Report of Various Size

Monthly data collection on the current reform of intelligence legislation

Submission template

Country: Sweden

Contractor's name: Emerga Research and Consulting

Author(s) name: Maria Nilsson

Reviewed by: Dr. Elisabeth Abiri

Period covered: August 2016 – April 2017

1. **Legislative reform(s)**
(Please, highlight the key aspect(s) of the reform, summarise any key report published in the context of the reform procedure)

The Government Bill of 2014, Covert coercive measures against serious crimes (*Hemliga tvångsmedel mot allvarliga brott*),[1] made a number of temporary acts on "covert coercive measures" permanent as of 1 January 2015. Amendments were also made to the Code of Judicial Procedure (*Rättegångsbalk [1942:740]*)[2] to include the permanent acts in the Code, which had not been included before due to their temporary nature. Some of the amendments of the Code differed somewhat from the Act on signals intelligence in the defence intelligence (*Lag [2008:717] om signalspaning i försvarsunderrättelseverksamhet*),[3] which in turn led to legal confusion. To resolve this, the Government presented the Bill on Reinstatement of the provision in the Act on signals intelligence of defence intelligence (*Återställande av bestämmelse i lagen om signalspaning i försvarsunderrättelseverksamhet, Proposition 2015/16:126*).[4] The so-called destruction obligation of section 7, paragraph 3 of Act was amended to be in tune with the Code. The provision now only applies to retrieved messages between a crime suspect and his or her defence attorney.[5] The Swedish Foreign Intelligence Inspectorate (*Statens inspektion av försvarsunderrättelseverksamhet [SIUN]*) is the oversight mechanism for the Act on signals intelligence in the defence intelligence (*Lag*

[1] Sweden, Ministry of Justice *(Justitiedepartementet),* Government Bill "Covert coercive measures against serious crimes" *(Proposition [2013/24:237] Hemliga tvångsmedel mot allvarliga brott*), 22 August 2014, available at: www.regeringen.se/contentassets/cc6ff48d963b40cea1eebed07ba09644/hemliga-tvangsmedel-mot-allvarliga-brott-prop.-201314237

[2] Sweden, Code of Judicial Procedure *(Rättegångsbalk [1942:740])*, 1 January 2015, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/rattegangsbalk-1942740_sfs-1942-740

[3] Sweden, Act on signals intelligence in the defence intelligence" *(Lag [2008:717] om signalspaning i försvarsunderrättelseverksamhet)*, 10 July 2008, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717

4 Sweden, Government Bill, "Reinstatement of the provision in the Act on signals intelligence of defence intelligence" *(Återställande av bestämmelse i lagen om signalspaning i försvarsunderrättelseverksamhet, Proposition 2015/16:126),* available at: http://riksdagen.se/sv/dokument-lagar/dokument/proposition/aterstallande-av-bestammelse-i-lagen-om_H303126

[5] Sweden, Government Bill, "Reinstatement of the provision in the Act on signals intelligence of defence intelligence" *(Återställande av bestämmelse i lagen om signalspaning i försvarsunderrättelseverksamhet, Proposition 2015/16:126),* available at: http://riksdagen.se/sv/dokument-lagar/dokument/proposition/aterstallande-av-bestammelse-i-lagen-om_H303126

[2008:717] om signalspaning i försvarsunderrättelseverksamhet),[6] which includes the paragraph on data destruction.[7]

On 6 December 2016, the Ministry of Justice (*Justitiedepartementet)* asked a number of relevant authorities, among them the Swedish Commission on Security and Integrity Protection (*Säkerhets och integritetsskyddsnämnden, SIN)*[8] to declare their position (*komma med ett yttrande*) on the Ministry's memorandum (*promemoria*) The temporary provision in the Data Collection Act remains in force (*Fortsatt giltighet av en tidsbegränsad bestämmelse i inhämtningslagen, Ju2016/08776/Å*). The memorandum itself is not available at the Ministry's website. However, the pronouncements from the Commission[9] and e.g. the Swedish Customs (*Tullverket*)[10] and the Swedish National Courts Administration (*Domstolsverket*)[11] are available online. The temporary provision concerns the third section of Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*).[12] The Data Collection Act was made permanent on

---

[6] Sweden, Act on signals intelligence in the defence intelligence (*Lag [2008:717] om signalspaning i försvarsunderrättelseverksamhet*), 10 July 2008, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717

[7] Sweden, Ordinance with instruction for the Swedish Foreign Intelligence Inspectorate (*Förordning [2009:969] med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*),15 October 2009, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2009969-med-instruktion-for-statens_sfs-2009-969

[8] The Commission on Security and Integrity Protection supervises the use by crime-fighting agencies of secret surveillance and qualified assumed identities and associated activities. The Commission also supervises the processing of personal data by the Swedish Police (*Polismyndigheten*), some parts of the Swedish Economic Crime Authority (*Ekobrottsmyndigheten*) and the Swedish Security Service (*Säkerhetspolisen, SÄPO*). The supervision aims at ensuring that the activities are conducted in accordance with laws and other regulations.

