Law in Cyberspace Summary

Lars Jeurissen, s1022856

January 19, 2022

1 What is Law

1.1 Definition of law

- There is *no clear definition* about what law is.
- However, law aims for legal certainty:
    1. You can find the rule in a statue. (Clarity of a rule preferred over nuanced rule)
    2. Certainty that law will be enforced.
    3. Certainty that law is applied consistently. (Similar cases will be treated similarly)
- But: law that's relevant for CS is often still developing! There are many grey areas in law.

1.1.1 Types of law

- Difference Europe and UK:
    - **Europe**: *Civil Law* - focuses on legal statutes
    - **UK**: *Common law* - focuses on case law (judge-made law)

    But, a difference of degree, case law is also relevant in civil law and statues also in common law
- Difference between national and international law:
    - **National laws**: applies within a state
    - **Public international law**: applies between states

1.2 Sources of law

- **Treaties**: A treaty binds the states that ratified the treaty and sometimes binds citizens (e.g. European Convention on Human Rights, or Treaty on the Functioning if the EU)
- **Legislation**: Enactments of a lawmaker, including constitution! Imposes legal norms on those within jurisdiction
- **Case law**: Collection of legal decisions by courts
- **Doctrine**: Texts by influential legal scholars (influential in civil law, not so in common law)
- **Fundamental principles of law**: General and abstract rules, implied in other legal sources (e.g. treat equal cases equal, government agencies should be impartial)
- **Customary law**: In absence of written law, but rare. Requires *Usus* (a habit of acting in a certain way) and *Opinio necessitatis* (shared opinion that habit is based on a duty) (e.g. prohibition of genocide)

1.3 What law does

- Law has *legal effect*: sometimes saying something makes it so. Examples:
    1. A civil servant pronounces that two people are married, after that, they are.
    2. Government appoints Supreme Court judge.
    3. A court says that a statue is invalid because it breaches a higher legal norm.
- What the law says can even lead to punishment and jailtime (important difference with habit, morals and ethics, where this is not the case)

1.4 Legal Rights

- Rights represent interests that are protected by law. 3 categories:
    1. **Rights against a person**: claims (rights *in personam*). E.g. a contract
    2. **Rights on an object**: property rights (rights *in rem*). E.g. ownership, intellectual property rights
    3. **Fundamental rights**: human rights. E.g. rights to privacy, right to freedom of expression, freedom from slavery
- Rights are always about the relationships between legal subjects (natural person/legal person)
- Typically, a right corresponds with a duty (Bob must repay 10 Euro to Alice) or the lack of a right (Bob may not take Alice's car)

2 Legal Reasoning and CJEU

2.1 Court of Justice of the European Union & Data Retention Directive 2014

- The **Court of Justice of the European Union (CJEU)** is based in Luxemburg
- It is the highest authority on explaining EU law
- National judges can/must ask CJEU about the interpretation/validity of EU law
- CJEU is **not** the European Court of Human Rights! Anyone can go to the ECHR, but not everyone can go to the CJEU
- Example is the **Data Retention Judgement**, which was a case about storing metadata of internet behavior. This had to be weighed against the Charter of Fundamental Rights of the European Union.
- Relevant rights (articles): 'Respect for private and family life' and 'Protection of personal data'
- However, human rights are rarely absolute, in certain cases they can be limited
- CJEU said that metadata retention serves a goal of general interest (fighting terrorism), however, they said it would go too far
- Eventually, CJEU said that the **Data Retention Directive** was invalid, because of a lot of reasons (invalid level of security, way too much surveillance)
- Following that, national laws that were implemented from the directive were still valid, but after court cases they became invalid all over the EU

2.2 Legal Reasoning

- Generally, legal reasoning looks like this:
    - **Major**: If a then b (**legal rule**)
    - **Minor**: a is the case (**facts**)
    - **Conclusion**: b (**legal effect**)
- Sometimes, two rules are in conflict. There are three possibilities to deal with this:
    1. **Lex specialis** More specific rule overrides more general rule
    2. **Lex posterior** Newer rule overrides older rule
    3. **Lex superior** Hierarchy among lawmakers (e.g. national law overrides city ordinance)
- Law is related to:
    - **Politics** (who establishes the law?)
    - **Morality & ethics** (how should people behave?)
    For example:
    1. Law shapes the playing field for politics (e.g. grants powers to police, but also imposes limits)
    2. Law creates level playing field for individuals and companies to act ethically (no environment pollution)
    3. Law enables and constrains politics (voting, constitution, respect for human rights)
- Helbert Hart said that it's typical for law to combine
    - **Primary rules** How to behave (e.g. 'Killing people is prohibited', 'Don't store data longer than necessary')
    - **Secondary rules** How to establish primary rules (e.g. 'How can a statute be developed?')
- Concept of law, argued by Gustav Radbruch:

