



Information Technology Law in the Global Society

Faculty of Law, University of Latvia


Class 12

5 May 2020

Shawn N. Sullivan



Midterm Grades by Friday



18. Consumer protection

General Consumer Protection Principles



- Many countries regulate business-to-business contracts only very lightly.
 - Freedom of contract.
 - Assumption businesses can take care of themselves.
- But long before the Internet, some countries began imposing special protections for people who purchase items for personal or household use (i.e., consumers).
- The rise of e-commerce presented special challenges for consumer protection, including the fact that the consumer usually doesn't get to see the actual product when buying it.

EU Consumer Rights Directive 2011/83/EU (CRD)

- Applies to all contracts concluded between a “consumer” and a “trader.”
- “Consumer” means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession.
- “Trader” means any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive.





3 Types of Consumer Contracts

- There are 3 categories of consumer contracts under the Consumer Rights Directive:
 1. Contracts concluded outside the trader's business premises (**Off-Premises Contracts**).
 2. Contracts concluded using distance communication (e.g., internet, telephone etc.) (**Distance Contracts**). The parties never meet. Generally all Internet sales are distance contracts.
 3. Contracts other than distance or off-premises contracts (**On Premises Contracts**).

Jurisdiction, choice of law, and consumer disputes

- Consumers who purchase goods or services online often find that
 - The trader is located in a different country.
 - The contract is governed by the law of a different country.
 - The contract determines where litigation may be brought to adjudicate a dispute.
- However, EU law restricts traders' ability to deprive consumers of their rights under their local law and prevents them from being forced to file a consumer action in a state other than their country of residence.



Jurisdiction, choice of law, and consumer disputes

- Consumers who purchase goods or services online often find that
 - The trader is located in a different country.
 - The contract is governed by the law of a different country.
 - The contract determines where litigation may be brought to adjudicate a dispute.
- However, EU law restricts traders' ability to deprive consumers of their rights under their local law and prevents them from being forced to file a consumer action in a state other than their country of residence.



Brussels Regulation (Recast)

Regulation (EU) No 1215/2012

Article 17.1(c) provides (among other things) that jurisdiction over a consumer contract dispute is governed by the Regulation if the other party “pursues commercial or professional activities in the Member State of the consumer’s domicile or, ... directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities.”



Special Rules for
Jurisdiction in
Consumer Contract
Disputes

Consumer's Right to Sue Trader in Consumer's Home Country

- Article 18.1: “A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled.

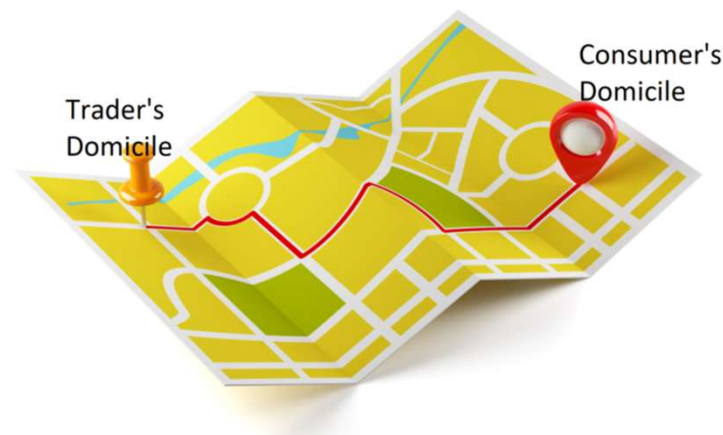
Brussels Regulation (Recast)

Regulation (EU) No 1215/2012



Consumer's Right to Sue Trader in Consumer's Home Country

- Article 18.1: “A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled.”



Brussels Regulation (Recast)

Regulation (EU) No 1215/2012

Consumer Can Be Sued Only in Country of Domicile

Art. 18.2: Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled.

