Enforcement and Dispute Resolution in a Digital Context: Criminal Law

JUS5650 Spring 2012

Inger Marie Sunde
Førsteamanuensis, EVU
Content: 4 hours 4 topics

- **Content**: ‘Computer crime and the possibilities and limits of technological “fixes”’
  - Ref: JUS5650 infosite

- **Topics**:
  - Jurisdiction and international cooperation
  - Computer data as evidence and object of coercive measures
  - Infringement of personal integrity in social media
  - Automatic law enforcement on the internet
Legal sources

- Council of Europe:
  - Convention on Cybercrime Nov. 23, 2001 (ETS 185) (“CC”)
  - European Human Rights Convention art. 6 “fair trial”; art. 7 “principle of legality”; art. 8 right to private life. (“EHRC”)

- EU:
  - Council Framework Decision on Attacks against Information Systems

- Norwegian Criminal and Criminal Procedural Law
  - The Norwegian Criminal Code of 1902 (“NCC”)
  - The Norwegian Criminal Procedural Code of 1981 (“NCPC”)

- Case law for illustration
  - EHRC, EU and Norwegian case law
JURISDICTION AND INTERNATIONAL COOPERATION

THE INTERNET CLOUD
1. Jurisdiction

Within the territory:

A state has **full jurisdiction**, i.e., the right to:

1) Prescribe law;

2) Adjudicate;

3) Enforce the rules / judgements.
   - E.g. serve a production order (subpoena) on an ISP.
   - Carry out a computer search.
   - Detain and imprison offenders.
Outside the territory

As regards actions/events taking place abroad, a state may

1) Prescribe law; 2) Adjudicate

3) But **may not enforce** rules / judgements abroad. Principle of sovereignty (connected to territory) i.e., a principle of international law relevant **between** states.

Therefore:
- International cooperation is needed in order to obtain digital evidence. Letter Rogatory / Mutual Legal Assistance Treaty (MLAT). CC chapt. III.
- LE Guidelines: E.g.:
  

---

27.02.2012 • Side 6
The CC structure:

• Section 1: Substantive criminal law:
  • Criminal provisions (art. 2-11) MS obligation to criminalize.

• Section 2: Procedural law
  • Art. 14: The CC procedural provisions must be implemented by the MS, to cover the CC-crimes (above) and in order to investigate and prosecute other types of crime.
  • Art. 15 Conditions and safeguards (HR and RoL-principles)
  • Art. 16-21: Coercive methods to be implemented in national legislation

• Chapter 3: International cooperation
  • Specifying alternative procedures depending on the existence of MLATs or not. The CC does not supersede existing bi-/multilateral conventions, is merely a supplement.
  • Mutual assistance with regard to the procedural measures specified above: Art. 29-34. Must be implemented.
  • Art. 35: 24/7 national contact point. Norway: NCIS (Kripos – Kriminalpolitisentralen).
The reach of national criminal law (space)

• Principle of legality:
  • Norwegian Constitution art. 96 and EHRC art 7: No one may be convicted for a crime unless it has been prescribed by law.

• The law must extend to the place where the crime was committed.
  • Outside the territory: Whether national criminal law is applicable or not depends on the legal connectors between the act of crime, the individual and the State.
Reach: Some legal connectors

• State has competence to criminalize acts committed:
  • On its territory
    – principle of territoriality (+ flag principle (crimes committed on ship, aircraft))
  • Outside its territory, if committed by an individual who is a citizen or a resident of that state
    – principle of nationality / domicile
  • Outside its territory and committed by a foreigner, if (i) the crime is very serious, and (ii) it is a crime in the state where it was committed
    – principle of universality + dual criminality.
  • Outside its territory and the act has an effect within its territory – effect principle.
Legal connectors of the NCC and the CC

- NCC art. 12:
  - **First paragraph:**
    - Item 1-2: Territoriality + flag principle
    - Item 3: Nationality and domicile
    - Item 4: Universality + dual criminality
  - **Second paragraph:** The effect principle

- Cybercrime convention art. 22: Jurisdiction
  - Each MS has a duty to ensure that it has jurisdiction over the offences mentioned in art. 2-11 according to the following principles:
    - Territoriality + flag principle
    - Nationality + dual criminality
    - Not universality, except in non-extradition cases. (an alleged offender from a third state is present in its territory). In order to avoid negative jurisdiction conflict.
Crimes mentioned in art. 2-11 of the CC

- The “CIA-offences” art 2-6: Confidentiality, Integrity, Availability
  - Art. 2 Illegal Access (computer system (stored data))
  - Art. 3 Illegal Interception (non-public transmissions of computer data)
  - Art. 4 Data Interference
  - Art. 5 System Interference
  - Art. 6 Misuse of devices (passwords / malware)

- Computer related offences: Forgery and Fraud (art. 7 and 8).

