border Data Flows and the Trans-Pacific Partnership*. Retrieved July 11, 2017, from The Diplomat: The Diplomat
- Koske, I., Bitetti, R., Wanner, I., & Sutherland, E. (2014). The Internet Economy - Regulatory Challenges and Practices". *OECD Economics Department Working Papers, No. 1171*.
- Ladbrokes Betting and Ladbrokes International, C-258/08 (Second Chamber June 3, 2010).
- Leung, H. (2019, April 2). *Time*. Retrieved April 2, 2019, from Singapore is the latest country to propose tough legislation against fake news: <http://time.com/5562501/singapore-fake-news-law-freedom-speech/>
- Makulilo, A. B. (2016). African Data Privacy Laws. In *Issues in Privacy and Data Protection*. Springer.
- Manila Principles on Intermediary Liability*. (2015, March 24). Retrieved from Electronic Frontier Foundation: https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf
- Matsakis, L. (2018, February 27). *Wired*. Retrieved from Microsoft Supreme Court case has big implications for data: Matsakis, Louise, "Microsoft Supreme Court case has big implications for data", *Wired*, February 27, 2018, <https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/>
- McAfee, & CSIS. (2018). *Economic Impact of Cybercrime— No Slowing Down*.

Regulation for Digital Markets

- Metz, R., & Purnhagen, K. (2012). *E-commerce in China and Germany : a Sino-German comparative analysis*. München: C.H. Beck.
- MGI. (2016). *Digital Globalization: The new era of global flows*. McKinsey Global Institute.
- Molinuevo, M., & Gaillard, S. (2018, December). Trade, Cross-Border Data, and the Next Regulatory Frontier: Law enforcement and data localization requirements. *Macroeconomics, Trade & Investment: MTI Practice Notes*, 3.
- Morphy, E. (2006, September 5). *Google to Comply with Brazilian Court Order*. Retrieved from TechNewsWorld: <https://www.technewsworld.com/story/52830.html>
- Munukutla-Parker, U. (2006). Unsolicited Commercial Email, Privacy, Concerns Related to Social Network Services, Online Protection of Children, Cyberbullying. *I/S: A Journal of Law and Policy for the Information Society*, Vol. 2, No. 3.
- Nakashima, E. (2006, September 2). *Google to Give Data to Brazilian Court*. Retrieved from Washington Post: <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/01/AR2006090100608.html>
- NTB. (2012). *E-commerce- New Opportunities, New Barriers: A survey of e-commerce barriers in countries outside the EU*. Stockholm: National Board of Trade.
- NTB. (2015). *No Transfer, No Production – a Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods*. Stockholm: National Board of Trade.
- OECD. (2000). *Guidelines for Consumer Protection in the Context of Electronic Commerce*. Paris: OECD.
- OECD. (2007). *Recommendation on Consumer Dispute Resolution and Redress*. Paris: OECD Publishing.
- OECD. (2013). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers*, No. 220.
- OECD. (2013). *The OECD Privacy Framework*.
- OECD. (2014). Consumer Policy Guidance on Mobile and Online Payments. *OECD Digital Economy Papers*, 236.
- OECD. (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. Paris: OECD Publishing.
- OECD. (2016). *Consumer Protection in E-commerce: OECD Recommendation*. Paris: OECD Publishing.
- OECD. (2016). *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*. OECD.
- OECD. (2016). *Working Party of the Trade Committee- Localising Data in a Globalised World*. Paris.
- OECD. (2018, April). Improving Online Disclosures with Behavioural Insights: Towards Better Outcomes for Consumers. *Directorate for Science, Technology and Innovation Policy Note*.
- Ortolani, P. (2016, Autumn). Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin. *Oxford Journal of Legal Studies*, 36(3), 602.

