**Submission by the Government of Finland**

**Study on Freedom of Expression and the Telecommunications and Internet Access Sector**

**1. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) that may permit authorities to require Telecommunications and Internet Service Providers to:**

**a) Suspend or restrict access to websites or Internet and telecommunications networks**

*Information Society Code (917/2014)*

According to the Act Information Society Code (917/2014) (‘*tietoyhteiskuntakaari’*) the information society service provider can be ordered by a court to disable the access to the information stored by it.

Section 185 - *Order to disable access to information*

Upon request from a public prosecutor or a person in charge of inquiries or on application by a party whose right the matter concerns, a court may order the information society service provider referred to in section 184 to disable access to the information stored by it if the information is clearly such that keeping its content available to the public or its transmission is prescribed punishable or as a basis for civil liability. The court shall urgently process the application. The application cannot be approved without an opportunity for the service provider and the content provider an opportunity to be consulted except if the consultation cannot be arranged as quickly as the urgency of the matter so necessarily requires.

A court order must also be made known to the content provider. If the content provider is not known, the court may order the information society service provider to take care of notification.

An order ceases to be in effect unless charges are raised for an offence based on the content or transmission of information referred to in the order or, when concerning a liability, action is brought within three months of issuing the order. On request by a public prosecutor, by an injured party or by an interested party within the time limit referred to above, the court may extend this time limit by a maximum of three months.

The information society service provider and the content provider have the right to apply for reversal of the order in the court where the order was issued. When dealing with a matter concerning reversal of the order, the provisions of Chapter 8 of the Code of Judicial Procedure shall be observed. However, the court takes care of the necessary procedures to hear a public prosecutor. The reversal must be applied for within 14 days of the date when the applicant was notified of the order. The information must not be made available again when the hearing of the case concerning the reversal is pending unless otherwise ordered by the court dealing with the case. A public prosecutor has also the right to appeal the decision that reversed the order.

Restrictions of access may also be related to copyright issues:

Section 189 - *Prevention of access to material infringing copyright or neighbouring right*

A holder of a copyright or his/her representative may request the information society service provider referred to in section 184 to prevent access to material infringing copyright as prescribed in this section and in sections 191–193. The same applies to a holder of a neighbouring right and his/her representative if it concerns material infringing this right. 74 A request must first be presented to the content provider whose material the request concerns. If the content provider cannot be identified or if he/she does not remove the material or prevent access to it expeditiously, the request may be submitted to the information society service provider by notification prescribed in section 191.

Also the Copyright Act (404/1961, amendments up to 715/2016) permits the courts to require ISPs (*Internet Service Providers*) to suspend or restrict access to websites or the internet as well as to provide or facilitate access to customer data. Similar provisions are included also in the legislation on industrial property rights that are developed by the Ministry of the Employment and the Economy. These laws and regulations mentioned are coherent with each other. The development of the provisions regarding a suspected copyright infringement is done at the Ministry of Education and Culture and they implement Art. 8.3 of the Information Society Directive and the Enforcement Directive. Since 2006 the Copyright Act includes sections 60a – 60g covering the abovementioned area. Since June 2015, the provisions have been streamlined and they now include even the possibility for the rightholder to request the ISP to block the communication to the public of copyright protected material even in cases where the actual/alleged infringer cannot be identified. Previously the law included a provision about a temporary disconnection until the infringement could be substantially established by the court. A case has to be filed against the infringer within one month. As we know, most illegal websites tend to disguise the people running them. If the infringer can be identified the measures include also blocking of access to an internet connection if this is required to cease the communication to the public taking place without permission.