- Content related offences: Child pornography art. 9
  - Bad expression. Better: Child abuse material. (Overgrepsbilder)

- Infringements on copyright and related rights: Art. 11
The "back door case" (Rt. 2004 s. 1619)

• Facts:
  • 2 Norwegians gained access to approx. 450 computers worldwide, many located in the USA, and installed "back doors". They used computers in Stavanger, Norway, to carry out the attacks. They were charged i.a. for illegal access pursuant to the NCC art. 145 second para.

  • Defense attorney claimed that the criminal provision was not applicable because the illegal access took place abroad.

• Q1: What did the Supreme Court say?

• Q2: Would the NCC art. 145 be applicable if the facts were the opposite? (US citizens attacking Norwegian computers?)
Executive jurisdiction (competence)

• Competence to investigate, to enforce the law, to use coercive measures...

• General principle: The competence of the police (state power monopoly) is limited to the territory.
  • Exception: “hot pursuit”

• Crossborder investigation w/o permission from third state => infringement on the principle of sovereignty
  • i.e. a matter between states, a matter of international law.
  • In case of contravention, does is amount to a procedural error?
  • What would the consequences be?
• The trial is a matter between the state and the defendant.
  • Not between states.
  • What are the procedural consequences of a breach of sovereignty?

• The procedural issue is whether the evidence must be regarded as having been unlawfully obtained, and if so, whether it can be presented as evidence or must be be barred (“fruit of the poisonous tree”).

• A matter of “fair trial” according to EHRC art. 6.

• Indirectly referred to in CC art. 15 (conditions and safeguards). The CC does not address the issue explicitly.
Norwegian procedural law:

• NCPC main rule: Free admissibility of evidence.
  • (Few formal cut off rules.)

• Cut off requires balancing of the different interests involved.

• A balancing test:
  • If the evidence has been unlawfully obtained, what kind of wrong is it?
  • Does the wrong infringe on fundamental HR, e.g. prohibition against torture.
  • Would the use of the evidence constitute a continued infringement on HR?
  • Does the wrong impair the quality of the evidence? What about chain of custody?
  • Is the evidence important to the case?
Case example:

- **Facts:**
  - A Norwegian investigator gains access to the suspect’s gmail a/c by use of the suspect’s username and password found on a piece of paper under the computer keyboard in a lawful house search.

- **Alt. 1:**
  - The investigator copy data from the gmail a/c. The prosecutor wants to present the data as evidence at the criminal proceedings.

- **Alt. 2:**
  - The investigator does not copy data because of risk of disturbance, but reads the mail. The Prosecutor wants to examine the investigator as witness in order to produce information about the crime contained in the mail.

- The defense attorney demands the evidence to be barred as illegally obtained.
a) Has the evidence been unlawfully obtained or not?

• **Problem in the “cloud”: Loss of location**
  - One cannot know the exact location of the data at a certain point in time. The service provider owns “server parks” scattered all over the world
    - (Spoenle p. 4).

• **CC art. 19.2**: One may extend a computer search from one system to another, if the system or part of it is located in its territory, in order to gain access to data “stored in ... its territory”
  - Not possible to determine.

• **CC art. 32**: Trans-border access to stored computer data:
  - One may freely access open source data irrespective of location. (N/A).
  - One may access data located in another state according to a lawful and voluntary consent...
    - Again: Location is not possible to determine.
Power of disposal:

One may reason as follows:

- No provision of CC is directly applicable, because the location of the data may not be determined (and all provisions make the location relevant).

On the other hand: The power of disposal may be determined and is internationally applied today:

- The power of disposal is held by the one holding the authentication credentials (username/password), and is in position to use and to exclude others from using, the account.
- Also held by the service provider.