Brussels Regulation (Recast)
Regulation (EU) No 1215/2012



Governing Law for Consumer Contracts

- Where trader directs activities to Member State of consumer's domicile or to several States including the Member State of consumer's domicile, and the contract falls within the scope of such activities, the contract will be governed by the law of the state of the consumer's domicile.
- The parties can agree that the contract will be governed by another state's law, but the choice of law provision in the consumer contract "have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law" of the consumer's domicile country.

Article 6 of the Rome I Regulation

Regulation (EC) No 593/2008



Rome I Regulation



Consumer Rights to Information in Distance Contracts

- Articles 6-8 of Consumer Rights Directive contain rules about pre-contractual information obligations for distance contracts, including:
 - The content of the information.
 - Identity of trader.
 - Trader's contact information.
 - Price & other costs.
 - Any delivery restrictions.
 - The time when the information must be given.
 - If the contract is concluded on the Internet, the information must be provided immediately before consumer places order.
 - Burden of proof. and certain formal requirements.
 - Burden of proof of compliance with the aforementioned obligations is on the trader

Consumer's Right of Withdrawal

“Since in the case of **distance sales**, the consumer is not able to see the goods before concluding the contract, he should have a right of withdrawal.... Concerning **off-premises contracts**, the consumer should have the right of withdrawal because of the potential surprise element and/or psychological pressure. Withdrawal from the contract should terminate the obligation of the contracting parties to perform the contract.”

Recital 37 of Consumer Rights Directive.





Consumer's Right of Withdrawal

“Save where the exceptions provided for in Article 16 apply, the consumer shall have a period of 14 days to withdraw from a distance or off-premises contract, without giving any reason, and without incurring any costs other than those provided for in Article 13(2) and Article 14.”

Article 9.1 of Consumer Rights Directive.

For more details on the Latvian Regulations

lexology.com/library/detail.aspx?g=d22e58ab-1b7a-433a-9707-ed1e460a79b0


LEXOLOGY Store Blog Events Popular Influencers About

Latest Coronavirus GTDT Research Learn Webinars Instruct

Back Save & file View original Forward Print Share Follow Like

Distance contracts and consumers rights - new regulation

SORAINEN



SORAINEN

Latvia | July 23 2014

Technological development allows businesses and consumers to choose ever more ways to sell and buy services and goods. In the meanwhile, new forms of goods and services appear that clearly result from development of new technologies. Choosing and ordering goods and services over the internet or the web has become the norm. Likewise, ordering goods and services over the phone, e-mail or TV is still topical. In all these cases when a buyer and a seller who are not at the same location agree on buying a product or service and they use these various means of distance communication, a distance contract is concluded. When these deals are made with consumers, this field is regulated by laws and regulations based on European Union (EU) law and that introduce the requirements of an EU directive. Thus on 13 June this year, amendments to the Consumer Right Protection Law and new Cabinet Regulations of 20 May 2014 regulating distance contracts came into force.

The new regulations¹ impose new legal obligations on sellers and service providers, including giving additional information to the consumer before entering into a contract. Likewise the new regulation adds to the scope of consumer rights, eg, to receive information before entering into a contract.

Regulating spam

The term "spam" refers to unsolicited commercial email (UCE) or unsolicited bulk email.



Regulating Spam: Art. 13 of Directive on Privacy and Electronic Communications



This Directive is widely believed to be in need of revision for new tech.

1. “The use of **automated** calling systems without human intervention (automatic calling machines), facsimile machines (fax) or **electronic mail** for the purposes of **direct marketing** may **only be allowed** in respect of subscribers who have given their **prior consent**.”
2. [Exception where marketer obtained email contact info from an earlier sale & marketer offers its own similar products/services, **if** “customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details.”]
...
4. “[S]ending electronic mail for purposes of direct marketing **disguising or concealing the identity of the sender** on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, **shall be prohibited**.”

Proposed E-Privacy Regulation



Has been under consideration for years but is still not finalized.

Intended to regulate the privacy of electronic communication data.