Regulation for Digital Markets

- Pagnan, R. (2006, November 28). *Orkut dá à PF "atalho" para barrar páginas*. Retrieved from Folha de S.Paulo: <https://www1.folha.uol.com.br/foiha/informatica/ult124u21063.shtml>.
- Rosenwald, M. (2011, November 24). *Washington Post*. Retrieved 2018, from https://www.washingtonpost.com/business/economy/cloud-centers-bring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html?utm_term=.789bafce1374
- Satyan, K. (2015, July 2). *Satyan, Kanika, E-Commerce and Consumer Rights: Applicability of Consumer Protection Laws in Online Transactions in India (July 2, 2015)*. Available at SSRN: <https://ssrn.com/abstract=2626027> or <http://dx.doi.org/10.2139/ssrn.2626027>. Retrieved from SSRN: Satyan, Kanika, E-Commerce and Consumer Rights: Applicability of Consumer Protection Laws in Online Transactions in India (July 2, 2015). Available at SSRN: <https://ssrn.com/abstract=2626027> or <http://dx.doi.org/10.2139/ssrn.2626027>
- Schmitz, A. J., & Rule, C. (2017, June 27). The New Handshake: Where We Are Now. *International Journal of Online Dispute Resolution*, 2016(3).
- Smedinghoff, T. J., & Ruth Hill Bro. (1999). Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce. *17 J. Marshall J. Computer & Info L.*
- SquareTrade. (2019). *SqaureTrade*. Retrieved from <https://www.squaretrade.com/>
- UNCITRAL. (1996). *UNCITRAL model law on electronic commerce, with guide to enactment, 1996: with additional article 5 bis as adoped in 1998*.
- UNCITRAL. (2001). *Model Law on Electronic Signatures*.
- UNCITRAL. (2017). *Technical Notes on Online Dispute Resolution*. New York: United Nations.
- UNCITRAL. (2017). *Technical Notes on Online Dispute Resolution*. New York: United Nations.
- UNCITRAL. (2019). Status of conventions and model laws - Note by the Secretariat. *United Nations Commission on International Trade Law - 52nd Session*. Vienna: UN.
- UNCTAD. (2017). *Consumer Protection in Electronic Commerce: A Note by the UNCTAD Secretariat*. Geneva: United Nations.
- UNCTAD. (2019, March 27). *Cyberlaw Tracker*. Retrieved from http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx
- USITC. (2017). *Global Digital Trade I: Market Opportunities and Key foreign Trade Restrictions*. The U.S. International Trade Commission.
- USTR. (2016). *National Trade Estimate Report*. Office of the United States Trade Representative.
- WEF. (2016). *Global Information Technology Report*. Geneva: World Economic Forum.
- WIPO. (2019). *Alternative Dispute Resolution*. Retrieved from <https://www.wipo.int/amc/en/index.html>

Regulation for Digital Markets

World Economic Forum. (2019, March). *The Global Governance of Online Consumer Protection and E-Commerce*. Retrieved from World Economic Forum:
http://www3.weforum.org/docs/WEF_consumer_protection.pdf

Annexes

Annex 1: Cross-country Comparisons of the Implementation of OECD Recommendation on Information Disclosure

OECD Recommendations	France ⁷	Tunisia ⁸	Uganda ⁹
<p>Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique</p>	<p>Loi n°2000-83 du 9 août 2000, relative aux échanges et au commerce électroniques</p>	<p>Electronic Transactions Act, 2011</p>	
<p>Paragraph 28. Businesses engaged in e-commerce with consumers should make readily available information about themselves that is sufficient to allow, at a minimum:</p> <p>i) identification of the business; ii) prompt, easy and effective consumer communication with the business; iii) appropriate and effective resolution of any disputes that may arise; iv) service of legal process in domestic and crossborder disputes; and v) location of the business.</p> <p>Paragraph 29. This information should include the legal name of the business and name under which it trades; its principal geographic address; an e-mail address, telephone number or other electronic means of contact; appropriate domain name registration information for web sites that are promoting or engaging in commercial transactions with consumers; and any relevant government registration or license information.</p>	<p>Article 19</p> <ul style="list-style-type: none"> • noms et prénoms (...) • raison sociale ; • adresse ; • son adresse de courrier électronique ; • coordonnées téléphoniques ; • un prix doit être indiqué de « manière claire et non ambiguë, et notamment si les taxes et les frais de livraison sont inclus. ». 	<p>Chapter V: On the Electronic Commerce Transaction - Article 25</p> <p>“In electronic commerce transactions, the merchant must provide the consumer, in a clear and comprehensible manner and before the execution of the contract, with the following information:</p> <ul style="list-style-type: none"> • Identity, address and phone number of the merchant or the service provider ; • A complete description of all transaction steps ; • Nature, specifications and pricing of the product ; • Product delivery and insurance costs as well as due taxes ; • Period for which the products is displayed with the indicated prices ; • Commercial guarantees and aftersale service conditions ; 	<p>Article 24: “Information to be provided by suppliers or sellers. (...)</p> <ul style="list-style-type: none"> • the full name and legal status of the person; • the physical address and telephone number of the person; • the web site address or e-mail address of the person; • membership of any self-regulatory or accreditation bodies to which the person belongs or subscribes and the contact details of that body; • any code of conduct to which that person subscribes • in the case of a legal person, the registration number, names of directors and place of registration; • the physical address where the person may be served with documents; • a description of the main characteristics of the goods or services offered by the person which is sufficient to enable a consumer to make an informed decision on the proposed electronic transaction; • the full price of the goods or services, including transport costs, taxes and any other fees or costs; • the manner of payment; • any terms or conditions of agreement, including any guarantees, (...) • the time within which the goods will be dispatched or delivered (...)