Is in defacto use today, e.g., preservation and production orders, CC art. 16-18. (refer to data that are “stored”, yet they are applied as basis for serving orders on the ISPs).
If using the suspect’s authentication credentials were to be regarded as a contravention of territorial sovereignty, how could ISPs offer their services to citizens world wide? There is no border control in relation to the users.

To think of borders in relation to user accounts in the “cloud” may be a misconception.

Conclusion: Investigators may logon to suspect’s user account in the cloud.

If negative conclusion: Is the gaining of access an infringement of fundamental HR? EHRC Art. 8?

• Depends whether safeguards and conditions of national procedural law has been complied with. Special safeguards may apply to email correspondence.
• If user authentication credentials have been obtained in a lawful house search, or by lawful consent, no violation of HR.
Letters rogatory /MLATs:
Prosecutor => local district Court => MoJ (Norway) => MoJ (USA) => federal prosecutor => submission to local District Court => obtains the evidence. Submitted by mail to Norway through formal channels.

Eurojustice.

(Expedited) preservation order: CC art. 16 and 17 (traffic data etc.). International coop.: Art. 29-30. Preservation for 90 days. NCPC art. 215a. Order issued by the prosecutor.

Purpose:
- To prevent deletion of the data prior to a formal production order
- Help trace the origin of a data transmission (source).
- Ref. also the Data Retention Directive (EU). Directive 2006/24/EF.
COMPUTER DATA AS EVIDENCE
AND AS OBJECT OF COERCIVE MEASURES
• Search
• Seizure
• Computer surveillance
• Interception
• Real time communication control
• Production order

Methods that police can carry out w/o assistance
Computer data as evidence

• Evidence law distinguishes between evidence in the form of
  • Statements: Examination of witness, defendant, victim, expert
  • Objects: Must be presented or somehow displayed to the court.

• Computer data is evidence in the form of an object.

  "Digital evidence is a digital object that contains reliable information that supports or refutes a hypothesis"
  » B. Carrier, File System Forensic Analysis (2010 p. 4.)

• Computer data is
  • a source of information
  • The object of the part of the investigation which is called "computer forensics"
Legal definition of computer data

“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”

CC art. 1.b

• Think of computer data as a computer file, or fragments of a file
  • Like fragments of a broken bottle or pieces in a puzzle
  • Forget about computer data as a “a string of ones and zeroes” (which is legally not more relevant than to describe the murder weapon as a heap of atoms)
DATA:

Lydfil: 04 Obé ! [Soup]

Bildefil: Fela / Fela Kuti / Phela Qt / Fela Anikulapo
Methods that interfere with the right to private life

- Search
- Seizure
- Computer surveillance
- Interception
- Real time communication control
- Production order

Methods that police can carry out w/o assistance
EHRC art. 8
Right to respect for private and family life

• 8.1: Everyone has the right to respect for his private and family life, his home and his correspondence.

• 8.2: There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others.

• Ref. CC art. 15: Conditions and safeguards. Item 1: EHRC and UNCHR.
• Ref. EU Charter art. 7, 8 and 53 + TEU art. 6.1 and 6.2.
EHRC art. 8 and Internet cases

- **Copland v. UK (2007)**: Surveillance at the work place: Internet activity logs, traffic data and email are protected within the meaning of art. 8.1. “private life and correspondence”. Ref. Halford v. UK (1997).

- **K.U. v. Finland (2008)**: Production order: Due to strict telecomsecrecy regulation ISP could not give police information about the identity of an end user, based on IP-adress used to post a message with illegal content on the Internet. Dead end to investigation and prosecution, to the detriment of 12 year old victim who in the email had been falsely presented as interested in pedofile sex. The Court: The State has not only a negative obligation to abstain from interference, but a **positive obligation to secure** that the right to private life may be effectively enjoyed by its citizens. The telecom secrecy regulation was too strict, because it made criminal prosecution impossible. Economic compensation to the victim not sufficient to fulfil the obligation.
Search and seizure

• Computer search vs. search in computer data
• Seizure of computer equipment vs. seizure of computer data