General Data Protection Regulation (GDPR) Applied to E-Mail Marketing

- GDPR will be discussed in more detail soon.
- For consent to be valid under GDPR, customer must actively confirm consent, such as ticking an unchecked opt-in box. Pre-checked boxes that rely upon customer inaction to assume consent are not valid under GDPR.
- “When assessing whether consent is freely given, utmost account shall be taken of whether... the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.” Art. 7(4).
- “The data subject shall have the right to withdraw his or her consent at any time. (...) It shall be as easy to withdraw as to give consent.” Art. 7(3).
- Requirement to retain evidence of consent. Art. 7(1).



- Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to \$43,280.

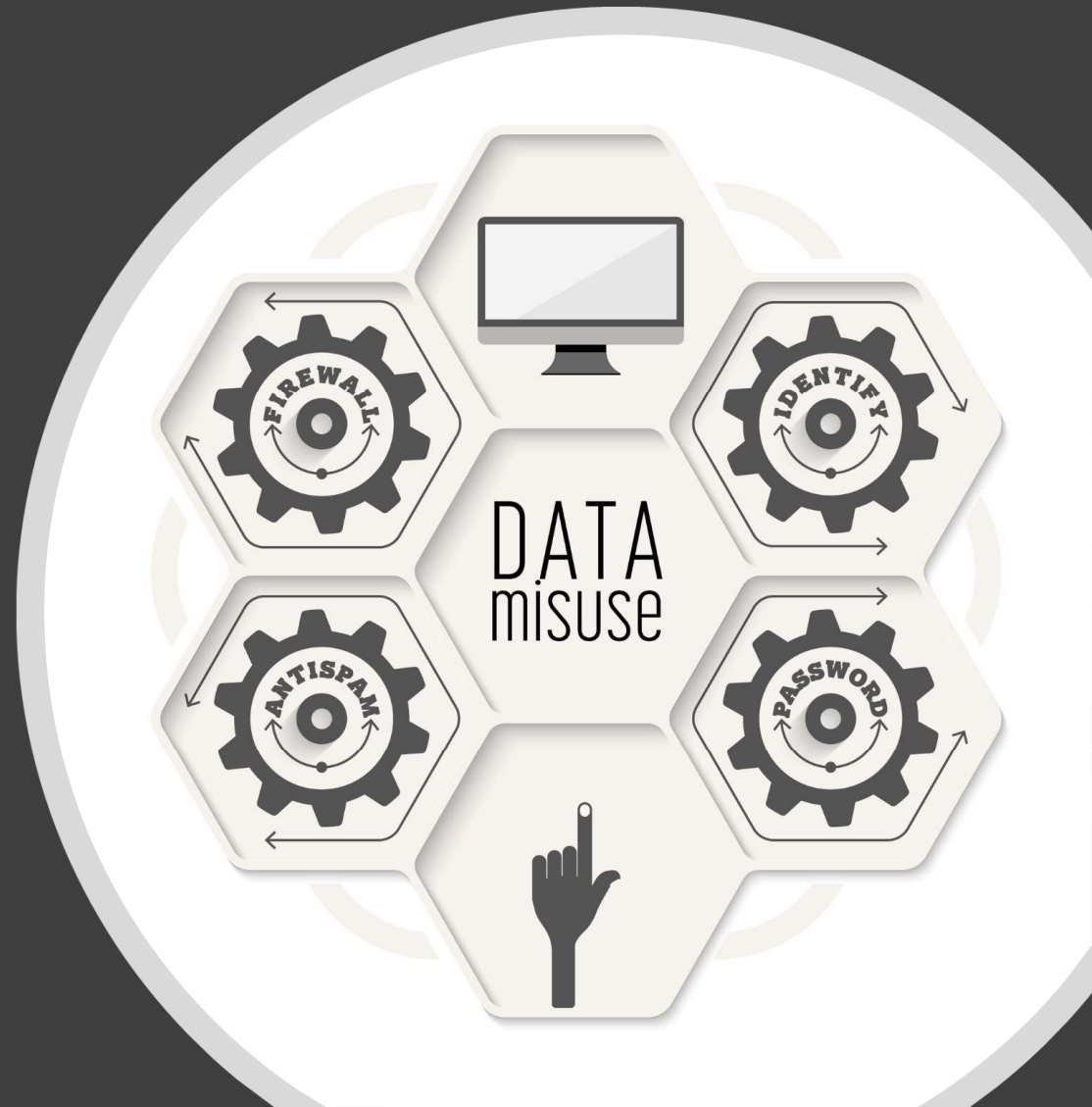
- Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to \$43,280.
- Prohibits:
 - False or misleading email header information.
 - Deceptive subject lines.
- Requires:
 - Clear identification that the message is an advertisement.
 - Valid physical postal address.
 - Clear and conspicuous explanation of how recipient can opt out of receiving further emails in the future.
 - Processing of opt-out requests for at least 30 days after message is sent.