*Act on the Exercise of Freedom of Expression in Mass Media (460/2003)*

Section 18

On the request of the public prosecutor, the head of a pre-trial investigation, or the injured party, a court may order that the publisher, broadcaster or keeper of a transmitter, server or other comparable device is to cease the distribution of a published network message, if it is evident on the basis of the contents of the message that providing it to the public is a criminal offence. The court shall deal with the request as a matter of urgency. Before issuing a cease order, the court shall reserve the intended addressee of the order and the sender of the network message an opportunity to be heard, unless the urgency of the matter otherwise necessitates. Notice of the cease order shall be served also on the sender of the network message referred to therein. If the sender is unknown, the court may order that the keeper of the transmitter, server or other comparable device sees to the service. A cease order referred to in subsection (1) shall lapse, unless within three months of its issue a charge is brought for an offence arising from the contents of the relevant message, or a demand referred to in section 22 is made, or a tort action pertaining to the contents of the message is brought. On the request of the public prosecutor or the injured party, submitted before the deadline referred to above, the court may extend that deadline by three months at the most. The person who has been issued with a cease order, as well as the sender of the network message, have the right to apply for the reversal of the cease order from the court that originally issued it. The provisions of chapter 8 of the Code of Judicial Procedure apply to the proceedings for the reversal of a cease order. However, the court shall take the necessary measures to hear the public prosecutor in the case. The applications for a reversal shall be filed within fourteen days of the service of notice of the cease order. The network message shall not again be provided to the public while the reversal proceedings are pending, unless the court seised of the matter otherwise orders. Also the public prosecutor has standing to appeal against the reversal of a cease order. On the request of the public prosecutor or an injured party, the court may issue a cease order referred to in subsection (1) also when it is hearing charges based on the contents of a published message, a demand for a sanction referred to in section 22, or a tort action pertaining to the contents of the message. A cease order under this subsection shall not be open to appeal as a separate matter.

Section 17 of the same act concerns the release of identifying information for a network message:

 Section 17

On the request of an official with the power of arrest, as referred to in chapter 1, section 6(1), of the Coercive Measures Act (450/1987), a public prosecutor, or an injured party, a court may order the keeper of a transmitter, server or other similar device to release the information required for the identification of the sender of a network message to the requester, provided that there are probable reasons to believe that the contents of the message are such that providing it to the public is a – 5 – criminal offence. However, the identifying information may be ordered to be released to the injured party only in the event that he or she has the right to bring a private prosecution for the offence. The request shall be filed with the District Court of the domicile of the keeper of the device, or with the District Court of Helsinki, within three months of the publication of the message in question. The court may reinforce the order by imposing a threat of a fine. […]

**b) Provide or facilitate access to customer data;**

*Information Society Code (917/2014)*

According to the Act Information Society Code (917/2014), some Telecommunications and Internet service providers are obliged to retain customer data for purposes of the authorities.

Section 157 - *Obligation to store data for the purposes of the authorities*

Notwithstanding the provisions of this Part concerning the processing of traffic data, an undertaking designated by a separate decision of the Ministry of the Interior that has submitted a telecommunications notification *(operator under the retention obligation)* shall ensure, under the conditions prescribed below, that data under the retention obligation as referred to in subsections 2 and 3 are retained in accordance with retention times laid down in subsection 4. Data to be retained may be used only for the purposes of solving and considering charges for criminal acts referred to in Chapter 10(6)(2) of the Coercive Measures Act (806/2011).

The retention obligation applies to data related to:

1. a telephone service or SMS service provided by an operator under the retention obligation including calls for which a connection has been established but the call remains unanswered or is prevented from being connected due to network management measures;
2. Internet telephone service provided by an operator under the retention obligation, meaning service provided by a service operator enabling calls that are based on Internet protocol through to the end customer;
3. Internet access service provided by an operator under the retention obligation; In services referred to in subsection 2(1 and 2) above the retention obligation applies to the name and address of a registered user or a subscriber, subscription identifier and data that can be used to identify a communications service user or communications, including call transfers, according to the type, receiver, time and duration of communications. With regard to service referred to in subsection 2(1) the retention obligation applies to data that can be used to identify the device used and the location of the device and the subscriber connection it uses in the beginning of communications. With regard to the service referred to in subsection 2(3) above the retention obligation applies to the name and address of a subscriber and registered user, subscription identifier, installation address, and data that can be used to identify the communications service user, the device used in communications and the time and duration of the service. The data to be retained must be limited to what is necessary for identifying the facts referred to above in this section, with due consideration to the technical implementation of the service

The data of the services referred to above in subsection 2(1) must be retained for 12 months, the data of the services referred to in subsection 2(3) for 9 months and the data of the services referred to in subsection 2(2) for 6 months. The data retention time starts with the time of the communications.

The retention obligation does not apply to the contents of a message or traffic data generated through the browsing of websites.

A requirement for the retention obligation is that the data are available and generated or processed in connection with publicly available communications services provided on the basis of this Act or the provisions of the Personal Data Act (523/1999).

Further provisions on a more specific definition of data under the retention obligation may be issued by Government Decree.

Technical details of data under the retention obligation are defined in a Finnish Communications Regulatory Authority regulation.