⁷ <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000801164>

⁸ <https://www.bct.gov.tn/bct/siteprod/documents/loi200083.pdf>

⁹ <https://www.ulii.org/ug/legislation/act/2015/8-3>

Regulation for Digital Markets

Paragraph 30. When a business publicises its membership in any relevant self-regulatory programme, business association, dispute resolution organisation or other body, the business should provide sufficient information to enable consumers to easily contact such body. Businesses should provide consumers with easy methods to verify that membership, access the relevant codes and practices of the organisation, and take advantage of any dispute resolution mechanisms offered by the organisation.

- Payment methods and procedures and, when necessary, conditions for available loans ;
 - Methods and time of delivery and of execution of contract and results of non-fulfillment of engagements.
 - Possibility of purchase cancellation and its deadline ;
 - Method for order confirmation ;
 - Method for product return or exchange and cost refund ;”
 - Etc.
- the return, exchange and refund policy of the person;
 - any alternative dispute resolution code to which the person subscribes and how the code may be accessed electronically by the consumer;
 - Etc.

Annex 2: Cross-country Comparison on the Three Main Features of the Right of Withdrawal

	Morocco	Turkey	Finland
Law	Law No: 31-08 on measures to protect consumers ¹⁰	Law No: 6502 on consumer protection ¹¹	Consumer Protection Act ¹²
Information Duty	Article 26 : « l'offre de contrat doit comporter les informations suivantes : (...) 4° L'existence du droit de rétractation »	Article 18 : “(2) (...) The seller or supplier is liable to prove that the consumer has been informed regarding the right of withdrawal.”	Section 13 : “(1) In distance selling, the consumer shall be supplied with the following information well in advance of the conclusion of the contract: (...) (8) the existence of the right of withdrawal”
Absence of Reason	Article 30 : le consommateur dispose d'un délai de sept jours francs pour exercer son droit de rétractation <u>sans avoir</u>	Article 18 : (1) The consumer is entitled to withdraw from the instalment sale contract <u>without giving any reason</u> and without	None

¹⁰ http://www.egov.ma/sites/default/files/projet_loi_31-08_21_1008.pdf

¹¹ http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/CountryDetail.aspx?country=tr

¹² <http://www.finlex.fi/en/laki/kaannokset/1978/en19780038.pdf>

Regulation for Digital Markets

	à justifier de motifs ni à payer de pénalités, à l'exception, le cas échéant, des frais de retour.	incurring any penalties within seven (7) days.	
Withdrawal period	Article 30 : le consommateur dispose d'un délai de <u>sept jours francs</u> pour exercer son droit de rétractation sans avoir à justifier de motifs ni à payer de pénalités, à l'exception, le cas échéant, des frais de retour.	Article 18: (1) The consumer is entitled to withdraw from the instalment sale contract without giving any reason and without incurring any penalties within <u>seven (7) days</u> .	Section 15: (1) In distance selling, the consumer is entitled to withdraw from the contract by notifying the business of the same <u>within 14 days</u> of receiving the confirmation (...)

Annex 3: Cross-country Comparisons of the Implementation of OECD Recommendation on Data Privacy Principles

	Senegal ¹³	Ghana ¹⁴	Mexico ¹⁵
	Loi sur la protection des données à caractère personnel (2008)	Data Protection Act, (2012)	Ley federal de proteccion de datos personales en posesion de los particulares (2010)
Collection limitation principle	Article 34 : La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse." "Article 33 : Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne son consentement.	Article 18 (1) A person who processes personal data shall ensure that the personal data is processed (a) without infringing the privacy rights of the data subject; (b) in a lawful manner; and (c) in a reasonable manner. (2) A data controller or processor shall in respect of foreign data subjects ensure that personal data is processed in compliance with data protection legislation of the foreign jurisdiction of that subject where personal data originating from that jurisdiction is sent to this country for processing.	Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley. Artículo 8.- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.
Data quality principle	Article 36 : Les données collectées doivent être exactes et, si nécessaire, mises à jour. Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles	Article 26 - A data controller who processes personal data shall ensure that the data is complete, accurate, up to date and not misleading having regard to the	Artículo 11.- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

