



POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

Experience of Norway on data protection and rule of law safeguards when investigating cybercrime

Eirik Trønnes Hansen
prosecutor, NCIS Norway

CyberSouth Launching Conference
Tunis, March 21-23, 2018



Agenda – themes in the presentation

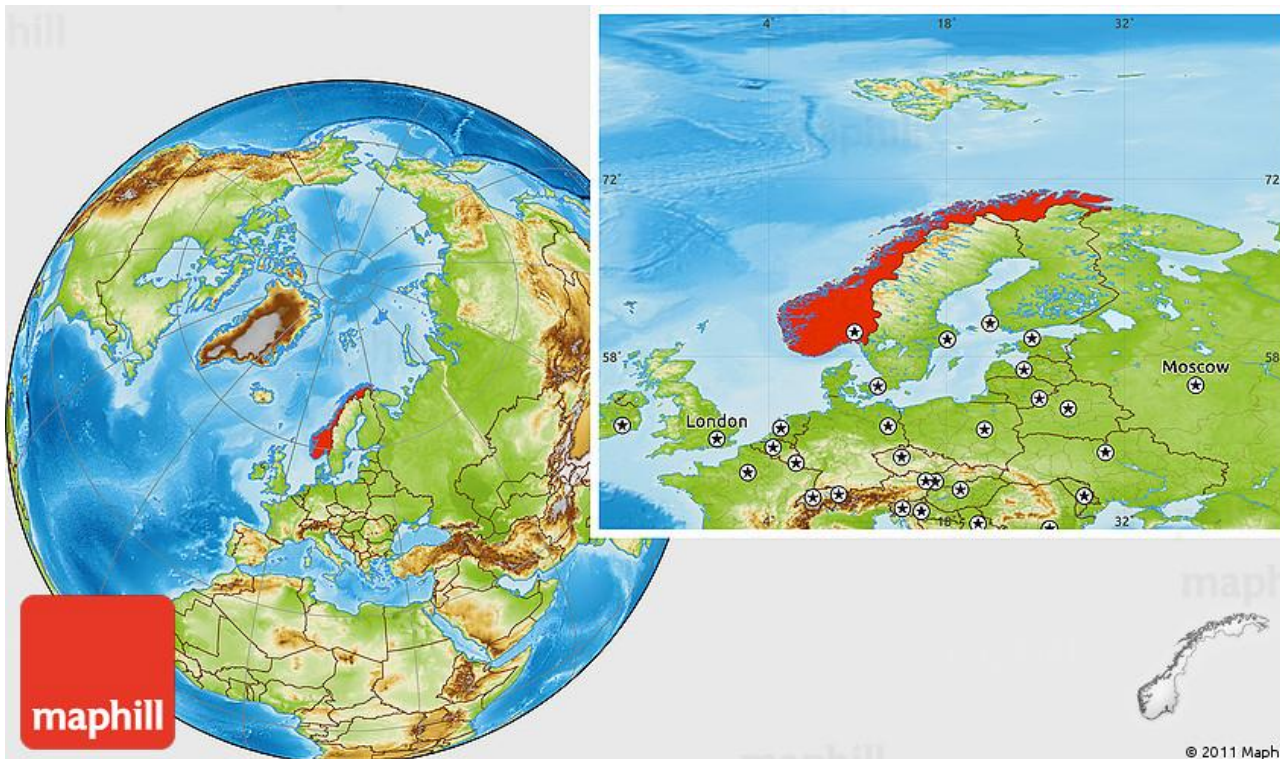
- Introduction
- Overview over current cyber-relevant criminal laws in Norway
- Overview over current data protection legislation in Norway
- Limitations and possibilities
- Conclusion



Norway:

Population: 5,3 million

Not member of EU, but due to the European Economic Area-agreement with EU, various EU regulation applies





POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

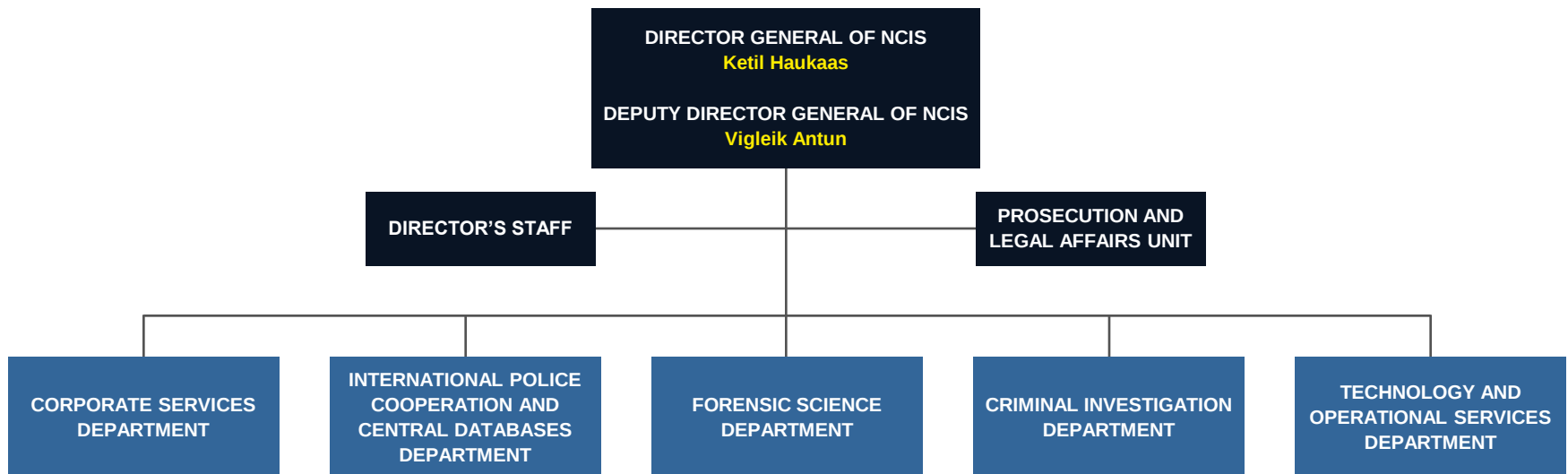
NCIS Norway (Kripas)