*Act on Military Discipline and Combating Crime in the Defence Forces (255/2014)*

Section 37 - *Powers of the Defence Command Finland’s (DCF) public officials when conducting criminal investigations*

The provisions of the Criminal Investigation Act, Coercive Measures Act and any other act on the powers of police officers in criminal investigations apply to the DCF’s public officials that are responsible for conducting criminal investigations. The DCF’s officials are allowed to use only the following covert coercive measures provided in Chapter 10 of the Coercive Measures Act: […] 6) gathering data identifying a network address or terminal end device.

Section 44 - *Right to obtain information from private organizations*

The DCF has the right to obtain contact information about a subscription that is not listed in a public directory or data identifying any subscription, e-mail address or other network address or terminal end device if the information is needed in individual cases to perform tasks referred to in section 35.

The provisions on the cases where the DCF is the competent authority to perform criminal investigations are laid down in section 35.

Section 89 - *Powers to prevent and detect crimes*

The provisions of the Police Act (872/2011) on powers to prevent and detect crimes apply to the powers of the public officials of the Finnish Defence Forces (FDF) responsible for preventing and detecting crime when they are performing tasks provided in section 86(1). Of the powers referred to in Chapter 5 (Secret methods of gathering intelligence) of the Police Act, the above-mentioned FDF’s public officials are allowed to use only […] 7) gathering data identifying a network address or terminal end device.

The secret methods of intelligence gathering may only be used to detect the following crimes:

1) compromising the sovereignty of Finland

2) incitement to war

3) treason and aggravated treason

4) espionage and aggravated espionage

5) disclosure of a national secret

6) unlawful intelligence operations

The FDF’s crime detection and prevention personnel must inform the Finnish Security Intelligence Service after using any methods of secret intelligence gathering.

The provisions of the Police Act apply to protection of secret intelligence gathering and use of surplus information (sections 46, 53 and 54).

Section 93 - *Right to obtain information from private organizations*

The public officials of the FDF who are responsible for preventing and detecting crimes have the right to obtain contact information about a subscription that is not listed in a public directory or data identifying any subscription, e-mail address or other network address or terminal end device if the information is needed in individual cases to perform tasks referred to in section 86(1).

The provisions on the FDF’s powers to perform tasks concerning crime prevention and detection are laid down in section 86(1).

Section 128 - *Oversight conducted by the Ministry of Defence*

This section refers to section 63 of the Police Act and section 65 of the Coercive Measures Act. According to these two sections, the Ministry of Defence shall provide the Parliamentary Ombudsman each year with a report on the use and oversight of secret intelligence gathering methods and on their protection, and on the use and supervision of covert coercive measures / secret intelligence gathering methods and their protection.

There is no legal requirement for the FDF to inform the target that the FDF has gathered data identifying a network address or terminal end device that has identified the target. Information on the use of secret methods of intelligence gathering is not in the public domain.

*The Emergency Powers Act (1552/2011)*

The Emergency Powers Act (1552/2011) lays down provisions on the means for the authorities to control overall access to the internet as a whole or to specific internet services (sections 60, 61 and 62). This Act belongs to the legislative field of the Ministry of Justice and the powers can be used by the Ministry of Transport and Communications. As stated in its Section 1, the Act shall only apply during a state of defence.

*New bill on civilian and military intelligence*

In Finland, a new bill concerning civilian and military intelligence is under preparation in concert by the Ministry of Justice, Ministry of the Interior and the Ministry of Defence. The main amendment to the current legislation would be the introduction of network traffic intelligence and intelligence on foreign information systems. These two new intelligence methods could have an impact on the area in question.

*Criminal investigations*

In Finland, the criminal investigation is conducted by the police. In addition to the police, the border guard, customs and military authorities can also act as criminal investigation authorities in some cases. Provisions on the criminal investigation of offences are laid down in the Criminal Investigation Act (805/2011) and provisions on the coercive measures used in the criminal investigation of offences are laid down in the Coercive Measures Act (806/2011). Chapter 5 of the Police Act (872/2011) regulates secret methods of gathering intelligence. (See sections 1-39) Section 25 regulates police rights gathering data identifying a network address or terminal end device. To prevent an offence, the police may use a technical device to obtain data identifying a network address or terminal end device if the most severe punishment by law for the offence to be prevented is at least one year’s imprisonment.