- **Legal positivism**: All law is **positive law**, meaning law that was created by being laid down. (written law, not ethical, god, etc.)
- However, if the difference between what positive law says and what justice requires becomes so big, an exception is made, and legal certainty must give way to justice
- But generally, positivist law applies, even if it leads to an unfair result

3 Domains and fields of law

- Legal rules require things from and give rights to **legal subjects**:
  - **Natural persons**: humans
  - **Legal persons**: e.g. company with limited liabilty (B.V./N.V.), foundation, municipality
- There are three domains of law:
  - **Private law**: Government as such does not play a role (relations between citizens). Can be divided into:
    * Property law
    * Contract law
    * Tort law
    * Family law, law of commerce, and more...
  - **Public law**: Field of law that regulates the state. Can be divided into:
    * Constitutional law: Constitution etc. (how is the state designed)
    * Administrative law: On relation between state and citizens (vertical law)
  - **Criminal law**

3.1 Private law

3.1.1 Contract law

- Set of rules and principles that govern transactions between parties, setting the rules and obligations of the parties.
- Law requires no formalities here! For example, buying things in a supermarket does not involve signing a contract, but you do enter a contract.
- Roughly: Law requires more formalities if the risk of both parties increases.
- Even if law requires no formalities, people can make a written contract. This is useful for proving things to a judge.
- A contract is usually about making an exchange, but not always.
- Important: Freedom of contract. Parties can choose whether they want to enter a contract, with whom, and about what.
- Freedom of contract is not absolute, though. Discrimination, hiring killers, selling organs, babies, sex, etc. usually not allowed.
- Individual autonomy is important, in principle, people are free to enter contracts
- Contract law should also be fair, many rules aim at protecting weaker parties (e.g. consumer protection law)

3.1.2 Property law

- There are two types of rights in private law:
  - **Property rights**: 'Absolute' rights, can be invoked against everyone ('erga omnes')
  - **Relative rights**: Can be invoked against a particular legal subject, e.g. a claim because of a contract
- Property rights have two subcategories:
  - **Tangible** (= tastbaar): e.g. house, land, car, etc.
  - **Intangible**: e.g. trademarks, copyrights, patents, etc.

3.1.3 Tort law

- Tort law is about damages. Basic rules: everybody bears their own damage. Tort law is about the exceptions.

- It is possible to claim damages from another legal subject.
- Two categories of liability:
    - **Fault liability**: A is liable for damage caused to B, because A *wrongfully* caused damage
    - **Strict liability**: A is liable for damage caused to B, even though A did not *intentionally or negligently* cause that damage. Two categories:
        1. Liability for damage caused by somebody else (e.g. parents liable for damage by children)
        2. Liability without tortfeasor, for damage caused by defective or dangerous thing or activity (e.g. owners liable for damage by pets). Incentives: protection for injured party, incentive for improving safety, better options for insurance, limiting procedural costs

3.2 Public law

3.2.1 Constitutional law

- Field of law that regulates the state; the state should comply with legal rules.
- E.g.: constitution (grondwet), convention of human rights, charter of fundamental rights.
- Constitutions are usually harder to amend.
- Usually a written document (sometimes scattered across multiple documents, in UK)
- Many constitutions aim at separation of state power: Trias Politica:
    1. Creating legislation (legislator, e.g. parliament)
    2. Practical implementation of rules (government)
    3. Deciding disputes (courts)
- Trias Politica not completely pure nowadays. Most important thing: **checks and balances**.
- Sometimes controversial: legislator and government should set policy, not judges