[9] Sweden, Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden,* SIN) Continued validity of a temporary provision in the Data Collection Act, memorandum (*Fortsatt giltighet av en tidsbegränsad bestämmelse i inhämtningslagen, Ju2016/08776/Å*), reference number 218-2016, 25 January 2017, available at: www.sakint.se/Fortsatt-giltighet-av-en-tidsbegraensad-bestaemmelse-i-inhaemtningslagen.pdf

[10] Sweden, Swedish Customs (*Tullverket*) Continued validity of a temporary provision in the Data Collection Act, memorandum (*Fortsatt giltighet av en tidsbegränsad bestämmelse i inhämtningslagen, Ju2016/08776/Å*), reference number STY 2016-1062, 23 January 2017, available at: www.tullverket.se/download/18.792224361590183a4d34193/1485166450208/STY+2016-1062+Promemoria+om+fortsatt+giltighet+av+en+tidsbegr%C3%A4nsad+best%C3%A4mmelse+i+inh%C3%A4mtningslagen.pdf

[11] Sweden, Swedish National Courts Administration (*Domstolsverket*) Consultation Response on the memorandum Continued validity of a temporary provision in the Data Collection Act, memorandum (*Remissyttrande över promemorian Fortsatt giltighet av en tidsbegränsad bestämmelse i inhämtningslagen, Ju2016/08776/Å*), reference number 2061-2016, 27 January 2017, available at: www.domstol.se/Publikationer/Remisser/2061-2016.pdf

[12] Sweden, Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), 16 May 2012,

1 January 2015 except for section 3, which has remained temporary first to 1 January 2016, with extensions first to 1 January 2017 and then to 1 January 2018. The memorandum proposes a fourth extension until 1 January 2019.

The overall aim of the Data Collection Act is to grant the Police (*Polisen*), the Secret Service (*Säkerhetspolisen, SÄPO*) and the Swedish Customs (*Tullverket*) permission to retrieve secret intelligence information on electronic communication[13] from the providers of electronic communications networks or electronic communications services.[14] The second (permanent) section of the Data Collection Act stipulates that the law enforcing authorities can collect data; 1) if the data may be of particular importance to anticipate, prevent or detect criminal activity involving the offenses that lead to imprisonment for two years or more; and 2) if the reasons behind the measure is more vital than the intrusion of the personal integrity of those affected.[15] However, the third (temporary) section allows for data collection also for offenses that lead to *less* than two years' imprisonment if there is a possibility that the measure may anticipate, prevent or detect sabotage, hijacking, maritime or aircraft sabotage or airport sabotage, violations of civil liberties, espionage, gross espionage, unauthorized handling of secret information, gross unauthorized handling of secret information or illegal intelligence activities against Sweden, against a foreign power, or against individuals, industrial espionage terrorist crimes as well financing of gross crimes.[16]

Interestingly, the Swedish Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden, SIN*) does not recommend (*tillstyrker*) that the temporary provision in the Data Collection Act remains in force for another year. The Commission refers to the preliminary ruling of the Court of Justice of the European Union on 21 December 2016 concerning the joint cases C-203/15 and C-698/15, which shows that the current Swedish

available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[13] The Data Collection Act only refer to meta data, i.e. which messages that are transferred to or from a particular phone number or address; which mobile phones or the like that has been in a certain area for a certain time; and which areas a particular mobile phone or the like has been at a certain time. The prerequisite is that it applies to "prevent, deter or detect" severe crime.

[14] Sweden, Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), 16 May 2012, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[15] Sweden, Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), section 2, 16 May 2012, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[16] Sweden, Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), section 3, 16 May 2012, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

arrangements regarding the storage and retrieval of electronic communications is not in conformity with EU law.[17]

Another memorandum Processing of personal data within the National centre for terrorist threat assessment (*Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning*)[18] that contains proposals to enhance the exchange of information within the National centre for terror threat assessment[19] was presented by the Ministry of Justice (*Justitiedepartementet*) in August and sent for referral in September 2016.[20] The aim of the memorandum was to suggest changes to a number of laws to enable the authorities in question to share necessary information electronically when making their strategic assessments of terrorist threats. The deadline for the responses was on 16 December 2016 and the summary of the responses is not available yet. However, it is important to follow the developments, since the memorandum suggests amendments to:

1. Act on the processing of personal data in the Armed Forces' Defence Intelligence and Military Security Service (*Lag [2007:258] om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst*);[21]
2. Act on the processing of personal data in the National Defence Radio Establishment's intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklings-verksamhet*);[22]

---

[17] Swedish Commission on Security and Integrity Protection (*Säkerhets och integritetsskyddsnämnden*) Declaration concerning the temporary provision in the Data Collection Act remains in force, reference number 218-2016 (*Yttrande om Fortsatt giltighet av en tidsbegränsad bestämmelse i inhämtningslagen,* Dnr 218-2016)*,* 25 January 2017, available at: www.sakint.se/Fortsatt-giltighet-av-en-tidsbegraensad-bestaemmelse-i-inhaemtningslagen.pdf

[18] Sweden, Ministry of Justice (*Justitiedepartementet*) Processing of personal data within the National centre for terrorist threat assessment (*Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning*), available at: www.regeringen.se/rattsdokument/departementsserien-och-promemorior/2016/09/ds-201631/

[19] National centre for terror threat assessment is a permanent official joint working group with staff from the Security Service (*Säkerhetspolisen, SÄPO*), the National Defence Radio Establishment (*Försvarets radioanstalt*) and the Military intelligence and security service of the armed forces (*Militära underrättelse- och säkerhetstjänt, MUST*).

[20] Sweden, Ministry of Justice, (*Justitiedepartementet)* Processing of personal data within the National centre for terrorist threat assessment (*Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning*), available at: www.regeringen.se/rattsdokument/departementsserien-och-promemorior/2016/09/ds-201631/

[21] Sweden, Act on the processing of personal data in the Armed Forces' Defence Intelligence and Military Security Service (*Lag [2007:258] om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst*)*,* 10 May 2007, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007258-om-behandling-av-personuppgifter-i_sfs-2007-258

[22] Sweden, Act on the processing of personal data in the National Defence Radio Establishment's intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*)*,* 10 May 2007, available at:

3. Police data act (*Polisdatalag [2010: 361]*);[23]
4. Ordinance on the processing of personal data in the Armed Forces' Defence Intelligence and Military Security Service (*Förordning [2007:260] om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst*);[24]
5. Ordinance on the processing of personal data in the National Defence Radio Establishment's intelligence and development activities (*Förordning [2007:261] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*);[25]
6. Police Data Ordinance (*Polisdataförordning [2010:1155]*).[26]