*Copyright issues*

According to Section 60a of the Copyright Act (Supply of contact information), the author or his representative are entitled, in individual cases, notwithstanding confidentiality provisions, by the order of the court of justice, to obtain contact information of a tele subscriber who, unauthorized by the author, makes material protected by copyright available to the public to a significant extent in terms of the protection of the author's rights. The maintainer of a transmitter, server or a similar device or other service provider acting as an intermediary is thus obliged to give the information without undue delay. The number of these cases have grown during the two last years as rightholders and law firms who represent them have started to also take action in cases of individual infringements.

**2. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) on the public disclosure of requests made or actions taken to a) suspend or restrict access to websites and telecommunications networks and the requests to provide or b) facilitate access to customer data.**

*Constitution of Finland*

According to the Constitution of Finland (731/1999), everyone has a right of access to information.

Section 12 - *Freedom of expression and right of access to information*

Everyone has the freedom of expression. Freedom of expression entails the right to express, disseminate and receive information, opinions and other communications without prior prevention by anyone. More detailed provisions on the exercise of the freedom of expression are laid down by an Act. Provisions on restrictions relating to pictorial programmes that are necessary for the protection of children may be laid down by an Act.

Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings.

*Act on the Openness of Government Activities (621/1999)*

This principle of publicity is further regulated in the Act on the Openness of Government Activities (621/1999).

According to the Act, all official documents are in the public domain, unless their publication has been specifically restricted. The objectives of the right of access and the duties of the authorities provided in the Act are to promote openness and good practice on information management in government, and to provide private individuals and corporations with an opportunity to monitor the exercise of public authority and the use of public resources, to freely form an opinion, to influence the exercise of public authority, and to protect their rights and interests.

*The Police Act (872/2011)*

As to authorities’ rights to obtain information, in the Police Act Chapter 4 section 3 there is a provision on obtaining information from a private organization or person. At the request of a commanding police officer, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members and employees of an organization. The police have the same right to obtain information needed in a police investigation referred to in Chapter 6 if an important public or private interest so requires.

In individual cases, the police have the right to obtain on request from a telecommunications operator and a corporate or association subscriber contact information about a network address that is not listed in a public directory or data identifying a network address or terminal end device if the information is needed to carry out police duties. Similarly, the police have the right to obtain postal address information from organizations engaged in postal services.

*Information Society Code (917/2014)*

There are also provisions in the Information Society Code (917/2014) about the right of certain other authorities to obtain information:

Section 321 - *The right of emergency services authorities to obtain information*

A telecommunications operator is obliged to disclose the following to an Emergency

Response Centre, a Marine Rescue Coordination Centre, a Marine Rescue Sub-

Centre or the police for processing purposes:

1) subscriber connection identifier and location data of the subscriber connection and terminal device from which an emergency call is placed, and information on the subscriber, user and installation address; and

2) identifier and location data showing the location of the user terminal device and subscriber connection to which the emergency call applies if, in the considered opinion of the authority receiving the emergency call, the user is in obvious distress or immediate danger.

The information referred to in subsection 1 above shall be released notwithstanding the secrecy obligation referred to in section 136 and the requirements for processing location data specified in sections 160–161, and without reference to what the subscriber or user may have agreed with the telecommunications operator concerning the secrecy of such information.

An added value service provider has the right to disclose information referred to in subsection 1 to the respective authority.

Section 322 - *Certain other authorities’ right to obtain information*

The right of authorities to receive traffic data for the purpose of preventing, uncovering or investigating crimes is laid down in the Police Act, Border Guard Act (578/2005), Act on the Processing of Personal Data by the Border Guard (579/2005), Customs Act (1466/1994), and Coercive Measures Act.

Data to be retained under section 157 of this Act is only obtainable from service providers by the authorities who have a legal right to obtain the data.

Section 159 - *Statistics concerning the use of data to be retained for the purposes of the authorities*

The Ministry of the Interior shall provide the Parliamentary Ombudsman on a yearly basis with statistics on using data retained by virtue of this Act. The statistics shall include: 1) the cases in which retained data were provided to the authorities; 2) the cases where the authorities’ requests for retained data could not be met; 3) the time elapsed between the date on which the data were retained and the date on which the authorities requested for the data.

The Ministry of the Interior shall also take the statistics referred to in subsection above into account in its reports about telecommunications interception and monitoring to the Parliamentary Ombudsman by virtue of the Police Act (872/2011), Coercive Measures Act or any other Act.