• CC. Art. 19 “Search and seizure of stored computer data”
  • 19.1: Access
  • A) access a computer system or part of it and computer data stored therein
  • B) access a computer-data storage medium in which computer data may be stored in its territory.
  • 19.2: Extended search
  • Extend the search when it has grounds to believe that the data sought is stored in another computer system or part of it in its territory.
  • 19.3: Seize /secure data accessed
  • Secure the computer system or storage media
  • Make and retain a copy of those computer data
  • Maintain the integrity of the stored computer data
  • Render inaccessible or remove those computer data in the accessed computer system
One may reason like this:

- The physical computer equipment /media are objects.
- The computer data is an object. The computer data is stored on physical media.
  - The analogy is not to a book, but to a box containing objects

- Situations vary:
  - Small media are seized and brought to the police station.
  - Large servers are searched and the data is copied (mirror/file copying)

- Evidence: Computer data (object).

- Confiscation: (i) Physical equipment and (ii) computer files.
Examples from Norwegian law

• **Rt. 2011 s. 296**: Search of a lawyer’s office. Lawyer charged as accomplice of criminal client: Police made a mirror copy of the server which contained privileged information. The copy was sealed and brought to the district court for it to filter out the privileged information (NCPC art. 205)

  • The copy of the data stored on the server did not amount to seizure.
  • The court control formed part of the search. (NCPC art. 205 in conj./w art. 192)
  • The filtered copy was returned to the police, for it to pick out the files relevant to the criminal charge. The examination of the copy was a continued search of the data.
  • Seizure takes place when relevant files eventually are picked out and registered as part of the case. Seizure NCPC art. 203 “object” (ting) . Computer data is an “object” w/in the meaning of the NCPC. See also Rt. 2011 s. 1188. (when files become case documents).
  • Computer data can be confiscated as “objects” related to a crime. NCC art. 35.
Computer surveillance

• To copy ongoing activity on a computer. Keystroke logging
• Not regulated in the CC.
• Permitted in Denmark and several European Countries + USA and Canada. Under discussion in Sweden and Norway. (NOU 2009:15 chapt.23).

• As a method: Differs from
  • Interception of communication (content data) (ref. CC art. 21), which concerns communication between different computers (communication devices). Keystroke logging is interception of electronic signals internal to one computer system (from keyboard to the main box).
  • On-line search: Is an intrusion into a computer over the net, looking around and/or copying of the content. Computer surveillance is of a continuing nature (say 4 weeks), while search is limited, carried out then and there.
Interception and real time collection of traffic data

• CC art. 20 and 21. International cooperation: art. 33 and 34.

• Ref. EHRC art. 8: Conditions
  • According to law (means formal legal provions) NCPC: Ch. 16a (art. 216a and 216b)
  • For a legitimate purpose (prevention of disorder and crime): Investigation of crime
  • Necessary in a democratic society: NCPC art. 170a Principle of proportionality and necessity

• NCPC Safeguards and controls:
  – Court control (ex ante),
  – Publicly financed defense attorney (“shadow”, duty of confidentiality, no contact with client)
  – Limited period of time,
  – Only allowed in cases of serious crime (interception of content: imprisonment min. 10 years; real time collection of traffic data: imprisonment min. 5 years) i.e. organized crime, drugs, terrorism...
  – Permitted may only be granted if it is deemed that the method will be of significant importance to the case, and not using the method will make completion of the investigation difficult (art. 217a)
  – Control system ex post (Kontrollutvalget).
**Principle of legality**

- **NCPC Art. 216b (c)** permits “the use of technical equipment” for the purpose of “identifying a communication device which is in possession of the suspect or the suspect is likely to use”

- **Rt. 2009 s. 394:**
  - Police used an IMSI catcher (tech.equipm) to locate a cell phone the police thought was used by the suspect, but was registered in the name of another individual.
  - Supreme Court: This is beyond the scope of art. 216b (c), because the wording only permits the identification of a “communication device”, not the identification of a person.
    - On this area (interference with private life and communication), the principle of legality as laid down in Norwegian law and in the EHRC art. 8 has strong priority.
    - Consequently, the method did not have foundation in law. Not permitted.

- **Rt. 2010 s. 1232:**
  - Police requested base station data from cell phone provider. Purpose: To identify a communication device as mentioned in art. 216b. Beyond the scope of art. 216b. Even if an IMSI Catcher may be regarded as a ‘false base station’, a provider’s base station cannot be regarded as “tech.equipm.” w/in the meaning of art 216b.
Production order

• CC art. 17, 18. International cooperation art. 30, 31.