On 21 December 2016, the Stockholm Administrative Court of Appeal (*Kammarrätten i Stockholm*) received a preliminary ruling (*förhandsavgörande*) from the Court of Justice of the European Union[27] in relation to case no. 7380-14 between Tele2 Sverige Ltd. and the Swedish Post and Telecom Authority (*Post- och telestyrelsen, PTS*), which it had required on 29 April 2015. Case 7380-14 concerned an order sent by PTS to Tele2 Sverige requiring the latter to retain traffic and location data in relation to its subscribers and registered users.[28]

---

https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007259-om-behandling-av-personuppgifter-i_sfs-2007-259

[23] Sweden, Police data act (*Polisdatalag [2010: 361]*), 20 May 2010, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/polisdatalag-2010361_sfs-2010-361

[24] Sweden, Ordinance on the processing of personal data in the Armed Forces' Defence Intelligence and Military Security Service (*Förordning [2007:260] om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst*), 10 May 2007, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2007260-om-behandling-av_sfs-2007-260

[25] Sweden, Ordinance on the processing of personal data in the National Defence Radio Establishment's intelligence and development activities (*Förordning [2007:261] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), 10 May 2007, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2007261-om-behandling-av_sfs-2007-261

[26] Sweden, Police Data Ordinance (*Polisdataförordning [2010:1155]*), 28 October 2010, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/polisdataforordning-20101155_sfs-2010-1155

[27] European Court of Justice, Judgment of the Court (Grand Chamber) ECLI:EU:C:2016:970, 21 December 2016, available at: http://curia.europa.eu/juris/liste.jsf?num=C-203/15

[28] Background: As a reaction on the ruling of the European Court of Justice on 8 April 2014, Digital Rights Ireland and Others ('the Digital Rights judgment', EU:C:2014:238) that found the EU Directive 2006/24 invalid, Tele2 Sverige, a provider of electronic communications services established in Sweden, informed the Swedish Post and Telecom Authority (*Post- och telestyrelsen, PTS*) on 9 April 2014 that it would cease, to retain electronic communications data, covered by the Law on electronic communications (*Lag [2003:389] om elektronisk kommunikation*) as from 14 April 2014, and that it would erase data retained prior to that date. On 15 April 2014, Rikspolisstyrelsen (*Swedish National Police Authority*) sent a

The legal proceedings had been temporarily stayed by the Stockholm Administrative Court of Appeal since 29 April 2015 in the anticipation of the preliminary ruling. The Court requested that the European Court of Justice should consider the following questions in its preliminary ruling:

1) Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

2) If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:

    a. access by the national authorities to the retained data is determined as [described in paragraphs 19 to 36 of the order for reference];

    b. data protection and security requirements are regulated as [described in paragraphs 38 to 43 of the order for reference]; and

    c. all relevant data is to be retained for six months, calculated as from the day when the communication is ended, and subsequently erased as [described in paragraph 37 of the order for reference]

---

complaint to the PTS concerning Tele2 Sverige's cessation to send such data to the Police Authority. On 29 April 2014, the Swedish Minister of Justice appointed a special rapporteur to examine the Swedish legislation at issue in the light of the Digital Rights judgment. In a report dated 13 June 2014, entitled Data retention, EU law and Swedish law; 'the 2014 report' (*Datalagring, EU-rätten och svensk rätt, Ds 2014:23*), the special rapporteur concluded that the national legislation on the data retention, as set out in paragraphs 16a to 16f of the Law on electronic communications, was not incompatible with either EU law or the European Convention on Human Rights. The special rapporteur stated that the Digital Rights judgment could not be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle. Consequently, on 19 June 2014 the PTS informed Tele2 Sverige that it was in breach of its obligations under the national legislation in failing to retain the data covered by the Law on electronic communications for six months. On 27 June 2014, the PTS ordered Tele2 Sverige to re-commence its data retention, by no later than 25 July 2014. Tele2 Sverige remained that 'the 2014 report' was based on a misinterpretation of the Digital Rights judgment and that the obligation to retain data was in breach of the fundamental rights guaranteed by the Charter. Thus, the company brought an action before the Stockholm Administrative Court (*Förvaltningsrätten i Stockholm*) challenging the PTS's order. When that court dismissed the action on 13 October 2014, Tele2 Sverige brought an appeal against that judgment before the Stockholm Adminstrative Court of Appeal (*Kammarrätten i Stockholm*).

The case C-203/15 was decided by the ruling of European Court of Justice on 21 December 2016.[29] The answer to the first question was that Article 15 (1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52 (1) of the Charter, must be interpreted as ruling out national legislation, which provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users of electronic communication for the purpose of fighting crime. The Court of Justice's answer to the second question was that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as ruling out national legislation governing the protection and security of traffic and location data and, especially, access of the competent national authorities to the retained data if the objective pursued by that access is not restricted solely to fighting serious crime, if access is not subject to prior review by a court or an independent administrative authority, and if there is no requirement that the data concerned should be retained within the European Union.