*The Copyright Act (679/2006)*

The Copyright Act includes Section 59a (679/2006) about the publication of judgement in a civil matter concerning copyright and upon the request of plaintiff of information about the final judgment in which the defendant has been found to infringe copyright. The court would in these cases order a defendant to recompense costs incurred. This provision has not been used frequently. Normally decisions are published on the website of the court so any other broader dissemination of the judgement would be based on this provision. As regards publishing or informing the customer who is subject to a request for supplying customer data, normally the customer of an ISP whose data has been requested by the rightholder will find out about the request only when the rightholder sends a letter to him/her about an alleged infringement of copyright.

 Section 59a

A court of justice may, in a civil matter concerning copyright and upon the request of plaintiff, order a defendant to recompense costs incurred from the dissemination, by using appropriate measures, of information about the final judgment in which the defendant has been found to infringe copyright. The order shall not be issued, if the dissemination of the information is limited elsewhere in the law. When considering the issuing of the order and the contents of it, a court of justice shall take into account the general relevance of the dissemination to the public, the quality and extent of the infringement, the costs which are caused by the dissemination and other corresponding matters.

A court of justice shall order a maximum amount of the reasonable dissemination costs to be recompensed by the defendant. The plaintiff is not entitled to compensation, if the information about the judgment has not been disseminated within the time that a court of justice ordered to be run from a passed non-appealable judgement.

**3. Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) governing the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers, and Internet exchange points;**

*Information Society Code (917/2014)*

The activities of private entities are regulated in the Information Society Code (917/2014).

Section 242 - *Availability and information security related to the data on location of telecommunications cable*

The telecommunications operator shall provide data on the location of telecommunications cable *(cable data)* in digital form. The telecommunications operator shall ensure that it is technically possible to provide cable data from one central location.

Cable data must be processed in a manner as to properly protect them against information security violations and threats.

Ficora [Finnish Communications Regulatory Authority] may issue further technical regulations on the digital form of cable data and information security when processing them.

Furthermore, Section 243 of the same Act lays down quality requirements for a communications network and service:

Section 243

Public communications networks and communications services and the communications networks and services connected to them shall be planned, built and maintained in such a manner that [*e.g.*]

1) the technical quality of electronic communications is of a high standard and information security is ensured;

2) the networks and services withstand normal, foreseeable climatic, mechanical, electromagnetic and other external interference as well as information security threats;

3) their performance, functionality, quality and reliability can be monitored; and that

4) significant information security violations and threats against them and other defects and disruptions that significantly interrupt their functionality can be detected.

In addition, the Finnish Act *‘radiolaki’* (Act on Radio Frequencies and Telecommunications Equipment (1015/2001)) lays down provisions on e.g. placing telecommunications equipment on the market and offering them for sale.

*New bill on civilian and military intelligence*

The abovementioned bill under preparation concerning civilian and military intelligence [see answer to 1b)] may create a need for the authorities to cooperate with private sector entities concerning allocation of entry points to the telecommunication cables and other means that are required to perform network traffic intelligence. There is however no intention to create a need for the authorities to require encryption algorithms from private entities or to establish cooperation between public and private entities in creating or installing backdoors to private sector software.

**4. Remedies available in the event of undue restrictions on Internet and telecommunications access or undue access to customer data**

There are legal remedies for the person concerned in the matter. A district court decides on the use of some coercive measures (for example many covert (secret) coercive means). If the measure is ordered by the police official or in some rare cases by the prosecutor the court shall on the request of the concerned person decide whether the measure is to remain in force (for example travel ban and seizure). Concerning some coercive measures the court shall on the request of the concerned person reconsider whether the measure is to remain in force (for example remand and seizure). All coercive measure court decisions are covered either by the possibility to make an ordinary appeal or by the possibility to make an extraordinary appeal (no time limit and an urgent hearing).

Concerning Market Court processes and copyright matters, the Market Court dealing with a claim for supply of information about a customer considers that the information can be supplied – the ISP will supply the information. It may also require that the ISP keeps any such information available from the date of the claim if this would be necessary to later file a law suit against the holder of this data. If the parties i.e. the recipient of the decision allowing access to the customer data considers that requirements in the law have not been fulfilled (i.e. material protected by copyright has not been made available to the public to a significant extent in terms of the protection of the author's rights) the parties need to appeal the decision. Currently the ISP customer whose information has been accessed based on the court order on supply of information and who considers that there has not been enough evidence or the court has not interpreted the law correctly is unable, at this stage of the Market

Court process, to file a claim in the case. Only if the case escalades into a civil case/procedure the defendant may appeal the decision.

Essential sanctions have to do with offences in office (the Criminal Code (39/1889, amendments up to 617/2016), Chapter 40) for example with violations of official duty (Section 9 of Chapter 40 of the Criminal Code) if officials’ rights to information have been misused.