• Obligation to submit specified computer data which is in control of the requested person, and stored on a computer system. The requested person must be in the territory.
  • “control”, “stored”, “territory”
  • Is applied to providers of cloud services as well as to other persons/organizations which are in possession of such data (may be witnesses, and no need for a search).
Production order

**NCPC:**

- **Art. 210 flw.:** Production orders regarding “objects” in general. Also computer data.
- Distinction betw: Historical and real time/future objects (data) and with or without notification to the suspect. Must be read in conj./w. art. 216b.

- **Art. 211:** Production order regarding email in the possession of the service provider. (stricter conditons, “correspondence” EHRC art. 8)
  - The legal discussion has been around the issue when the possession of the email is transferred from the service provider to the end user (addressee /suspect): **Options:** Under transmission (not practical), when it arrives at the inbox RG 2008 s. 1477, when the suspect reads the mail. RG 1998 s. 1155.
  - Perhaps one could as well consider the email to be in the possession of both as long as they both may exert control, over it?
INFRINGEMENT OF PERSONAL INTEGRITY IN SOCIAL MEDIA
Sosiale medier
The Ecosystem Effect

- Social media
- User-generated content
- Distribution – integration of services – hyperlinks, RSS-feed, Mashup
- Search engines (Google, Yahoo)
- Filesharing (torrent technology, P2P)
- Repeated distribution – duplicates
- Unmediated
- Unlimited space for publishing and storage
- Digitization digitization digitization ...
The problem is

“The globalized aggregate volume”
David S. Wall, criminologist, UK, 2007

“the seriousness [of cybercrime ] lies in their globalized aggregate volume [..] if cybercrimes are indeed, minor in nature but large in aggregate, this may affect the way we construct victim profiles”
Internet is a gigantic collective external memory

Case: Hemmelig.com (Secret.com)

• 26 000 Norwegian users
• A legal service. Purpose: To seek sexpartners
• Dec. 2011: Hacked, list of users and chatlogs copied
• List of users is published in social media
• List of users is distributed on torrents (P2P)
• Many users are identified
• The news service abcnyheter.no receives the user list
Dagbladet: “The users of secret.com are politicians, high ranking military personell, people in the security branch, aircraft pilots, physicians, lawyers, celebrities and private industry top managers”

Dagbladet, large Norwegian newspaper
Slettmeg.no (delete.me.no)

“it is hard to be deleted from the user database of secret.com which has been distributed on the net. ... The reason is that the document is primarily shared on torrents. It means that the document as such is stored on the computers of private end users, and you cannot delete it from there.”
Duplicates – P2P og “dog poop turns crime”

• “User generated content”:

• Does not mean that the user has created the content. It only means that social media are unmediated publishing space for content.

• There is no “bottle neck” as regards publishing or storage space. Space is unlimited.
Everlasting / perpetual infringement of integrity
Økosystemeffekten

Sosiale medier

+ Repeated copying, duplicates

+ Digitization, digitization and digitization

+ Storage services Dropbox, Google
The virtual and the physical dimensions are parts of reality

- Hemmelig.com (Secret.com)

- Hamarungdom.no (TeenslivinginHamar.no): Social site for teenagers from Hamar.

- Blogg used for bullying a 16 year old girl, named. Prosecution. Misdemeanor. Considered callous behaviour which infringed on the private sphere of another person, NCC art. 390 a.

- Court: The girl had “to a larger extent than usual, been bullied by pupils at school ... and has always been tormented”
The net cannot be "shut out"

Hemmelig.com

Hamarungdom.no

Speech has an influence on other people who reads it, thereby producing an effect on the victim’s integrity.
Protection of personal integrity in social media – protection agains whom and against what?

• Between private individuals.

• Between commercial corporations and the individual: Data protection regulation. Norway: Personopplysningslovgivningen.