¹³ <http://www.wipo.int/edocs/lexdocs/laws/fr/sn/sn009fr.pdf>

¹⁴ <https://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf>

¹⁵ <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

Regulation for Digital Markets

	sont collectées et traitées ultérieurement, soient effacées ou rectifiées.	purpose for the collection or processing of the personal data	<p>Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.</p> <p>El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.</p>
Purpose specification principle	Article 35, 1st paragraph : Les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.	<p>Article 22. A data controller who collects personal data shall collect the data for a purpose which is specific, explicitly defined and lawful and is related to the functions or activity of the person.</p> <p>17. A person who processes data shall take into account the privacy of the individual by applying the following principles:</p> <p>(c) specification of purpose,</p>	<p>Artículo 12.- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.</p> <p>Artículo 13.- El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.</p> <p>Artículo 15.- El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.</p>
Use limitation principle	Article 35 : Elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement. Elles doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées. Au-delà de cette période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.	Article 25 - Further processing to be compatible with purpose of collection 25. (1) Where a data controller holds personal data collected in connection with a specific purpose, further processing of the personal data shall be for that specific purpose.	Artículo 12.- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.
Security safeguards principle	Article 71 : Le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées,	Article 28. (1) A data controller shall take the necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures to prevent (a) loss of, damage to, or unauthorised destruction; and (b) unlawful access to or	Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no

Regulation for Digital Markets

endommagées, ou que des tiers non autorisés y aient accès. Il prend, en particulier, toute mesure visant à :

Etc.

unauthorised processing of personal data. (2) To give effect to subsection (1), the data controller shall take reasonable measures to (a) identify reasonably foreseeable internal and external risks to personal data under that person's possession or control; (b) establish and maintain appropriate safeguards against the identified risks; (c) regularly verify that the safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated in response to new risks or deficiencies. (3) A data controller shall observe (a) generally accepted information security practices and procedure, and (b) specific industry or professional rules and regulations.

17. A person who processes data shall take into account the privacy of the individual by applying the following principles:

(g) data security safeguards

Article 17. A person who processes data shall take into account the privacy of the individual by applying the following principles

(f) openness,

adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

<p>Openness principle</p>	<p>Article 37 : Le principe de transparence implique une information obligatoire de la part du responsable du traitement portant sur les données à caractère personnel.</p>	<p>(g) data security safeguards Article 17. A person who processes data shall take into account the privacy of the individual by applying the following principles (f) openness,</p>	<p>Artículo 16.- El aviso de privacidad deberá contener, al menos, la siguiente información:</p> <p>I. La identidad y domicilio del responsable que los recaba;</p> <p>II. Las finalidades del tratamiento de datos;</p> <p>III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;</p> <p>IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;</p> <p>V. En su caso, las transferencias de datos que se efectúen, y</p> <p>VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley. En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.</p>
<p>Individual participation principle</p>	<p>Article 58 : Lorsque des données à caractère personnel sont collectées directement auprès de</p>	<p>Article 32. (1) A data subject who provides proof of identity may request a data controller to (a) confirm at reasonable cost to the data subject whether or not the data controller holds personal data about that data subject, (b)</p>	<p>Artículo 28.- El titular o su representante legal podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen.</p>

Regulation for Digital Markets

la personne concernée, le responsable du traitement doit fournir à celle-ci, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

7) l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ;

give a description of the personal data which is held by the party including data about the identity of a third party or a category of a third party who has or has had access to the information, and (c) correct data held on the data subject by the data controller. (2) The request shall be made (a) within a reasonable time; (b) after the payment of the prescribed fee, if any; (c) in a reasonable manner and format; and (d) in a form that is generally understandable.

Article 33. (1) A data subject may request a data controller to (a) correct or delete personal data about the data subject held by or under the control of the data controller that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or (b) destroy or delete a record of personal data about the data subject held by the data controller that the data controller no longer has the authorisation to retain. (2) On receipt of the request, the data controller shall comply with the request or provide the data subject with credible evidence in support of the data. (3) Where the data controller and the data subject are unable to reach an agreement and if the data subject makes a request, the data controller shall attach to the record an indication that a request for the data has been made but has not been complied with. (4) Where the data controller complies with the request, the data controller shall inform each person to whom the personal data has been disclosed of the correction made. (5) The data controller shall notify the data subject of the action taken as a result of the request. Manner of access 34. The provisions of any legislation relating to the right to information of any data subject shall be additional to data subject rights under this Act.

Article 17. A person who processes data shall take into account the privacy of the individual by applying the following principles:

data subject participation.

Article 17. A person who processes data shall take into account the privacy of the individual by applying the following principles:

(a) accountability

Chapter IV of the law deals with the rights of data subjects.

Accountability principle

Article 70 :
Le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions.

Article 17. A person who processes data shall take into account the privacy of the individual by applying the following principles:

Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley