Legislation

Information Security

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2011 – Week 3

Learning objectives

After this week, the students will have

- an overview of the most relevant legislation for IT and Information Security professionals
- a working understanding of how the judicial system works

The teaching is based primarily on Norwegian law. Exchange students who are not able to read the Norwegian code of law, should study relevant legislation from their own country (or the UK or the US).

Lovdata

- The complete Norwegian Code of Law is available online
  - `http://www.lovdata.no`
- Not necessarily official (worth checking)
  - there could be errors

Outline

Background for the legislation

Why do we have a code of law?

What is the foundation of our law?

Background for the legislation

Why do we have a code of law?

What is the foundation of our law?

Norwegian Constitution

- Principle o separation of powers
  - Stortinget (national assembly or parlament) passes laws and budgets
  - The government (regjeringa) is the executive power
    - Justisdepartementet (Department of Justice)
    - Police
    - Prison service
  - Courts of law pass judgment in accordance with the code of law
- The principle stems from the French revolution
  - Independent courts is quite common in modern states
  - Separation between parlament and government may be fluid

Different laws and regulations

- Constitution (Grunnlov)
- Acts of parlament (lov)
- ‘Regulations’ (forskrift), mandated by acts of parlament but not passed by parlament
- International law and treaties
- Common law (sedvanerett og rettspraksis)
- International precedent

International law

- EU directives
- Human rights
- International treaties
    - FN
    - Interpol
- Foreign law influences our every day life
    - SPAM og cyber crime
    - Which jurisdiction applies?

Outline

Penal code

Straffeloven

Is cyber crime a new sort of crime? Or an old sort of crime on a new arena?

Many crimes are illegal

Many classic crimes see new opportunities with ICT

- Fraud
- Sabotage
- Espionage
- Unauthorised use of equipment
- Embezzlement (underslag)

They are still illegal

Many concepts become ambigious

- What is a *document*?
    - a definition covering electronic documents is emerging
- What is theft?
    - Theft of artefact is clear
    - Theft of information is not theft
- Breaking letters and locks
    - Breaking protective mechanisms is illegal
    - Reading open information is not
    - The penal code explicitely includes electronic information

If you have questions, ... find a lawyer.

Outline

History

- *Personregisterlova* 1978
  - Datatilsynet was established
- Personopplysningsloven 2000
  - principle: all use of personal informationn to be reported
- Personopplysningsforskriften
  - exceptions from the obligation to report use and registers
- EU directives

Scope

- All electronic processing of personal information
- Manual registers of personal information
- Except: an individuals use of personal information for private use
    - i.e. you are allowed to record phone numbers of your friends

Responsibilities

- Management is responsible for the security of personal information
  - clear roles and responsibilities are required
- Risk analysis
- Regular security audit
- Authorisation of personnel
- Documentation

Exception from reporting

- Many types of records are exempt from reporting
  - membership databases, customer records, etc.
- NOT excempt from the security requirements

Rights of the Citizen

- Anyone can demand disclosure of personal information held about them
- Information has to be correct

Privacy abroad

- EU/EEA has been active in data protection legislation
- Limitations on export of personal information
- Destination country must have similar legislation;
- or the receiving organisation must be an approved ‘safe harbour’.

Outline

Public Sector

Public sector is more heavily regulated by codes of law, than anything else. Why?

- Directly under parlament, any regulation becomes law
- Government agencies enjoy particular protection and powers
  - financial
  - through the authority of parlament and government
- These powers must be strictly controlled

The goals of the legislation

- Ensure transparent processes and decisions
  - the public must be able to check that processes are fair
- Protect citizens from abuse
- Protect confidentiality of the massive amounts of data processed
- Prevent curruption

Laws for Public Sector

Arkivlova requiring filing of information in public sector institutions

Forvaltningsloven governing administrative processes in public sector, incl. confidentiality

Offentlighetsloven «Freedom of Information Act» (cf. USA and UK)

Outline

Outline

Sector-specific legislation

- Many sectors are subject to specific legislation
- If you ever do work for the sector
  - you need to look into it

Sikkerhetsloven

National Security

- Concernt *National Security*
- Relevant for Civil Service
  - and those who supply public sector, when the procurement is classified
- Establishes levels of classification
  - requirements from those who obtains classified information
- Establishes *Nasjonal Sikkerhetsmyndighet*
  - approves cryptographic technology
  - accredits information systems

Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)

National Security

- Concerns the use of ICT in banks and financial institutions
- Passed by *Kredittilsynet* (financial services authority) 2003
- Requires planning, documentation, and routines to ensure
  - confidentiality, integrity and availability
  - good risk management
- No answers to how security is achieved
- No hard targets in terms uptime or frequency of incidents
- Just a demand for documents ...