The ruling of the European Court of Justice led Tele2 Sverige to request an inhibition of the appealed order by the Swedish Post and Telecom Authority (*Post- och telestyrelsen, PTS*), that required the company to retain traffic and location data in relation to its subscribers and registered users until the Stockholm Administrative Court of Appeal (*Kammarrätten i Stockholm*) delivers its verdict. The inhibition was granted until further notice on 22 December 2016.[30]

On 8 March 2017, the Stockholm Administrative Court of Appeal (*Kammarrätten i Stockholm*) passed its judgement in the case above.[31] The Court of Appeal followed the preliminary ruling from the Court of Justice of the European Union. In their judgement, the Stockholm Administrative Court of Appeal (*Kammarrätten i Stockholm*) noted that the preliminary ruling of the Court of Justice of the European Union concerning the joined Cases C-203/15 and C-698/15, make it is clear that the Swedish laws and regulations[32] are inconsistent with Article 15.1 of Directive 2002/58/EC and Articles 7, 8, 11 and 52.1 of the EU's Charter of Fundamental Rights. Consequently, the Swedish legislation is in breach of EU law. On the same day, 8 March 2017, the Swedish Post and Telecom Authority (*Post- och telestyrelsen, PTS*) informed that the judgement of the Stockholm Administrative Court of Appeal (*Kammarrätten i Stockholm*)

---

[29] European Court of Justice, Judgment of the Court (Grand Chamber) ECLI:EU:C:2016:970, 21 December 2016, available at: http://curia.europa.eu/juris/liste.jsf?num=C-203/15

[30] Sweden, Stockholm Administrative Court of Appeal (*Kammarrätten i Stockholm*) Decision (*Beslut*) Case 7380-14, available at: www.pts.se/upload/Domar/2016/KR-beslut-2016-12-22-i-mal-7380-14.pdf

[31] Sweden, Stockholm Administrative Court of Appeal *(Kammarrätten i Stockholm)* Judgement *(Dom)* Case 7380-14, available at: www.kammarrattenistockholm.domstol.se/Domstolar/kammarrattenistockholm/Domar/2017%20jan-juni/Dom_7380-14.pdf

[32] Sweden, sections 16a – e of the Act on electronic communication (*Lag [2003:389] om elektronisk kommunikation*), 1 May 2012, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2003389-om-elektronisk-kommunikation_sfs-2003-389 and sections 37 – 45 of the Ordinance on electronic communication (*Förordning [2003:396] om elektronisk kommunikation*), 1 May 2012, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2003396-om-elektronisk_sfs-2003-396

clarified that the Swedish legal provisions that require operators to retain data for law enforcement purposes cannot be applied. A consequence of the judgement is that operators no longer have an obligation to retain data for law enforcement purposes.[33]

Presently, the Swedish legal provisions on data retention for law enforcement purposes is under review. On 16 February 2017, the Government appointed a public inquiry, Data Retention and EU Law (*Datalagring och EU-rätten*) that will propose the necessary changes to the Swedish laws and regulations.[34] The aim is to adapt them to EU law as it is interpreted by the Court of Justice of the European Union in its preliminary ruling of 21 December 2016. The adaptation must ensure an appropriate balance between the protection of individual integrity and privacy on the one hand, and the need for information in order to prevent, detect, investigate and prosecute crimes on the other.[35] The Swedish Post and Telecom Authority (*Post- och telestyrelsen, PTS*) states that it looks forward to contributing to the inquiry by suggesting balanced rules that meet both the needs of law enforcement and the individual's right to confidential communication and privacy.[36] The inquiry will report back to the Government on 9 October 2017.

1. **Reports and inquiries by oversight bodies**

The Swedish Police (*Polisen*), the Swedish Secret Service (*Säkerhetspolisen*) and the Swedish Customs (*Tullverket*) have the right to collect data on individuals under certain conditions.[37] However, all authorities must receive permission by a court before any covert collection of internet traffic data from single individuals (on suspicion of a specific crime) is initiated. According to the Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*) the application for such permission may be handled by any district courts (*tingsrätter*).[38] For

[33] Sweden, Swedish Post and Telecom Authority (*Post- och telestyrelsen; PTS*), Regulations on data retention not to be implemented (*Regler om datalagring ska inte tillämpas*), webpage, available at https://www.pts.se/sv/Nyheter/Internet/2017/Regler-om-datalagring-ska-inte-tillampas/

[34] Sweden, Ministry of Justice (*Justitiedepartementet*), Data Retention and EU Law, government directive 2017:16 (*Datalagring och EU-rätten, direktiv 2017:16*) available at: www.regeringen.se/rattsdokument/kommittedirektiv/2017/02/dir.-201716/

[35] Sweden, Ministry of Justice (*Justitiedepartementet*), Data Retention and EU Law, government directive 2017:16 (*Datalagring och EU-rätten, direktiv 2017:16*) available at: www.regeringen.se/rattsdokument/kommittedirektiv/2017/02/dir.-201716/

[36] Sweden, Swedish Post and Telecom Authority (*Post- och telestyrelsen; PTS*), Regulations on data retention not to be implemented (*Regler om datalagring ska inte tillämpas*), webpage, available at https://www.pts.se/sv/Nyheter/Internet/2017/Regler-om-datalagring-ska-inte-tillampas/

[37] Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*) 16 May 2012, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[38] Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*) 16 May 2012, available at:

expediency the Stockholm District Court (*Tingsrätten i Stockholm*) is assigned to handles the majority of these permission cases. The courts' decisions as well as the actual data collection are monitored by the Swedish Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden, SIN*).[39] The Commission supervises the use by crime-fighting agencies of secret surveillance and qualified assumed identities and associated activities. The Commission also supervises the processing of personal data by the Swedish Police, some parts of the Swedish Economic Crime Authority and the Swedish Security Service. The supervision aims in particular at ensuring that the activities are conducted in accordance with laws and other regulations. The Commission exercises its supervision through inspections and other investigations. The Commission may make statements on established circumstances and express its opinion on the need for changes in the activities and shall strive to ensure that any deficiencies in laws and other regulations are remedied.[40] During 2016, the Commission monitored the Gothenburg Police's execution of covertly collected mobile data during the investigation of a suspected case of money laundering. This was done even though the offense in question the offense is not punishable by imprisonment for over two years, which is required.