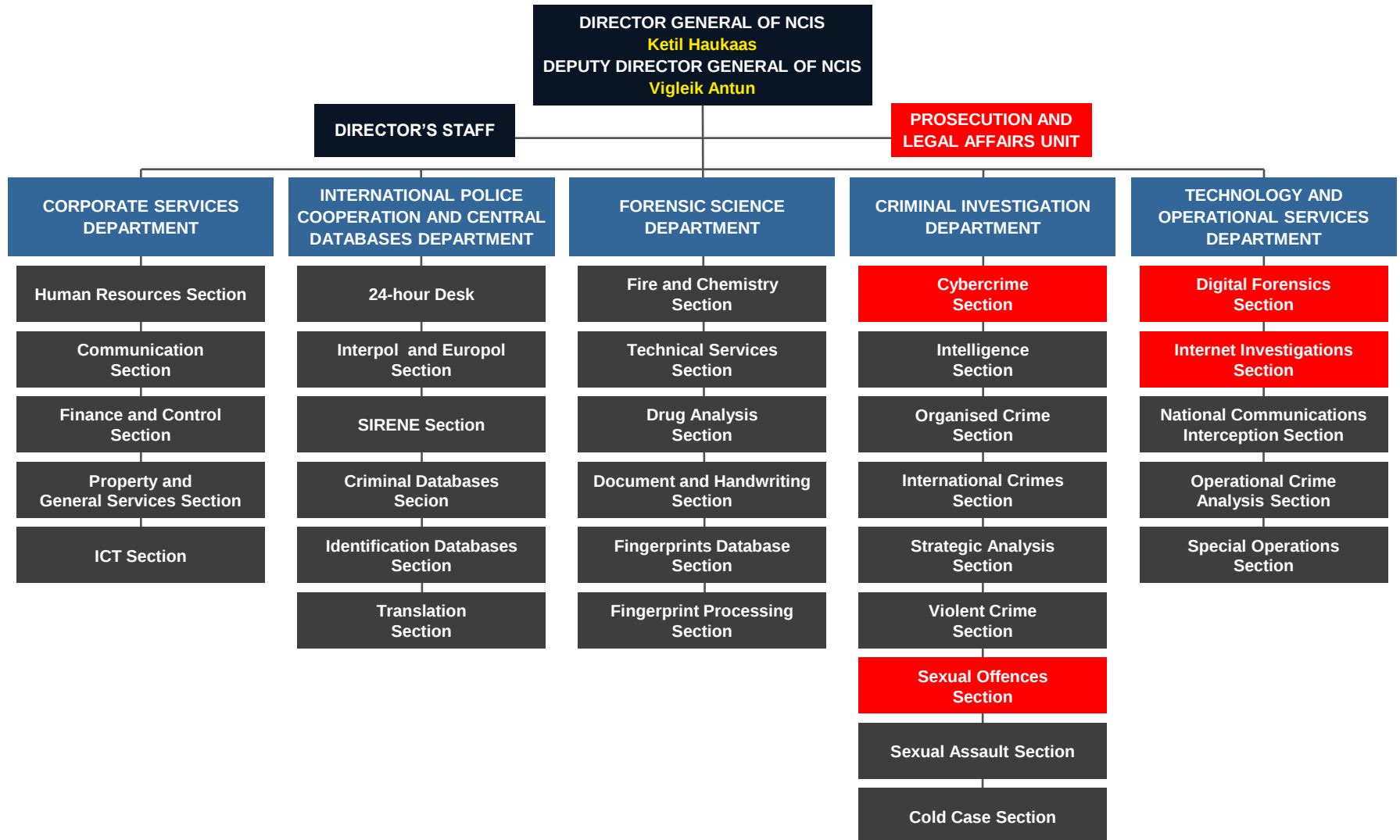




POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service







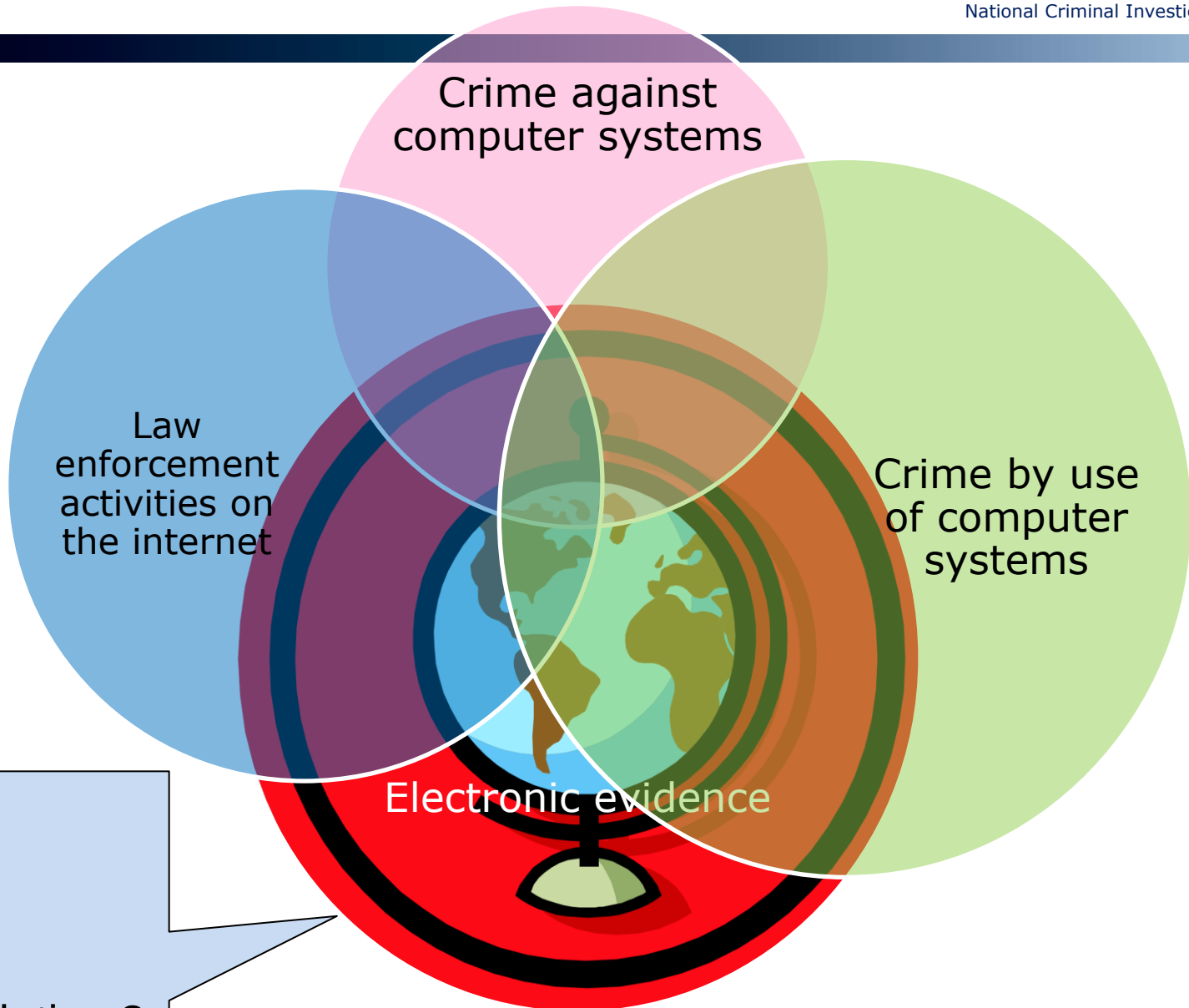
Core functions for NCIS Norway

- The Norwegian contact point for Interpol, Europol, SIRENE (Schengen information system) and the 24/7 network (The Budapest Convention art. 35)
- Forensic services, including digital forensics and analysis
- Develop and maintain several central police databases
- Investigating and prosecuting
 - organised and other serious crimes
 - crimes against humanity and war crimes
 - cases regarding child abuse images, online child abuse, grooming etc
 - computer crime: computer intrusion, data interference and system interference (DDoS etc), internet banking fraud



POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service



What?
Who?
Where?
How?
How much time?



Current cyber challenges

- Increasing use of cloud services
- More use of encryption and encrypted services
- More non-retention of data
- New jurisdictions for data/electronic evidence, ex: U.S. Companies with European data controller offices in Ireland
- Compliance with new EU data protection regulation (GDPR)
- "Big Data"
- Resources...



Access to electronic evidence?

- What kind of electronic evidence?
- Who has it – company/unit of company?
- Where – correct jurisdiction?
- How?
- How much time?
- Securing evidence while waiting for access?
- Documentation: to use electronic evidence in court, the evidence and the chain of custody must be documented and presented in a transparent and reliable way.



Norwegian general practices