Outline

Authors' rights

Opphavsrett

- Åndsverkslova 1961
  - amended many times, incl. 2006
- Åndsverk – intellectual creation?
  - software, databases, photo, video, music, text
- The law restricts *publication* of such creations
- Some (recent) prohibitions
  - download of illegally published material
  - circumvention of technical preventive measures

Copying and publication

- Copying for personal use is normally allowed
  - it is the distribution which is restricted
  - Beware: there are some tricky exceptions
- What is ‘personal use’?
  - Which challenges have emerged over the last 10-15 years?
- Hordes of ‘friends’ on social media becomes a gray area

Non-transferable rights

- The creator can reassign his rights
- In some cases, rights belong to the employer
  - incl. software
  - not for text
- The creator has a right to be named as author
  - this right is non-transferable
- Note that this automatic right does not exist in all countries

Outline

Digital Signatures

When we accept electronic documents, we need electronic signatures.

1. What are the key traits of handwritten signatures?
2. What is an electronic signatures?
3. Which traits of the handwritten signatures do we lose?

Legal principle

- Agreements are legally binding whatever the format
    - no signature is required in principle
- Written contracts and signatures serve as evidence
    - resolving disputes over what was actually agreed
- E-mail exchange and any other electronic documents may be put forward as evidence
- The main question is not valid versus invalid
    - but the quality of the evidence

Lov om elektronisk signatur

- Clarifies digital signatures to be legally equivalent to handwritten signatures
- Requirements for certificate issuers
- Post- og teletilsynet as watchdog
- BankID has been approved as qualified signatures

What risks for the consumer does BankID cause?

Some issues concerning risk of Digital Signatures

- BBS has blanket signature right on behalf of client
    - the signature is out of the client's control
- Threats include system faults and deliberate attacks
    - Probability is very low
    - Impact could be unlimited
- An unauthorised signature will be perfect
    - very hard to prove abuse and errors
- The signature scheme is technically very complex
    - Is the court qualified to assess the likelihood of failure?

Outline

Aksjeloven og Allmennaksjeloven

- Two different types of limited companies
- Separate laws — many identical paragraphs
- Defines the responsibilities of the Board and the Managing Director(s)

> *Styret (...) plikter å påse at dets [selskapets] virksomhet (...) er gjenstand for betryggende kontroll*

- Worth remembering for a chief security officer
- The board has a responsibility for *compliance*
  - and to avoid *excessive risk*
- Reliable management information

Security view at Board level

What should be your focus when you bring security issues in front of the board?

- You need to put it in a high-level business perspective
  - accounting, business operations, estate management
- They understand
  - Compliance
  - Cost and Revenue
  - Excessive risk — try to quantify it
- Don't get bogged down by technical detail

Security view at Board level

What should be your focus when you bring security issues in front of the board?

- You need to put it in a high-level business perspective
  - accounting, business operations, estate management
- They understand
  - Compliance
  - Cost and Revenue
  - Excessive risk — try to quantify it
- Don’t get bogged down by technical detail

Security view at Board level

What should be your focus when you bring security issues in front of the board?

- You need to put it in a high-level business perspective
  - accounting, business operations, estate management
- They understand
  - Compliance
  - Cost and Revenue
  - Excessive risk — try to quantify it
- Don't get bogged down by technical detail

Security view at Board level

What should be your focus when you bring security issues in front of the board?

- You need to put it in a high-level business perspective
    - accounting, business operations, estate management
- They understand
    - Compliance
    - Cost and Revenue
    - Excessive risk — try to quantify it
- Don't get bogged down by technical detail

Sarbanes-Oxley Act (SOX)

USA

- Similar objectives to *Aksjelova*
- Very strict audit requirements
- Protection of whistleblowers
- Independent auditors
- Audit procedures must follow established standards
  - CObIT, COSO, et c.

Outline

What to do when you are responsible?

- We have discussed some of the most relevant laws and regulations
- We have not covered them
  - law is inherently complex
  - if you have questions, ask a lawyer
- As a professional, you should be aware of, at least
  - copyright legislation
  - data protection
- In some industries, you may need to consult others