**5. Other relevant laws, policies or initiatives to promote or enhance Internet**

**accessibility and connectivity, including measures to promote network**

**neutrality**.

The national information security strategy (adopted by the Ministry of Transport and Communications according to the Strategic Programme of Prime Minister Juha Sipilä’s Government) is also intended to focus on promoting and protecting privacy and other fundamental rights. According to the strategy Finland will strive to reduce the country risks within the EU and the international community so that the free flow of data can be secured without compromising the fundamental rights of citizens and the objects of legal protection of businesses. Finland’s goal is to achieve a common approach within the EU and the international community to the conditions and limitations of state interference in the privacy or information security of a person in another State.

Measures to promote network neutrality have been part of the Finnish legislation for long and the situation was further clarified when the Information Society Code was implemented in 2015. Since then the EU has adopted Regulation (EU) 2015/2120 on open Internet access and roaming on public mobile communications networks, which has led to revocation of the conflicting sections of the national legislation. At present, there are no major issues concerning network neutrality in Finland and the Regulation has not been de facto applied. Should this be necessary in the future, national authorities would be guided by the BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.

Additional measures to promote Internet accessibility and connectivity in Finland include all consumers’ and businesses’ right to obtain basic communications services, i.e. the services pertaining to universal service, to their place of residence or to place of business. Such services include e.g. fixed or wireless telephone subscription as well as Internet access of at least 2 Mbps, which is to be gradually increased to 10 Mbps by the year 2021. These provisions have in practice improved access to Internet in areas with low population density by increasing the numbers of commercial service providers in those areas, as universal services are often more expensive to provide.

Finland is known to have fast and extensive mobile networks that supplement fixed broadband networks, as well as affordable broadband subscription prices. This results partly from an effective national spectrum policy as well as market-based policies.

*Open Science and Research Initiative*

As to some initiatives, the Ministry of Education and Culture of Finland promotes research information availability and open science through the Open Science and Research Initiative (*ATT, Finnish acronym*), set out for the years 2014 – 2017. The objective for Finland is to become one of the leading countries in openness of science and research by the year 2017 and to ensure that the possibilities of open science will be widely utilized in our society. In addition to this, the ambition is to promote the trustworthiness of science and research, support the culture of open science within the research community, and to increase the societal and social impact of research and science.

Open science and research excites citizens, companies and decision-makers, and embraces new ideas and generates valuable understanding. Open science increases the opportunities to participate in scientific research. This calls for an extensive accessibility to open publications, open research data, open research methods and tools, as well as increasing skills, knowledge and support. The status of the openness of research organizations’ operational culture was evaluated in 2015.According to this analysis, no higher education institution has yet reached the highest set level of openness. The Universities of Helsinki and Jyväskylä have reached the second-highest level. Five institutions were placed at the third level, 14 at the fourth, and 9 at the lowest. Over half of all institutions have been actively promoting openness. When it comes to openness, universities are clearly ahead of polytechnics. The role of libraries in promoting openness in higher education institutions on local level is a key for success. In order to monitor progress, a similar analysis will be repeated annually during the Open Science and Research Initiative, that is, until 2017. In 2016, also funding organizations are evaluated. (<http://openscience.fi/>)

*Some general notions on countering cybercrime and on police action*

Measures used in preventing and detecting crimes are regulated in the Police Act (872/2011) and measures used in investigations are regulated in the Coercive Measures Act (806/2011). They include interfering with the use of human rights and fundamental freedoms. Deeply interfering measures are usually allowed only in investigations of serious offences. In the Police Act (872/2011) are provisions concerning police duties and powers. In the first chapter there are general principles that have to be taken into account when using the power regulated in the Act.

Police Act (872/2011)

Section 2 - *Respecting fundamental and human rights*

The police shall respect fundamental and human rights and, in exercising their powers, choose from all reasonable options the course of action that best asserts these rights.

Section 3 - *Principle of proportionality*

Police action shall be reasonable and proportionate with regard to the importance, danger and urgency of the duty; the objective sought; the behavior, age, health and other specifics of the person targeted by the action; and other factors influencing the overall assessment of the situation.

Section 4 - *Principle of minimum intervention*

The police shall not take action that infringes anyone’s rights or causes anyone harm or inconvenience more than is necessary to carry out their duty.

Section 5 - *Principle of intended purpose*

The police may exercise their powers only for the purposes provided by law.