3.2.2 Administrative law

- Administrative law is about the relation between state and citizens.
- Has grown a lot, since more functions are expected from state: peace, infrastructure, healthcare, ...
- Typical topics in administrative law:
    - Administrative authorities (e.g. RIVM, DPA (Data Protection Authority))
    - Objection procedures
    - Protection by courts against the state
- Two functions of administrative law:
    1. **Instrumental function**: Rules that bind the administration in its tasks
    2. **Safeguarding function**: Rules about supervision by courts

3.3 Criminal Law

- Very roughly: rules by which the state prohibits certain forms of conduct, enable punishment, procedures for the above
- There are *a lot* of unlawful actions, but only a small subset of those are **criminal offences**
- Criminal law court cases are between the state and the defendant (possibility for punishment)
- Two important functions of criminal law:
    1. Tool to maintain public order and control deviant social behaviour
    2. Tool to protect the human rights of civilians (incl. criminals) against the state
- Distinction between **substantive law** and **procedural law**:
    - **Substantive law**: Rules that give people rights, or determine what people should (not) do
    - **Procedural law**: Rules for court proceedings, the organisation of the judiciary
- Always tension between security and liberty
- Important underlying human right: presumption of innocence (= innocent until proven guilty)

4 International law and EU law

4.1 International law

- Originally two types of law:

- **National law**: About legal relations within a single State and the organisation of that State
- **International law**: About the legal realtions between States

But, the distinction is no longer so clear (e.g. EU law)
- **Jurisdiction** roughly refers to legal power and where such power is applicable:
  1. The competence to legislate, adjudicate, and enforce
  2. The territory or domain over which an entity holds jurisdiction in the first sense
- Law is primarily national law (since 1648). Internal sovereignty: each state has exclusive power within its own territory. External sovereignty: principle of non-interference.
- The main actors in international law are States, but there are also NGOs, international organisations (e.g. UN) and individuals
- The sources for international law include:
  - **Treaties** (e.g. European Convention on Human Rights and Cybercrime Convention)
  - **Customary law** (Usus and Opinio necessitatis)
- We have Monism and dualism:
  - **Dualism** is where national and international law are 2 different legal orders (e.g. in the UK), and the state must implement a national statue after signing a treaty
  - **Monism** is where national and international law are part of 1 legal order (e.g. in NL, judges can apply ECHR)
- Roughly: national statute provisions do not apply if they conflict with binding treaty provisions

4.2 The law of Europe

- Supranational law is a form of international law where a state gives part of their sovereignty to a supranational organisation (e.g. EU law)
- European Union started in 1952, as the 'European Coal and Steel Community'
- European Union is covered by treaties (last update in 2007)
- Sources of EU law:
  - **Primary EU law**:
    * Treaty on the European Union (TEU)
    * Treaty on the Functioning of the European Union (TFEU)
  - **Secondary EU law**:
    * **Regulations**: A regulation has general application, and is binding in all member states (e.g. GDPR).
    * **Directives**: A directive is a result that each Member State should achieve, but can choose how to themselves (e.g. Data Protection Directive (pre-GDPR)).
    * **Decisions**:
    * **Case law**, Court of Justice of the EU (CJEU):
- Main EU institutions (all in Brussels, except CJEU (Luxemburg)):
  - **European Commission (EC)**: Proposes and enforces laws, manages the EU
  - **European Parliament (EP)**: Adopts laws, can't propose laws
  - **European Council**: 27 heads of state, decide priorities and political direction of EU
  - **Council of the EU**: Also called 'Council', or 'Counsil of Ministers' 27 relevant ministers, e.g. agriculture ministers, justice ministers, etc., also have a role in adopting laws, just like European Parliament.
  - **Court of Justice of the EU (CJEU)**: Interprets EU rules. Gives advise to national judges.
- The Internal Market consists of four freedoms:
  1. Free movement of goods: Transporting things (no taxes and quantitative restrictions)
  2. Free movement of people: You can take a job in Germany
  3. Free movement of services: You can paint houses in Germany
  4. Free movement of capital: Investing in other EU states is possible
- Two limitations on power of EU, two important requirements:
  1. **Legal Basis**: EU can only do what Member States allow it to do (e.g. no secret services)
  2. **Subsidiarity**: EU can only act if conforms with subsidiarity (= only do something if the member states can't do it better) and proportionality (= measures should be suitable, necessary, and not worse than the problem it addresses).
- Euroscepticism (and Brexit), 3 factors:

1. The feeling of a community is lacking (people don't feel like an 'EU citizen')
2. EU has grown very large very quickly, big differences between views. Also: decision-making became harder, because more members.
3. 'Democratic defecit' of the EU (how much we can influence the EU). This is debatable.

5 Human Rights

- Human Rights (or fundamental rights) are right that:
    1. every person has
    2. by virtue of existing
    3. that aim to secure for that person certain benefits or freedoms that are of fundamental importance to any human being.
- There are some national and regional differences. E.g. in the US, freedom of expression has more weight than privacy. In Europe, same weight.
- United Nations (UN): (non-enforced) Universal Declaration of Human Rights, 1948
- More relevant: European Convention on Human Rights, treaty of the Council of Europe (COE).
- The CEO is NOT the EU! The CEO is the most important human rights organisation in Europe. 47 member countries, including 27 EU member states.
- In Europe, human rights protect natural persons and legal persons.
- Human rights have duty bearers, typically the state (vertical relations). Nowadays, more and more between private actors, too (horizontal relations). E.g. GDPR.
- Types of duties:
    - **Negative/liberty rights**: Demand that the state does **not** do something (e.g. torture)
    - **Positive/welfare rights**: Demand that the state **does** do something
- Positive rights are typically more controversial as they are typically more expensive
- Human rights are largely driven by courts
- There are three generations of human rights:
    1. Liberty rights
    2. Social and economic rights
    3. Newer, more controversial construction: Obligations towards nature etc.
- Examples of human rights include the Right to life, Prohibition of torture, Prohibition of slavery, Right to liberty, Right to a fair trial, Right to privacy and Freedom of expression

5.1 The right to privacy

- Privacy is notoriously hard to define, law must constantly be adapted to new developments in technology. There are three perspectives:
    1. **Confidentiality**: The right to be let alone
    2. **Control**: Having control over your own personal information (heavily embedded in GDPR)
    3. **Identity construction**: Freedom from unreasonable constraints on the construction of one's own identity
- Human right to privacy and private life (private and family life, home, and correspondence)
- This right is not absolute, can be restricted under circumstances
- Case law is important, ECtHR decides on cases (e.g. telephone is also privacy)
- ECtHR does not use a single definition of privacy, to be adaptive
- Most national constitutions also protect privacy (many additional rules, e.g. stalking prohibited)

5.2 The right to data protection

- Welfare state led to large-scale data collection, people were worried
- To combat this, data protection law was invented. Council of Europe adopted (non-binding) resolutions that called upon member state to create data protection.
- Since a lot of different laws, EU stepped in, created Data Protection Directive
- Then also Charter of Human Rights was created. Copies right of privacy, and added right to protection of personal data:
    1. Everyone has the right to the protection of personal data concerning him or her

2. Such data must be processed fairly for specified purposes, and lawful
3. Everyone has the right to access and delete data concerning him or her
4. Compliance with these rules shall be subject to control by an independent authority. This is important, because Data Protection Authorities (DPAs) must enforce rules against public and private law.

6 The GDPR: when does it apply?

- The GDPR starts with recitals which help interpret law, but are not actually binding. Instead, read the provisions (articles) that come after.
- GDPR adopted in 2016, applies since 25 May 2018 (replaced DPD)
- Important new point for the GDPR was that DPAs can impose huge fines (up to 20m or 4% of worldwide turnover)
- The GDPR applies to the *processing* of *personal data*.
- **Personal Data** is any information relating to an *identified or identifiable natural person* (**data subject**); an identifiable natural person is one *who can be identified*, directly or indirectly, *in particular* by reference to an identifier *such as* a name, ID, location, . . .
- Data **Processing** includes almost anything: 'Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.
- There are exceptions to the processing of personal data:
    - Outside scope of EU law (secret services)
    - Household activity (contact list in phone)
- Two main players in data processing:
    - **Data subject**: Person whose personal data are processed
    - **Controller**: Body that determines purposes and means of processing the data
    - **Processor**: Processes personal data for the controller (may not use personal data for its own)
- Territorial scope of GDPR:
    1. Controllers established in the EU
    2. Controllers outside the EU, when processing is related to offering services to subjects in the EU or monitoring of behavior of EU citizens as far as their behavior takes place within the EU

7 GDPR

7.1 Principles

- GDPR applies to private and public sector, applies immediately as personal data are processed (omnibus approach).
- Advantage: when new technology is developed, the law doesn't need changing
- Disadvantage: Rules must be quite general and abstract, which leads to discussions
- The 7 overarching GDPR principles:
    1. Lawfulness, fairness & transparency
        - Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
        - Clear information required (e.g. privacy notice)
    2. Purpose limitation
        - Personal data shall be collected for specified, explicit and legitimate purposes.
        - It is not allowed to save data for 'data might become useful', 'for commercial goals', etc.
        - Data that is processed for one purpose, cannot be processed for another purpose
    3. Data minimisation
        - Data shall be adequate, relevant and limited to what is necessary
        - Prohibited: collection as much data as possible
    4. Accuracy
        - Personal data shall be accurate and, where necessary, kept up to date.
        - Standards for accuracy depend on the goal of the data processing
    5. Storage limitation
        - Personal data shall be kept in a form which permits identification of data subjects for no

longer than is necessary
- Prohibited: keeping data for a long time, 'just in case'
- It can be unclear how long you can keep data, GDPR says 'no longer than necessary'
6. Integrity and confidentiality
   - Personal data shall be processed in a manner that ensures appropriate security of the personal data
   - Data should be protected against external and internal threats
   - The GDPR does **not** require *perfect* security, only *appropriate security*
   - Also: data breach notification requirement:
     * To DPAs, unless risk for data subjects are unlikely
     * To data subject, when 'high risk to the rights and freedoms of natural persons'
7. Accountability
   - The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 ('accountability')
   - Concrete: controllers must maintain records about their processing
   - Sometimes a data protection officer (DPO) is required (independent person!).

7.2 Legal basis

- When processing data, a legal basis for this processing is required
- The requirement for a legal basis applies *in addition to* the other GDPR rules
- There are 6 possible legal basis:
  1. **Consent**
     - Requirements for valid consent are that the information is:
       (a) freely given, (literally no form of external pressure is allowed)
       (b) specific, informed and
       (c) unambiguous indication of the data subject's wishes
     - Usually, a clear action is required (e.g. slider or button)
     - It is **not** allowed to hide consent in e.g. terms and conditions or opt-out system
  2. **Contract**
     - Allowed when data is necessary for the performance of a contract in which the data subject is party (e.g. pizza service needs address to deliver pizza)
  3. Legal obligation for controller
     - When required by law: e.g. when storing data for the tax office
  4. Vital interests of data subject or other person
     - When in vital interest: e.g. when you've been in an accident and people need information from your doctor, but you can't give consent
  5. Task in the public interest
     - Typically when state bodies use personal data.
     - In most cases, a statue exists to say what state bodies can do with the data
  6. **Legitimate interests that override data subject's interests**
     - Very complex legal basis
     - Allowed only when processing is necessary for legitimate interests of the controller, except where such interests are overriden by the interests/rights of the data subject.
     - Example: data can be kept for e.g. better customer service by a pizzeria, or sending a menu by post, etc.
     - But: data subject can also object! When marketing is involved, this right is absolute.
- In the private sector, consent, contract and legitimate interests are the most relevant

7.3 Special categories of data

- Sometimes called 'sensitive data' (not fully correct)
- Special categories of data include racial or ethnic origin, political opinion, etc.
- Main rule is that use of special category data is prohibited
- Exceptions exist:
  1. Explicit consent

    2. Medical sector
    3. Public interest in the area of public health
    4. And some more specific and narrowly defined exceptions...
- Even if an exception applies, data controller must still have a legal basis

7.4 Various GDPR topics

Note: a lot of these topics have already been discussed and are already in the summary

- Responsibilities of data controllers:
  - Accountability; the controller must keep records of its data management (decisions)
  - Detailed transparency requirements, information must be given to data subjects
  - Data protection should be by design and by default, e.g. should be built into systems
  - The security of data must be accurate
  - Data breaches must be notified
- Rights of data subject rights (e.g. access rights)
  - The data subject has the right to ask for all data that a controller has of them.
  - The controller must explain which data it has on you, for which purpose, etc.
- GDPR enforcement
  - DPAs can impose fines
  - Data subject can complain to DPA, sue controllers, or go to NGOs