• The State vs. the individual : EHRC art. 8.2
  • Automated intelligence, policing the net.
  • Computer surveillance.
  • Infiltration and UCOs.
Between the individuals

1. Physical infringements, actions.

2. Illegal speech.

3. Speech which is legal but becomes a problem over time.
European Court of Human Rights

• There is a need for increased vigilance of the right to privacy in light of the digital communications technology’s ability to store and reproduce private information.
  • Von Hannover v. Tyskland (2004) avsnitt 70
  • A dispute between private individuals (Caroline of Monaco and German media corporations)

• This statement by the Court is commonly used in cases about state surveillance of its population. This time it was used to highlight a point in an assessment which gave priority to privacy, making a caveat in the right to free speech. Indicates increasing weight of digital communications technology in legal balancing of privacy vs. freedom of speech.
1. Physical abuse, physical action

- The use of social media to commit rape over the net.
  - Rape or "sexting"?

- Hacking and data interference of the user profile.
  - CC art. 2 og 4.

- "Facerape"
2. Illegal speech

- Sexual abuse material of children
- Intimate photographs published w/o consent.
- The question is: Does there exist a right to have the perpetual infringement brought to an end?
- If such a right exist, can it be enforced?
- One possible approach: The positive obligation of the State to secure the right to private life for its citizens, EHRC art. 8.1. in conj. w/ art. 1.
Sexual abuse material of children

• The duplicates represent a perpetual infringement of the child on the photograph.

  » Norwegian Supreme Court, Rt. 2002 s. 1187, s. 1192.

  “In addition to the enormous distribution of the images which is achieved by publishing on the net, it is not practically possible to delete them. Children who have suffered abuse for years in the production of pornography may experience to be recognized for years. It is in these cases appropriate to talk about a perpetual infringement of the child. One should also to take into account that the risk of recognition represents a considerable additional burden to be carried by the victim later in life.”

• This is equally valid for adults who suffer comparable infringements of privacy.
Perpetual infringement of privacy
AUTOMATIC LAW ENFORCEMENT ON THE NET
Filtering of duplicates

• Legitimate filtering is open, transparent, narrowly focused, and accountable to citizens and users.
  • Bambauer, see L Edwards p. 654-655.

• De lege lata: Confiscation of objects.

• Confiscation of computer files (a file is an object). Confiscation can be enforced in the net by filtering of the duplicates.

• The technology is well known.
• The problem is well known.
• The problem is serious, but foreseeable (standardized, duplicates)
• Hence, the State cannot be excused for not taking action to protect the victim’s right to respect for private life.
EU Court judgement of Nov. 24 2011

• Case number C-70/10. SABAM (composers) v Scarlet (ISP)

• About the interpretation of art. 15 of the e-commerce directive, prohibition to impose a general monitoring obligation on the ISPs (ecommerce directive art. 15).

• Legal issue boils down to the design of the technical scheme, and a legal balancing test of the different interests involved.

Enforcement of confiscation in the net: “Automatized confiscation”

The point is that automatized confiscation can and should be done according current legal rules. Any insecurity is not caused by the principle of legality and its requirement of adequate legal provisions, but is caused by a lack of insight as to how law (de lege lata) may be operationalized in the technical environment.

• Automatisert inndragning.

3. Speech which is legal, but becomes a problem over time

• 25 yeas old student had problems to get a job because of privat photos on Myspace (role model).
  • Partyhat and a colorful drink in the hand.
  • Decontextualization

• Norwegian politician – forever stigmatized because of spontaneus utterances on Facebook about Norwegian MGP winner
  • “Gimme meg laps (sami), ice bears and moscus. I think, that is what we should sell, not that our immigration asylums are wide open” (said about Stella Mwangi, background from Kenya, winner of Norwegian MGP contest)
A right to be forgotten?

• A biologically grounded aspect of the right to private life?
  • Rt. 1952 s. 1217 (To suspicious persons) “a veil of forgetfulness / oblivion”
  • Default has shifted from delete to save and forever store data. Viktor Mayer-Schonberger. Delete: The Virtue of Forgetting in the Digital Age. 2011.

• Rules of preclusion (punishment, debt...)

• Fundamental principles of data protection:
  • Purpose and deletion when purpose has been achieved.

• Proposal for a revised general personal data regulation 25. januar 2012.
  • Com (2012) 11 Final
  • Article 17: Right to be forgotten. Right to erasure.
Would it be possible to enforce a right to be forgotten?

- Impose an obligation on the ISP to delete data upon request?
  - Would not solve the torrent problem

- Search engines
  - Introduce a prohibition to make names of private individuals searchable?

- "Expiry date" on data
  - It could solve the torrent problem, but has unexpected and indefinite side effects?