The Swedish Data Protection Authority (*Datainspektionen*) carried out a new review of the personal data processing at the National Defence Radio Establishment (*Försvarets radioanstalt*) during 2016. The result of the review was presented on 24 October 2016.[41] Besides the overall review the report also considered a principally important case brought to attention by the Swedish Foreign Intelligence Inspectorate (*Statens inspektion av försvars-underrättelseverksamhet, SIUN*) in 2015.[42] If the Inspectorate finds that a defence intelligence agency is not acting in line with the laws, it can lead to a notification of the case to Chancellor of Justice (*Justitiekanslern, JK*), the Prosecutor General (*Riksåklagaren*) or as in this case to the

www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[39] Sweden, Swedish Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden, SIN*), official webpage: www.sakint.se/InEnglish.htm

[40] Sweden, Ordinance with instruction for the Swedish Commission on Security and Integrity Protection (*Förordning [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden*), 22 November 2007, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20071141-med-instruktion-for_sfs-2007-1141

[41] Sweden, Data Protection Authority (*Datainspektionen*), Review of the processing of personal data in the National Defence Radio Establishment's defence intelligence and development activities (*Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), reference number 2331-2015, available at www.datainspektionen.se/Documents/beslut/2016-10-24-fra.pdf

[42] Sweden, Swedish Foreign Intelligence Inspectorate (*Statens inspektion av försvarsunderrättelseverksamhet*), Summary of Swedish Foreign Intelligence Inspectorates inspections of the National Defence Radio Establishment (*Sammanställning över SIUNs inspektioner av FRA)* and Swedish Foreign Intelligence Inspectorates Annual report 2015 (*Årsrapport 2015*) available at www.fra.se/download/18.7fa21d9714ce119787c8000168/Siuns-inspektioner_Sammanstallning.pdf http://www.siun.se/dokument/Arsredovisning_2015.pdf

Data Protection Agency.[43] The review was initiated by the Data Protection Authority after a number of questions about the personal data processing operations had been posed in writing to National Defence Radio Establishment (*Försvarets radioanstalt*).

In the report Review of the processing of personal data in the defence surveillance and development activities of the Defence Radio Establishment (*Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*),[44] the Data Protection Agency stated that the National Defence Radio Establishment's ways to process personal data violates of section 2, Chapter 3 of the Act on processing of personal data in the National Defence Radio Establishment (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*)[45] by neglecting to conduct regular follow-up logs on its defence intelligence activities.[46] So far there have been no consequences of the National Defence Radio Establishment's violations of the Act in question – besides the note/criticism from the Data Protection Agency itself and similar reviews by the Swedish Foreign Intelligence Inspectorate. According to the National Defence Radio Establishment, the Swedish Foreign Intelligence Inspectorate has conducted more than 80 audit cases of the Radio Establishment since 2008. Only 14 of them led to any form of note/criticism from the Inspectorate. If the Inspectorate finds a serious fault, it has the mandate to order the

[43] Swedish Foreign Intelligence Inspectorate (*Statens inspektion av försvars-underrättelseverksamhet [SIUN]),* webpage The result of an audit *(Resultatet av en granskning),* available at: www.siun.se/resultat_granskning.html

[44] Sweden, Data Protection Authority (*Datainspektionen*)*,* Review of the processing of personal data in the National Defence Radio Establishment's defence intelligence and development activities (*Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*)*,* reference number 2331-2015, available at: www.datainspektionen.se/Documents/beslut/2016-10-24-fra.pdf

[45] Sweden, Act on processing of personal data in the National Defence Radio Establishment's defence intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), 10 May 2007, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007259-om-behandling-av-personuppgifter-i_sfs-2007-259 According to chapter 3 section 2 of the Act, the National Defence Radio Establishment must take appropriate technical and organizational measures to protect the personal data processed. A part of this responsibility includes logging and log monitoring to ensure that the measures to protect personal privacy is properly applied. The Data Protection Agency points out that a log is a basic security requirement to ensure traceability, for example, to detect unauthorized access to personal data or unauthorized searches. The logs must also be monitored regularly and its users should be informed that logging and log monitoring as a preventive measure.

[46] Sweden, Data Protection Authority (*Datainspektionen*)*,* Review of the processing of personal data in the National Defence Radio Establishment's defence intelligence and development activities (*Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*)*,* reference number 2331-2015, available at: www.datainspektionen.se/Documents/beslut/2016-10-24-fra.pdf

Radio Establishment to terminate the data collection or submit the case to a prosecutor. However, this has never been done.[47]

According to section 43 of the of the Personal Records Act (*Personuppgiftslag [1998:204]*),[48] the Data Protection Agency has the right to: 1) access the personal data processed in the organisation in question; 2) to receive information and documentation of the processing of personal data and security of processing; and 3) access the organisation's premises where the processing of personal data in carried out. After the Agency's audits a protocol is written that the audited organisations may give their opinions on. Thereafter, a decision is taken by the Agency. Either the Data Protection Agency decides to close the case without any comment or the audited organisation is required to correct the deficiencies pointed out by the Agency. If the Data Protection Agency finds more serious deficiencies, it may force the organisation in question to pay a fine. In these cases, the organisation is given a certain amount of time to correct the deficiencies. If this is not done the organisation is liable to pay the fine.[49]

The Data Protection Agency required that the National Defence Radio Establishment establishes a central log analysis function of the kind set out in the report. Furthermore, the Data Protection Agency ordered the National Defence Radio Establishment to submit a written statement of the measures it has taken and intends to take concerning the required central log analysis tool by 1 May 2017. The specific case in the Agency's report[50] that was brought up by the Swedish Foreign Intelligence Inspectorate (*Statens inspektion av försvarsunderrättelseverksamhet, SIUN*) concerned the National Defence Radio Establishment's interpretation and application of Chapter 1, section 13 of the Act on processing of personal data in the National Defence Radio Establishment's Defence intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*).[51] The section in question states that the processing of information

---

[47] Sweden, the National Defence Radio Establishment (*Försvarets radioanstalt*), webpage: Article in the Dagens Nyheter about the Swedish Foreign Intelligence Inspectorate's review of the National Defence Radio Establishment (*Artikel I DN om SIUN-granskning av FRA*), available at: www.fra.se/snabblankar/nyheterochpress/nyhetsarkiv/nyheter/artikelidnomsiungranskningavfra.287.html

[48] Sweden, Personal Records Act (*Personuppgiftslag [1998:204]*), section 43, 29 April 1998, available at http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204

[49] Sweden, Personal Records Act (*Personuppgiftslag [1998:204]*), section 45, 29 April 1998, available at http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204

[50] Sweden, Data Protection Authority (*Datainspektionen*), Review of the processing of personal data in the National Defence Radio Establishment's defence intelligence and development activities (*Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), reference number 2331-2015, available at: www.datainspektionen.se/Documents/beslut/2016-10-24-fra.pdf

[51] Sweden, Act on the National Defence Radio Establishment's Defence intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), chapter 1, section 13, 10 May 2007, available at:

containing personal data is allowed in the stage when it cannot be determined if the information contains personal data or not. [52] However, if the Radio Establisment is only allowed to process personal data when it does not know what the data in question contains personal data, the data collection cannot be used to search for suspicious personal data. As mentioned above, the Swedish Foreign Intelligence Inspectorate (*Statens inspektion av försvarsunderrättelseverksamhet*) referred this specific task to the Data Protection Agency in order for the Agency to review whether the National Defence Radio Establishment's interpretation of the section is in line with the meaning of the law. The National Defence Radio Establishment's interpretation expands the provision to not only refers to the stage when it cannot yet be determined if the information contains personal data, but also to the stage when the National Defence Radio Establishment does not yet know what kind of personal data the information includes. The Data Protection Agency considered that the provision cannot be interpreted as the National Defence Radio Establishment has done, which is a concern since the Radio Establishment's adherence to the legal provisions is of paramount importance if it shall be held responsible for its actions. However, the Agency stated that the current wording of the provision in practice is incompatible with data collection through signals intelligence in the way that it appears to have been assumed when the Data Collection Act" (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*) was introduced'.[53]

According to the Data Protection Agency, it can be assumed that virtually all information collected through signals intelligence contains personal data, which makes a literal interpretation of "when it has not yet been determined whether the information contains personal information" (*det skede av behandlingen då det ännu inte kunnat fastställas om informationen innehåller personuppgifter*) implies that the provision in chapter 1, paragraph 13 in the Act in question could never be applied correctly in practice.[54] It is therefore clear that the provision is not adapted to the needs and conditions that apply to the National Defence Radio

---

www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007259-om-behandling-av-personuppgifter-i_sfs-2007-259

[52] Sweden, Act on the National Defence Radio Establishment's Defence intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), chapter 1, section 13, 10 May 2007, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007259-om-behandling-av-personuppgifter-i_sfs-2007-259

[53] Sweden, Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), 16 May 2012, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[54] Sweden, Data Protection Authority *(Datainspektionen),* Review of the processing of personal data in the National Defence Radio Establishment's defence intelligence and development activities *(Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet),* reference number 2331-2015, p. 18, available at: www.datainspektionen.se/Documents/beslut/2016-10-24-fra.pdf

Establishment's activities today. The Data Protection Agency concluded that it is not possible to apply Chapter 1, paragraph 13 of the Act on processing of personal data in the National Defence Radio Establishment's defence intelligence and development activities in line with the Data Collection Act. The Agency noted that the wording of the current provision does not exclude the application of Chapter 1, section 6 and sections 8-12[55] in cases where it is known that the collected information contains personal data. The Data Protection Agency underlines that the question on how section 13 should be interpreted should have been addressed when the Data Collection Act was introduced. However, this was never done. Accordingly, the provision needs to be reviewed and adapted to the new mandate that the legislature has given the National Defence Radio Agency through the Data Collection Act. Against this background, the Data Protection Agency found it necessary to alert the Swedish government (Ministry of Defence [*Försvarsdepartementet*]) of this need. Until the Ministry has addressed the interpretation problem, the National Defence Radio Establishment will carry out its work using its current interpretation of section 13, since the Data Protection Agency's review[56] confirmed that it is not possible for the Radio Establishment to apply Chapter 1, section 13 of the Act on the National Defence Radio Establishment's Defence intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*)*[57]* when conducting signal intelligence in accordance with the Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*).*[58]*

---

[55] Sweden, Act on the National Defence Radio Establishment's Defence intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), chapter 1, section 6 and sections 8-12, 10 May 2007, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007259-om-behandling-av-personuppgifter-i_sfs-2007-259 The sections in question concern the basic requirements for the processing of personal data (section 6), when the processing of personal data is permitted in defence Intelligence (section 8) and in development activities (section 9), processing of sensitive personal data (section 11) and processing of personal register numbers (*personnummer*), (section 12),

[56] Sweden, Data Protection Authority (*Datainspektionen*), Review of the processing of personal data in the National Defence Radio Establishment's defence intelligence and development activities (*Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), reference number 2331-2015, p. 18, available at: www.datainspektionen.se/Documents/beslut/2016-10-24-fra.pdf

[57] Sweden, Act on the National Defence Radio Establishment's Defence intelligence and development activities (*Lag [2007:259] om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*), chapter 1, section 13, 10 May 2007, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007259-om-behandling-av-personuppgifter-i_sfs-2007-259

[58] Sweden, Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), 16 May 2012, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

The Swedish Commission on Security and Integrity Protection *(Säkerhets- och integritetsskyddsnämnden, SIN)* presented its Annual Report for 2016 in February/March 2017.[59] According to the report, the Commission's oversight of secret surveillance activities had found a number of problems, e.g. a prosecutor's decision not to inform a person of secret coercive measures, the late destruction of records of secret coercive measures, documentation issues and decisions concerning data collection in accordance with the Act on the collection of data on electronic communication in the law enforcement intelligence (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*).[60]