8 Cookies and GDPR judgement

- Concerned with e.g. cookies
- Very roughly summarised: storing or accessing information on a user's device only allowed after consent
- Exception when storing is necessary for service requested by user or for transmitting communication
- Refers to GDPR for consent
- You have cookie/tracking walls (that deny access if you don't accept cookies), EDPB say that tracking wall does not comply, but no case law yet
- Has fines like in GDPR, but unclear wheter it will be adopted (as council of ministers made it stricter)

9 Cybercrime and Cybersecurity

- **Cybercrime** concerns a broad range of different criminal activities where computers/information systems are involved either as a primary tool or target
- So, there are crimes with a computer (e.g. sending spam) and crimes against a computer (e.g. DDoS), but also crimes in the context of computers (e.g. online child pornography)
- **Cybersecurity** is about the preservation of the availability and integrity of computer systems and infrastructure and the confidentiality of the information contained therein
- So, about the preservation of CIA
- There is overlap between cybercrime and cybersecurity when the computer is the object of the crime

9.1 Cybercrime

Cybercrime is special because of Distance (problem for law, possibly no jurisdiction), Scale (can be automated), Speed, Distribution (hard to determine authorship of crime), Invisibility (criminal is hard to find) and Visibility (Makes victims visible)

9.1.1 Cybercrime Convention (CC)

The most important international instrument against cybercrime is the **Cybercrime Convention (CC)**:

- An international treaty which is implemented through national law
- Made by the Council of Europe, but also open to other countries

- It does a number of things:
  1. Defines cybercriminal activities
  2. Creates competences for cybercrime investigation (adapted to specificities of cybercrime)
  3. Thereby creates legal certainty (definition of offences and corresponding investigative powers)
  4. It has proportionality between the fight against cybercrime and preservance of fundamental rights (privacy, protection of data)
- It protects against **CIA crimes**:
  - **Illegal access**: e.g. hacking. Not directly a CIA crime, as it does not do anything to data yet. It is a preliminary step.
  - **Illegal interception**: interception of non-public transmission of computer data (e.g. active or passive MITM)
  - **Data interference**: Damaging, deletion, deterioration, alteration or suppression of computer data (e.g. ransomware)
  - **System interference**: The serious hindering of a computer system (e.g. DDoS)
  - **Misuse of devices**: mainly black market
  - **Forgery**: Creation of inauthentic data
  - **Fraud**: Act against a victim in order to cause a loss of property (attempt is not sufficient, has to succeed!)
  - **Prohibition of child pornography**: Also *a person appearing to be* or *realistic images presenting* a minor engaged in sexually explicit conduct
  - **Prohibition of copyrights infringements**: Establish as criminal offences under its domestic law the infringement of copyright and related rights
- Note that there are **legal conditions** for each of these crimes, the conditions are displayed in the slides
- It defines the powers of competent authorities to investigate cybercrime. Each power must be grounded into a legal basis (principle of legality). The following powers exist:
  - Competent authorities can order:
    a) Of a person **in its territory**, specified computer data in that person's possession or control and data that is stored in a computer system or a computer-data storage medium (e.g. USB stick)
    b) Of an internet provider offering its services in the territory ANY information relating to services in its possession or control (metadata)
  - Additional competences include real-time collection of traffic data and real-time interception of content data (this is the only provision about content of the data)
  - Search and seizure of stored computer data. Competent authorities can:
    * Search or access computer systems and/or data and computer-data storage mediums
    * Perform a Network search, search other computer through the original computer (but only if there are grounds to believe that the data sought is stored there)
    * Make and retain a copy, and render data inaccessible or remove it
    * Ask for passwords
- **Legality Principle**: All offenses must be in the law, and all powers for competent authorities must be in the law
- Powers and procedures must be subject to safeguards provided for under its domestic law (adequate protection of human rights, and must incorporate proportionality). Safeguards include judicial supervision, grounds, limitation of the scope and duration of power. Furthermore, the impact must be considered (proportionality test!)

9.2 Cybersecurity

- Cybersecurity is key to the EU, as internal markets and activities are being digitalized
- Most important and key legal measure is the **Network and Information Security Directive (NIS)**, its goal is to achieve a high level of cybersecurity
- But, the GDPR also addresses cybersecurity (in the form of security and data breaches)
- In the GDPR, a **risk-based approach to security** is taken, which is to ensure that an appropriate level of security for the risk is ensured (zero risk is impossible). But, whenever a breach has taken place, that needs to established immediately!

- There are various risks for individuals (physical, material and non-material)
- A risk can be measured by looking at its factors (type of breach, nature/sensitivity/volume of data, amount of data subjects, type of data subject, type of data controller)
- A lot of security measure can be taken, e.g. pseudonymisation and encryption of data, ability to ensure CIA, ability to restore availability and access, a process for regular testing, assessing and evaluating the effectiveness of measures
- A data breach must be notified unless it is unlikely to result in a risk to the rights and freedoms of natural persons. But, you must always have internal documentation of all breaches
- DPA must be notified with undue delay and where feasible within 72 hours, with a lot of information (nature of the breach, name and contact details of contact point, likely consequences of the breach and the mitigation measures
- If there is a high risk, the data subjects must also be notified (using clear and plain language)

10 Private law liability

- In liability, we have the Victim, Tortfeasor, Tortious Act and Damage
- In general, everyone bears their own damage, the exceptions are covered in liability law
- There are two types, contractual liability and extra-contractual liability

10.1 Contractual liability

- About agreements between parties whereby they create binding effects
- Applied when a contract is breached (non-performance). Three types: Delay in performance, Non-performance and Defective performance
- Three types of damages: Delay damages, Damages in lieu and Collateral damages
- There is always a priority to performance. Whenever a contract is not executed, a **Notice** should be given first, asking them to perform. You don't need to write a notice when performance is not an option or the damage already took place
- Repairing damages must be **compensatory** (only what you lost, no punishment)
- A contract can also be **terminated**. In that case, there are no more obligations and you can claim back what has already been performed. Sometimes, damages can be claimed on top of termination.
- But, termination is a nuclear option. Should be avoided at all costs (balancing exercise). Can only be done if there is serious enough (fundamental) non-performance.

10.1.1 Case Study: Directive for contracts for supply of digital content (DCD)

- About contracts between consumers and traders about digital content
- Content must be supplied without undue delay and accessible for downloading
- Content must be conformed to what was promised and can reasonably be expected (quantity, quality, functionality, compatibility, accessibility, continuity, security, updates)
- There is liability for any failure to supply the content and liability for lack of conformity
- In case of failure of supply, you can send a notice, and after that terminate the contract
- In case of failure of conformity, you can bring into conformity, reduction in price, or also terminate the contract

10.2 Extra-contractual liability (tort law)

- Aristotle's 2 theories of justice and the goal of tort law:
  1. **Corrective justice**: Focus on the fault, person who has caused harm must rectify damages. Goals are to compensate victim, possibly punish tortfeasor
  2. **Distributive justice**: Focus on compensation of damage regardless of fault, e.g. accidents at work or environmental damage
- 3 elements of tort liability include Tort (fault), Damage and Causality link
- There is a fault in case of voluntary action, or unvoluntary action (but only if caused by negligence)
- Hand formula is that you are negligent if the *burder of precautions* is smaller than the *probability of the accident* times the *gravity of injury*
- Creates a balance between costs of precautionary measures and cost of accidents

- Damage is either "Harm", Material or Immaterial
- 3 (4?) types of damages:
  1. Bodily integrity
  2. (Fundamental rights)
  3. Property rights
  4. Pure economic loss
- In **causation**, you have to avoid the **butterfly effect**. Only take **foreseeable damage** into account (so not someone getting a depressure after an injury)
- There is also no-fault liability, two cases:
  1. **Vicarious liability**: it's someone else's fault (employer for employee, parents for child). Uses the "Deep pockets theory" to look at the party who can best repair the damage
  2. **Strict liability**: it's nobody's fault (e.g. defective product, animal, or activity)
- Two measures against no-fault liability: insurance and damage funds
- Example is the E-commerce Directive, where i.e. a website owner is not liable for illegal content if they had no knowledge of it, or removed it as soon as they knew it

11 Intellectual property and freedom of expression

11.1 Intellectual property

- Intellectual property (IP) law gives right-holders an incentive to share their work, and ensures that the work becomes available for all after a certain period
- Copyright is an absolute right, it can be invoked against anyone ('erga omnes'), but a copyright license is a relative right
- Three IP rights: Copyright, Patent and Trademark

11.1.1 Patent

- A patent is an exclusive right granted for an invention
- In exchange for a patent, the patent owner makes technical information about the invention publicly available
- To qualify for a patent, the intellectual good must be An invention, That is novel, and Has an industrial application
- To obtain a patent, you must register the patent

11.1.2 Trademark

- A trademark is a sign capable of distinguishing the goods or services of one enterprise from those of other enterprises
- To obtain a trademark, you must register the trademark

11.1.3 Copyright

- Copyright is a legal term used to describe the rights that authors have over their literary and artistic works
- Two aspects of copyright:
  1. Moral right to be credited with authorship (non-transferable)
  2. Economic rights. (Copyright can be transferred or licensed)
- The author is granted a copyright automatically, by the mere act of creation
- In Europe, the copyright sign is not required! It acts as a reminder
- Copyright is included in many international trade agreements
- 4 goals of copyrights:
  1. Reward the author
  2. Provide the author exclusionary control over the use others can make of their work
  3. Incentivise investment in creative expression and innovation
  4. Ensure the societal benefit of having such expression in the public domain after a certain period

- Scope of copyright control contains Publication, Reproduction, Distribution, Right to prohibition of these three, and Right to license others to exercise rights of these three
- There is no EU-wide private law, so there is also no EU-wide copyright law. But there are directives

11.2   Freedom of expression and privacy

- These freedoms are in the ECHR and EU Charter
- Privacy is the right to respect for private and family life. No interference, except when in accordance with the law and is necessary for the interests of national security or protection of rights and freedoms of others
- So, also the right to freedom of expression of others
- Freedom of expression consists of the right to impart opinions (speaker) and right to receive information (listener). Also applies to the means of transmission
- But, there are exceptions, e.g. when prescribed by law and in the interests of national security or for the protection of the reputation or rights of others
- So, also the right to privacy
- These two rights are often in tension. According to the ECtHR, the rights deserve equal respect. A balance must be found on a case-by-case basis
- There is an enormous body of nuanced case law that deals with this balance
- ECHR used to be applied only in vertical relations, but now also in horizontal relations

12   Right to be forgotten

- In this lecture, a LOT of case law was discussed. The results are in this summary
- CJEU decided that, under certain circumstances, people have the right to have search results for their name de-listed (de-referenced). This also applies to lawfully published information
- This handles with a difficult balance between freedom to impart and receive information, and privacy
- CJEU decided that there is no right to be forgotten in respect of personal data in a company register
- CJEU decided that outside the EU, the 'right to be forgotten' does not apply. Therefore, current law in the EU does **not** require de-listing on all versions of the search engine
- But, there are exceptions (e.g. sex video's without consent)
- Data about criminal convictions can only be processed by public authorities or based on law (with appropriate safeguards)
- CJEU said that search engines did not have to de-list public information about criminals (e.g. news articles)

13   AI and the risk of discrimination

- Computer systems/AI can (accidentally) cause discrimination, where e.g. higher prices are charged based on personal data (address, ethnicity, etc.)
- Can happen especially with machine learning, where discriminatory training data is used (often by accident)
- The two most relevant fields of law are non-discrimination law and data protection law

13.1   Discrimination law

- Two types of discrimination:
  - Direct discrimination: Openly discriminate a group of people (rare in AI)
  - Indirect discrimination:
    * Definition: An apparently neutral practice that harms people with certain ethnicity (is banned). Doesn't matter whether discrimination happens by accident or on purpose.
    * Exception: when practice has legitimate aim and practice is proportionate.
- Weak points of non-discrimination law:
  1. Automated (AI-driven) discrimination may remain hidden
  2. Ban on indirect discrimination is nuanced, but vague (causes problems for companies)

3. Law is silent on 'the poor paying more than the rich', this is not prohibited :(
- Summary of non-discrimination law: necessary but insufficient

13.2   Data protection law

- GDPR says that organisations must offer transparency about their use of personal data
- For risky personal data use the 'Data Protection Impact Assessment (DPIA)' is required
- There are specific rules on automated decision-making (people may not be subjected to certain automated decisions with far-reaching effects)
- So there is a prohibition of certain automated decisions with far-reaching effects
- Organisations must provide meaningful information about the logic involved
- The GDPR is also necessary but insufficient