Question 1

Liam is a student in London. He has recently bought a new laptop computer from 'computadoras para la venta' (CPV), an online retailer in Spain. The laptop was sold under CPV's standard terms and conditions which state that the contract is concluded when the goods are shipped and that goods may only be returned for a refund if they are faulty under Spanish law. They also state that the contract will be governed by Spanish law and is subject only to the jurisdiction of the Spanish courts. They further state that refunds will only be given if goods are returned in their original packaging within seven days of receipt and that the buyer must bear the cost of both the return and original shipping costs. The CPV website makes no reference to any right to cancel under distance selling regulations and indeed gives few details about CPV. There is no business address, company registration, or tax details. The returns address is simply a PO Box. Liam has had the laptop for six weeks and has found in the last two weeks that there are problems with the power supply, which means that at times the laptop is rendered unusable. This could be remedied by simply having a new power supply module supplied but CPV say they do not do this and in any event this does not make the laptop faulty under Spanish law and more than seven days has passed. They refuse to talk to Liam any further.

19. Computer Misuse



Early Hacking Cases

- Textbook refers to early English case in early 1980s involving unsuccessful attempt to prosecute the unauthorized accessing of a computer system under the historic UK forgery statute.
- At the time there were virtually no laws anywhere specifically addressing hacking, and laws developed for the analogue world didn't fit.
- U.S. Congress enacted the Computer Fraud and Abuse Act in 1986.
- UK Parliament enacted the Computer Misuse Act 1990.



U.S. Computer Fraud and Abuse Act

- Obtaining National Security Information.
- Accessing a Computer and Obtaining Information
- Trespassing in a Government Computer.
- Accessing to Defraud and Obtain Value.
- Damaging a Computer or Information.
- Trafficking in Passwords.
- Threatening to Damage a Computer.
- Attempt and Conspiracy.

Criminal penalties & civil remedies



HACKER



BRUTEFORCE



VIRUS



TROJAN HORSE

UK Computer Misuse Act 1990

Prohibits:

- unauthorised access to computer material
- unauthorised access with intent to commit or facilitate commission of further offences
- unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.





Convention on Cybercrime of the Council of Europe - Budapest Convention

- Signed 21 November 2001 / in force since July 2004
- Ratified by all Council of Europe states except Ireland & Sweden
- In force in Latvia since 2007.
- Also ratified by several non-COE states, including Canada, Japan, South Africa, the United States, Australia, Panama, Dominican Republic.

“[T]o deter action directed against the **confidentiality, integrity and availability** of **computer systems, networks and computer data** as well as the **misuse** of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable **international co-operation**.”

Purpose of the Budapest Convention

Some Budapest Convention Definitions

“Computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

- Includes smartphones that produce, process, & transmit data.

“Computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.



Offenses under Budapest Convention

Article 2 – **Illegal access**: Accessing the whole or any part of a computer system without right.

Article 3 – **Illegal interception**: Interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system.

Article 4 – **Data interference**: damaging, Deletion, deterioration, alteration or suppression of computer data without right.