All problems lifted and criticism raised in the annual report had already been presented as so-called Statements with Decision (*Uttalande med beslut*) throughout 2016. These statements are published on the Commission's website and also referred to the relevant authorities. Most of the statements conclude with the Commission's decision to close the case in question after the presentation of them. For example, in one case the Commission stated that the Security Service (*Säkerhetspolisen, SÄPO*) had entered incomplete classifications of crimes (*brottsrubricering*) in its records over its decisions on data collection. Furthermore, the Security Service has incorrectly registered that the data collection decisions in question have been made in accordance with section 2 of the Data Collection Act (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*) when this was not the case. However, the Commission decided to close the case after its presentation.[61]

Another example is a case[62] that was closed after its presentation concerned the Police's incorrect processing of data in a number of cases The Commission stated that the Police's

---

[59] Sweden, Swedish Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden, SIN*), Annual Report, (*Årsredovisning*), available at: www.sakint.se/SIN-aarsredovisning-2016-Beslutad.pdf The report was signed by the chair and board members on 16 February 2017 and published on the Commission's website in the beginning of March 2017.

[60] Act on the collection of data on electronic communication in the law enforcement intelligence (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), 16 May 2012, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[61] Sweden, Swedish Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden, SIN*), Statement with decision: Collection of data on electronic communications by the Secret Service, ref. 208:2016 (*Uttalande med beslut*: *Inhämtning av uppgifter om elektronisk kommunikation vid Säkerhetspolisen, Dnr 208-2016*), 29 March 2017, available at: www.sakint.se/Uttalande-med-beslut-IHL-saepo-dnr-208-2016.pdf

[62] Sweden, Swedish Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden, SIN*), Statement with decision: Collection of data on electronic communications by the Police Authority, ref. 80-2016, Region South (*Uttalande med beslut*: *Inhämtning av uppgifter om elektronisk kommunikation vid Polismyndigheten, region Syd, Dnr 80-2016*), 15 December 2016, available at: www.sakint.se/Uttalande-med-beslut-dnr-80-2016-IHL-PM-region-Syd.pdf

incorrect processing of data collection cases was questionable and the nonchalance of the decision-maker had been staggering. Even so, the Commission's decision was to close the case.

However, sometimes a case may be referred to the Prosecutor's Office. One of these cases[63] concerned the Police Authority that for some time had conducted secret surveillance of mobile phone numbers without the required permits to do so. Once, the Police continued its secret surveillance of the texts sent and received to the numbers in question for 34 hours after the surveillance permit had expired. Another time, secret surveillance went on for more than 9 hours without any permit. The Commission states that these errors by the Police may constitute criminal offences. Consequently, the Commission decided to bring its information to the attention of the public prosecutor in accordance with section 20 of the Ordinance with instructions for the Commission on Security and Integrity Protection (*Förordning [2007:1141]) med instruktion för Säkerhets- och integritetsskyddsnämnden*).[64] The Commission concluded the statement with pointing out that it looked forward to the prosecutor's decision in the preliminary investigation question.

During 2016, the Commission initiated 38 cases. This means that the commission independently decides on a number of organisations or cases that it want to look at closer, without any prior report or complaint. Three of the cases concerned the Security Service's processing of personal data, six that concerns the Police's processing of personal data and 29 cases concerning the use of secret surveillance.[65] The Commission was also informed of 1,188 decisions on collection of data on electronic communication that have been approved by a district court. The majority of the 1,188 cases have been approved by the Stockholm District Court (*Tingsrätten i Stockholm*), which is assigned to handles the majority of such cases. The decisions to collect data was requested by the Swedish Police (*Polisen*), the Security Service (*Säkerhetspolisen, SÄPO*) and the Customs Service (*Tullverket*).[66]

---

[63] Sweden, Swedish Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden, SIN*), Statement with decision: Implemetation of secret surveillance of electronic communications (*Uttalande med beslut: Inhämtning av uppgifter om elektronisk kommunikation*), 14 September 2016, available at: www.sakint.se/dokument/rapporter-och-uttalanden/Dnr-144-2016-Uttalande-om-verkstaellighet-av-hemlig-oevervakning-av-elektronisk-kommunikation-vid-Polismyndigheten.pdf

[64] Sweden, Ordinance with instructions for the Commission on Security and Integrity Protection (*Förordning [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden*), 22 November 2007, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20071141-med-instruktion-for_sfs-2007-1141

[65] Sweden, Act on the collection of data on electronic communication in the law enforcement intelligence (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), 16 May 2012, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[66] Sweden, Act on the collection of data on electronic communication in the law enforcement intelligence (*Lag [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), 16 May 2012, available at:

After checking all the other relevant oversight bodies we conclude that no specific or ad hoc parliamentary or non-parliamentary commission have issued any new work during the period in question.

2. **Work of specific ad hoc parliamentary or non-parliamentary Commissions**

The Government's yearly report/communication (*skrivelse*) to the Parliament on the results of the monitoring and review of signals intelligence in defence intelligence activities that were carried out in 2015 was presented to Parliament on 8 December 2016. The yearly reporting is requested by parliament in connection with the processing of the Act on signals intelligence in the defence intelligence (*Lag [2008:717] om signalspaning i försvarsunderrättelseverksamhet*).[67] The report is quite bland but is nevertheless a report related to the theme of surveillance. The communication is titled Government Communication: privacy in signals intelligence in defence intelligence (*Regeringens skrivelse: integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet, Skr 2016/17:70*).[68]