- Many providers have "law enforcement guidelines", and in individual cases, it's usually quickest to follow this route
- If possible: expedited preservation (The Budapest Convention art. 29). Some providers accept "freeze request" directly from police in other jurisdictions
- If possible: the CoE 1959 Convention art. 15 nr. 2: sending request from prosecutor to prosecutor.
Standard forms etc for MLA requests
- If possible: consider direct contact with the authority in question in the other jurisdiction (The Budapest Conv. Art. 35)
- Criminal investigations are separated from intelligence services; evidence used and obtained in a criminal investigation will be presented to the defense counsel and in open court. This includes evidence obtained in other countries and evidence obtained by private parties.



Direct requests to service providers

- Many different types of internet-related providers:
 - Telecoms
 - Social media and e-mail companies (Facebook, Microsoft, Google etc)
 - Website hosting companies
 - Internet registrars
 - Proxy, VPN and other anonymity service providers
 - Internet financial service providers (PayPal, Western Union, TransferWise..)
 - Etc
- Different companies, different jurisdictions, different rules... and different responses to direct requests.



Experiences and challenges

- Uncooperative companies?
- Deleted data, encrypted data?
- Practical difficulties in accessing the data in question, example: co-hosting solutions
- Securing data vs accessing data
- Data protection regulations?

For cross-border investigations, also:

- Jurisdiction?
- Legal challenges based on local legislation
- The mutual legal assistance process takes time



Cloud services: jurisdiction?

- Location of the HQ for the person/company that runs the service where the data is stored/processed?
- Location of the subsidiary company where the data is stored/processed?
- Location of data controller?
- Location of the server?
- Power of disposal: the location of the customer/victim/suspect?
- Multi-jurisdiction solutions? Multi-tiered solutions?
- Different jurisdiction solutions regarding criminal cases, civil cases and/or public regulators (Data protection agencies etc)?



Jurisdiction principles?

- Company HQ?
- Where the company (and their "law enforcement guidelines") states as jurisdiction?
- Where the data is stored (physical location of server)?
- Office for Data Controller?
- "Business presence", f.ex. an office for advertising sales?
- "Online presence"?
- "Power of disposal": nationality/location of customer?
- Physical access to unit logged on to cloud services? (Ex: e-mail on iPhone)
- Nationality/location of the victim?
- Multiple jurisdictions?
- Different solutions for different sets of data? (one for subscriber information, another for content data?)
- Different solutions for different types of providers?
- Compare with principles and solutions from other legal areas for guidance, eks. jurisdiction for data protection, consumer protection copyright protection, international contract law, tax legislation...



POLITIET
KRIPOS

"Visit Luleå!"



The Telegraph

Home Video News World Sport Finance Comment Culture Travel Life Women Fas

Apple iPhone Technology News Technology Companies Technology Reviews Video Games Tec

HOME » TECHNOLOGY » **FACEBOOK**

Facebook to build server farm on edge of Arctic Circle

Facebook is to build a multi-million 'mini town' on the edge of the Arctic circle to house all its computer servers, which would use as much electricity as a town of 50,000 people.

2K 629 0 0 3K Email



Luleå is situated at the northern tip of the Baltic Sea, just over 62 miles South of the Arctic Circle Photo: Alamy



By Richard Orange, Malmö
2:47PM BST 26 Oct 2011

30 Comments

The enormous server farm facility in Luleå, northern **Sweden**, to be announced officially on Thursday morning, is the first time that the social networking giant has chosen to locate a server farm outside the US.

Print this article

Facebook

News » World News »
Europe » Sweden »
Technology »



The best tablets

In Facebook



Mark Zuckerberg's
Year of Books: the full
list





HQ in California, but the data in Luleå, Sweden...

<https://www.facebook.com/careers/life/facebook-lulea-sweden>

Facebook Lulea Sweden | Facebook-jobber - Internet Explorer

https://www.facebook.com/careers/life/facebook-lulea-sweden

Facebook Lulea Sweden

Work at Facebook | Teams | Locations | University Students | Benefits | Facebook Life



Located in the beautiful town of Luleå, Sweden our world class data center is where Facebook's mission to make the world more open and connected comes to life. Everyone is encouraged to collaborate and share ideas openly and we empower the people who work at Facebook to make an impact and when you're in charge of making a difference, there's no limit to what you can do.

Growing in Facility Operations, IT Operations and Networking

Facebook Luleå is growing and we are looking for the best talent to come join us in our mission to make the world more open and connected. We currently have several exciting opportunities across the core areas of Facility Operations, IT Operations and Networking. To learn more about these open positions and to apply visit our [Careers page](#).

Or learn more by [taking a tour of our data center](#).

Luleå

Luleå is an exciting city with plenty of culture, great shopping, beautiful scenery and lots of outdoor pursuits, to find out more [click here](#).

Relocating to Luleå

Positions in Luleå, Sweden

- Chief Building Engineer (Luleå)
- Data Center Technician (Luleå)
- Electrical Specialist, Subject Matter Expert (Luleå)
- Network Engineer Deployment and Support (Luleå)
- Security Operations Center Manager - Luleå (Luleå)

Related Posts



Solutions Engineering at Facebook





POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

... and the data controller in Dublin, Ireland

Facebook-jobber - Internet Explorer
https://www.facebook.com/careers/locations/dublin/

facebook Registrer deg

E-post eller mobil _____ Passord _____ Logg inn
☐ Forbli innlogget Glemt passordet?

Work at Facebook Teams **Locations** University Students Benefits Facebook Life

Dublin, Ireland 88 open positions

Find your job Dublin

- ✓ Dublin
- Forest City
- Fort Worth
- Geneva
- Gurgaon
- Hamburg
- Hong Kong
- Hyderabad
- Jakarta

Stéphan G. PRODUCTION EN OFFICE: DUBLIN SINCE: JULY 2

"We're on the edge of technology. We face things that we're the first to tackle."

Opened in 2009 as Facebook's international headquarters, Dublin has transformed from a small landing team of 30, growing to almost 1,000. Located in the heart of the Irish tech scene, our team serves developers, advertisers, employees and our communities throughout the entire EMEA region.

facebook

100%



Significant differences – for good reasons?

Type	Legal regulation	Direct requests from own jurisdiction?	Direct requests from other jurisdictions?
Telecom providers	Specific, national telecom provisions, duty of confidentiality.	Some requests, based on national law, ex. subscriber information.	Usually not, this may be specifically against national law.
Social media and e-mail companies (Google, MS, Facebook...)	Data protection laws, user agreements, other provisions	Some requests, based on national law, ex. subscriber information. Production order?	Some requests, based on national law, ex. subscriber information. Different practices in the U.S., vs. EU vs. others. MLA?
Website hosting companies	Data protection laws, user agreements, other provisions	Some requests, based on national law, ex. subscriber information. Production order?	Some requests, based on national law, ex. subscriber information. Different practices in the U.S., vs. EU. MLA?
Internet registrars	Data protection laws, user agreements, other provisions	Some requests, based on national law, ex. subscriber information. Production order?	To some extent. Some data is in searchable public registers. MLA?



Same laws, different practices

CoE, T-CY report, "Criminal justice access to data in the cloud" (2016) page 7:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>

"The six providers cooperate in a very inconsistent manner with different Parties.

In terms of disclosure rates, for example:

- Google cooperates above average with Finland (83%), Netherlands (81%) and Japan (79%) but below average with Poland (29%) and Slovakia (8%) and not all with Hungary (0%) or Turkey (0%).
- Microsoft on the other hands cooperates rather well with Hungary (83%) and Turkey (76%).
- Facebook also responds well to Hungary (83%) and Turkey (66%), but less to Poland (29%), Portugal (38%) and Spain (37%).
- Yahoo cooperates rather well with Australia (51%) but **responds not at all** to Netherlands, **Norway**, Portugal and Switzerland.
- Microsoft on the other hand cooperates very well with Netherlands (83%), **Norway (82%)**, Portugal (85%) and Switzerland (74%).
- Twitter cooperates above average with Australia (58%), Japan (36%) and **Norway (50%)** but not at all with Turkey (0%) and below average with France (11%), Germany (16%) or Spain (12%)."



Norway: The Criminal Procedure Act of 1981

- General provisions, electronic evidence not regulated specifically
- No Norwegian case law available regarding transborder search for electronic evidence
- For the telecom sector: separate regulation. According to the Electronic Communication Act (based on the EU E-Privacy Directive) Section 2-9, third subsection, the police in Norway can request user information directly from telecom providers, without court order. This does not apply to non-telecom internet services, f.ex. website hosting.



The Criminal Procedure Act, Section 192:

“If any person is with just cause suspected of an act punishable pursuant to statute by imprisonment, a search may be made of his residence, premises or storage place in order to undertake an arrest or to look for evidence that may be seized or on which a charge may be created. (...)”

Does this apply also to transborder search?



Section 203:

“Objects that are deemed to be significant as evidence may be seized until a legally enforceable judgement is passed. The same applies to objects that are deemed to be liable to confiscation or to a claim for surrender by an aggrieved person.”

The term “objects” include electronic evidence, bank accounts, domain names etc.



Section 210

”A court may order the possessor to surrender objects that are deemed to be significant as evidence if he is bound to testify in the case. (...)

If delay entails a risk that the investigation will be impaired, an order from the prosecution authority may take the place of a court order. The decisions of the prosecution authority shall be submitted to the court for approval as soon as possible.”



Section 208

”Every person who is affected by a seizure may immediately or subsequently require the question whether it shall be ratified to be brought before a court. The prosecuting authority shall ensure that any such person shall be informed of this right.”



2017: a new legal instrument

The Criminal Procedure Act, Section 199a:

*When conducting a search of a data-processing system, the police may order everyone who is dealing with the said system to provide the information necessary for gaining access to the system **or to open it by use of biometric authentication.***

If someone refuses to comply with an order of biometric authentication as mentioned in the first subsection, the police may perform the authentication by use of force.

Decision regarding use of force in accordance with the second subsection, is done by the prosecuting authority. In case of urgency, the decision may be done by a police officer at the scene. The decision shall promptly be reported to the prosecuting authority.



Norway and The Budapest Convention

- The convention was signed by Norway 23.11.2001, ratified 30.06.2006 and went into force 1.10.2006.
- In 2005, Norwegian legislation were amended to harmonise the local legislation with the convention.
- Example: article 16, expedited disclosure of stored computer data and the new Section 215a in the Criminal Procedure Act
- Norway takes an active part in the work connected to the Convention, and we hope that the Convention can be extended to even more parties.
- NCIS Norway is the national 24/7 contact point.



Legal access to data in Norway – main points

- Search and seizure possible, based on general provisions in the Criminal Procedure Act
- Duty to assist, the Criminal Procedure Act, Article 199a: During a search of a computer system, the police can oblige anyone responsible for the system to give necessary information to access the system. This duty does not apply to suspects.
- Production orders, the Criminal Procedure Act, Article 210 Does not apply to suspects.
- Information about subscriber information for telcos, the Electronic Communications Act, Section 2-9, 3. subsection
- Legal access to services in other jurisdictions?



Human rights

Compare with international standards such as the European Convention on Human Rights, including

- Article 6: right to fair trial (including protection against self-incrimination)
- Article 8: right to respect for private and family life
- Article 10: freedom of expression
- The CoE Convention on Human rights is implemented in Norwegian law.



Data protection laws in Norway

- The general view: data protection laws and functioning institutions and practices to follow up the laws, are important to ensure public trust. With a high level of public trust, it's possible to collect and share data, and also to ensure that data are of high quality – recent and reliable information.
- The first Data Protection Act in Norway (1978), was inspired by a similar Swedish law (1973), the first data protection law in Europe. These laws, as well as other laws from this time period, were part of the background for CoE Convention 108.
- Current law in Norway based on the EU Directive 95/46/EC, to be updated in accordance with GDPR, as well as the Convention 108 principles.



2015: findings in EU supported research (the SURPRISE project)

http://surprise-project.eu/wp-content/uploads/2014/10/D6.6_Country_report_Norway_final_30.9.pdf

"The Norwegian Data Protection Authority ("Datatilsynet") is responsible for monitoring and enforcing the PDA. Their main task is to "facilitate protection of individuals from violation of their right to privacy through processing of their personal data" .

The Data Protection Authority is organized under the Ministry of Local Government and Modernization but executes its tasks independent from the Government and private interests. The DPA has existed since 1980, and is well known and respected among Norwegian citizens. The DPA is funded under the National Budget, and has in 2014 a budget of 38,624 mill NOK (approximately Euro 4,783,000). The budget has increased somewhat the last five years, from Euro 3,627,500 in 2009. The DPA has 40 employees. Decisions made by the Data Protection Authority may be appealed to the Privacy Appeals Board (Personvernemnda)."



Preserving or deleting data?

- The EU Data Protection **Directive 95/46/EC** Article 6 nr. 1 e):
"Member States shall provide that personal data must be: (...)
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected (...)
- Same principle in the new EU regulation, **GDPR**, Art. 5 nr. 1 b) and c)
1. Personal data shall be: (...)
*(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation**');*
*(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');*
- In other words: a certain duty to delete some personal data.
- This principle may limit the possibilities of voluntary data preservation for service providers in jurisdiction where this EU regulation applies.'
- These rules apply also in the Norwegian data protection act.



Law enforcement access vs data protection laws

- 2009: the Data Protection Authority in Norway reviewed practices at two ISPs, and concluded that they stored their customer's IP logs longer than necessary. Originally storing the logs for up to 5 months was based on billing purposes, but the ISPs had introduced flat rate subscriptions.
- A letter from the DPA: up to 21 days of storing IP logs would be acceptable, based on the ISPs internal security needs. No legal obligation to store IP logs.
- 2011: the Parliament later voted to implement the EU Data Retention Directive, but in 2014 the EU Court of Justice set this directive aside. The Norwegian data retention law had not yet been implemented, so the 2009 letters from the DPA were the only regulation left.
- Law enforcement in Norway had supported data retention, but in this case, the general principles in the data protection act combined with a lack of legal obligation to retain certain data for certain time periods, means lack of access to data logs older than 21 days (or less).
- Still, the reduced access to data due to data protection laws, is in principle not different to reduced access due to criminal procedural laws, foreign jurisdictions, deleted and/or encrypted data and several other challenges.



Legal access to IP logs vs data protection laws

- 2009: the Data Protection Authority in Norway reviewed practices at two ISPs, and concluded that they stored their customer's IP logs longer than necessary. Originally storing the logs for up to 5 months was based on billing purposes, but the ISPs had introduced flat rate subscriptions.
- A letter from the DPA: up to 21 days of storing IP logs would be acceptable, based on the ISPs internal security needs. No legal obligation to store IP logs.
- 2011: the Parliament later voted to implement the EU Data Retention Directive, but in 2014 the EU Court of Justice set this directive aside. The Norwegian data retention law had not yet been implemented, so the 2009 letters from the DPA were the only regulation left.
- Law enforcement in Norway had supported data retention, but in this case, the general principles in the data protection act combined with a lack of legal obligation to retain certain data for certain time periods, means lack of access to data logs older than 21 days (or less).
- Still, the reduced access to data due to data protection laws, is in principle not different to reduced access due to criminal procedural laws, foreign jurisdictions, deleted and/or encrypted data and several other challenges.



Data protection laws and the police registries

- The police has a clear interest to prevent unauthorised access and sharing of information from the police registries.
- NCIS Norway is the data controller for 17 central police data registers in Norway
- At NCIS Norway, currently 7 data protection officers (6 of them lawyers) to ensure compliance with the Police Registry Act and the general data protection laws, including the GDPR
- Some aspects: what information to store, how to process it, who to share it with, what to delete, when to delete it, access control of data, logging who has accessed the data in question
- Ensured compliance with the GDPR and the CoE Convention 108, also ensures trusted cooperation with other parties, including Europol
- Public trust in how the police handles personal data is important to get information from individuals and businesses. Example: cases regarding internet banking fraud.
- The Data Protection Authority have inspected NCIS Norway, including the police registries. These inspections have focused on documenting internal rules and regulations, documenting who has what responsibilities etc – the DPA is not looking into individual files or searching through the registries themselves.



From mutual trust to cooperation

September 2014:
NCIS Norway
received the "Rosing"
IT Security award
from The Norwegian
Computer Society,
based on work
against internet
banking fraud.

Rosing Årskonferanse
-et DND-event
Onsdag 25. november 2015, Kulturkirken Jakob, Oslo

KEYNOTE 2014 | PROGRAM 2014 | PRISENE 2014 | BILDER 2014 | GJESTER 2014

Årets IT-Sikkerhetspris: KRIPOS

IT-sikkerhetsprisen: KRIPOS

Årlig deler vi ut IT-sikkerhetsprisen for å skape interesse for, fokusere på og markere betydningen av IT- og informasjonssikkerhet.

Juryen for Rosing sikkerhetspris 2014 består av 6 representanter, 2 fra ISF, 2 fra ISACA og 2 fra DND.

Juryen har i år valgt en aktør som med begrensede ressurser har levert på høyaktuelle saker relatert til informasjonssikkerhet, og vist at Norge har dyktige og erfarne ressurser på området.

Vinneren utmerker seg ved å gå grundig til verks, analysere, dokumentere, åpent etablerer smidig samarbeid med aktuelle aktører for så å levere når saken fremdeles er aktuell

Årets Toppleder

- > Se vinner og nominerte
- > Se tidligere vinnere

Årets IT-direktør

- > Se vinner og nominerte
- > Deles ut for første gang

IT-sikkerhetsprisen

- > Se vinner og nominerte
- > Se tidligere vinnere

Årets Girl Geek

- > Se vinner og nominerte
- > Deles ut for første gang



POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

Eirik.tronnes.hansen@politiet.no