Article 5 – **System interference**: Serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – **Misuse of devices**: Production, sale, possession, etc., of devices for committing the above offenses.

Article 7 – **Computer-related forgery**: Input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic

Article 8 – **Computer-related fraud**: Alteration, deletion, etc., of data or interference with system for purpose of obtaining an economic benefit.

Article 9 – **Offences related to child pornography**.

Article 10 – **Offences related to infringements of copyright and related rights**.



EU Directive 2013/40/EU on Attacks against Information Systems

- European Union has limited competence to legislate in criminal law but harmonizes Member States' laws regarding:
 - Art. 3: Illegal access to information systems.
 - Art. 4: Illegal system interference.
 - Art. 5: Illegal data interference.
 - Art. 6: Illegal interception.
 - Art. 7: Tools used for committing offences.



Latvia Criminal Law

Section 241. Arbitrary Accessing Automated Data Processing Systems

(1) For a person who commits arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused thereby,

the applicable punishment is the deprivation of liberty for a period of up to two years or temporary deprivation of liberty, or community service, or a fine.

(2) For a person who commits the criminal offence provided for in Paragraph one of this Section, if it has been committed for the purpose of acquiring property,

the applicable punishment is the deprivation of liberty for a period of up to four years or temporary deprivation of liberty, or community service, or a fine, with or without the confiscation of property.

(3) For the acts provided for in Paragraph one of this Section, if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security,

the applicable punishment is the deprivation of liberty for a period of up to five years or temporary deprivation of liberty, or community service, or a fine, with or without the confiscation of property.

[25 September 2014]



Latvia

Section 243. Interference in the Operation of Automated Data Processing Systems and Illegal Actions with the Information Included in Such Systems

(1) For a person who commits unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby,

the applicable punishment is the deprivation of liberty for a period of up to two years or temporary deprivation of liberty, or community service, or a fine.

(2) For a person who knowingly commits interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused,

the applicable punishment is the deprivation of liberty for a period of up to three years or temporary deprivation of liberty, or community service, or a fine.

(3) For the criminal offence provided for in Paragraph one or two of this Section, if it has been committed for the purpose of acquiring property,

the applicable punishment is the deprivation of liberty for a period of up to five years or temporary deprivation of liberty, or community service, or a fine, with or without the confiscation of property and with or without probationary supervision for a period of up to three years.

(4) [13 December 2012]

(5) For the commission of the acts provided for in Paragraph one or two of this Section, if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to the political, economic, military, social or other security of the State, or for the criminal offence provided for in Paragraph one or two of this Section, if it has been committed by an organised group,

the applicable punishment is deprivation of liberty for a period of up to seven years, with or without confiscation of property and with or without probationary supervision for a period of up to three years.

[28 April 2005; 13 December 2007; 8 July 2011; 13 December 2012; 25 September 2014; 8 June 2017]



Latvia

Latvia Criminal Law

Section 244. Illegal Operations with Automated Data Processing System Resource Influencing Devices

(1) For a person who commits the illegal manufacture, adaptation for utilisation, disposal, distribution or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for the purpose of committing a criminal offence,

the applicable punishment is the deprivation of liberty for a period of up to two years or temporary deprivation of liberty, or community service, or a fine.

(2) For the commission of the same acts, if serious consequences have been caused thereby,

the applicable punishment is the deprivation of liberty for a period of up to five years or temporary deprivation of liberty, or community service, or a fine.

[28 April 2005; 13 December 2012; 25 September 2014]



Latvia

Latvia Criminal Law

Section 245. Violation of Safety Provisions Regarding Information Systems

For a person who commits violation of provisions regarding information storage and processing which have been drawn up in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerised information systems, if it has been committed by a person responsible for conformity with such provisions, if it has been a cause of stealing, destruction or damage of the information, or other substantial harm has been caused thereby,

the applicable punishment is a temporary deprivation of liberty or community service, or a fine.

[13 December 2012]



Latvia

Latvia Criminal Law

Next Week's Reading

Chapters 22 and 23