The annual reports of the Military Intelligence and Security Service (*Militära underrättelse- och säkerhetstjänsten, MUST*) and the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) as well as the Full Year Assessment of the National Centre for Terror Threat Assessment (*Nationellt centrum för terrorhotbedömning, NCT*)[69] and the Military Intelligence and Security Service (*Militära underrättelse- och säkerhetstjänsten, MUST*) were presented during February 2017. MUST's annual review was presented on 21 February 2017. The review is a public report, which presents organisation's mission and organisation, its supervising bodies, defines the concepts of military defence intelligence service and security service, and describes the organisation's tasks e.g. following the development in the region, participating in international interventions, collecting and processing (mainly IT-related) security disturbances at Swedish authorities. According to the director, Mr. Gunnar Karlson, much of MUST's work

---

https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

[67] Sweden, Act on signals intelligence in the defence intelligence (*Lag [2008:717] om signalspaning i försvarsunderrättelseverksamhet*), 10 July 2008, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717

[68] Sweden, Government Communication: privacy in signals intelligence in defence intelligence (*Regeringens skrivelse: integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet, Skr 2016/17:70*), available at: www.regeringen.se/4af295/globalassets/regeringen/dokument/forsvarsdepartementet/skrivelser/2016_17_70_integritetsskydd-vid-signalspaning-i-forsvarsunderrattelseverksamhet

[69] Sweden, National Centre for Terror Threat Assessment (*Nationellt centrum för terrorhotbedömning, NCT*), available at: http://sakerhetspolisen.se/download/18.1beef5fc14cb83963e73383/1484663040490/NCT_Helarsbedomning_2017.pdf

during 2016 focused on actions against different kinds of influence operations against Swedish interests (*påverkansoperationer*) and on operations against cyber threats and risks.[70]

The National centre for terror threat assessments (*Nationellt centrum för terrorhotsbedömning, NCT*), presented its so-called full year assessment of the terrorist threat against Sweden on 18 February 2017.[71] This is a forward-looking public document assessing the threat level for 2017. According to the assessment, Sweden remains on the overall terror threat level 3. A 3 includes the possibility of a terrorist attack, even though it is not likely that Sweden is a priority for large and coordinated terrorist attacks. According to the NCT's assessment, the greatest terrorist threat to Sweden is constituted by Islamist motivated terrorism. The assessment indicates that there are a few players who probably has both the intent and ability to carry out a terror attack in Sweden. Among these are both returnees from armed conflicts for so-called violence-promoting Islamist groups and other persons, who have not participated in the conflicts themselves, but are nevertheless inspired by violence-promoting Islamist propaganda.[72] Furthermore, the National centre assesses the terror threat level for terror attacks by domestic extremist groups, both autonomous leftist groups and the White Power movement include individuals who advocate for violence and armed struggle. However, during 2016 both groups did rarely commit any acts of violence that could be classified as terrorist attacks.[73] The terror threat level is assessed continuously by the National centre for terror threat assessments, and may be changed during the year if necessary.[74]

---

[70] Sweden, Military Intelligence and Security Service (*Militära underrättelse- och säkerhetstjänsten, MUST*), Annual Review 2016, Military intelligence and security service (*Årsöversikt 2016, Militära underrättelse- och säkerhetstjänsten*), *available at* www.forsvarsmakten.se/siteassets/3-organisation-forband/hogkvarteret/must/must-arsoversikt-2016.pdf

[71] Sweden, National centre for terror threat assessments (*Nationellt centrum för terrorhotsbedömning, NCT*), Full year evaluation: Assessment of the terrorist threat against Sweden in 2017 (*Helårsbedömning: Bedömning av terrorhotet mot Sverige 2017*), available at: www.forsvarsmakten.se/siteassets/3-organisation-forband/hogkvarteret/must/must-arsoversikt-2016.pdf

[72] Sweden, National centre for terror threat assessments (*Nationellt centrum för terrorhotsbedömning, NCT*), Full year evaluation: Assessment of the terrorist threat against Sweden in 2017 (*Helårsbedömning: Bedömning av terrorhotet mot Sverige 2017*), available at: www.forsvarsmakten.se/siteassets/3-organisation-forband/hogkvarteret/must/must-arsoversikt-2016.pdf

[73] Sweden, National centre for terror threat assessments (*Nationellt centrum för terrorhotsbedömning, NCT*), Full year evaluation: Assessment of the terrorist threat against Sweden in 2017 (*Helårsbedömning: Bedömning av terrorhotet mot Sverige 2017*), available at: www.forsvarsmakten.se/siteassets/3-organisation-forband/hogkvarteret/must/must-arsoversikt-2016.pdf

[74] Sweden, National centre for terror threat assessments (*Nationellt centrum för terrorhotsbedömning, NCT*), Full year evaluation: Assessment of the terrorist threat against Sweden in 2017 (*Helårsbedömning: Bedömning av terrorhotet mot Sverige 2017*), available at: www.forsvarsmakten.se/siteassets/3-organisation-forband/hogkvarteret/must/must-arsoversikt-2016.pdf

The Annual Report from the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) was presented on 17 February 2017.[75] The signal intelligence carried out by the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) is intended to provide information and forewarnings of the situation outside of Sweden. The signal intelligence may focus on: 1) the military capacity of foreign countries; 2) support for the Swedish military operations abroad; 3) the development and proliferation of weapons of mass destruction in other countries; 4) international terrorism; 5) cyber-attacks from abroad to access sensitive information in Sweden; and 5) human rights in countries under authoritarian rule. The Radio Establishment is tasked to provide signal intelligence to the Government, the Government Offices (*regeringskansliet*), the Armed Forces (*Försvarsmakten*), the Security Service (*Säkerhetspolisen, SÄPO*) and the National Operations Department of the Police Authority (*nationella operativa avdelningen, NOA på Polismyndigheten*)The aim of the intelligence is to find out any possible threats to Sweden, but also to provide support to implementation of the government's foreign policy, security policy and/or defence policy.[76] Signals intelligence concerns the collection of signals and data. The collected signals and data are then processed and analysed and will finally result in intelligence which is reported to the clients of the National Defence Radio Establishment. The collection of signals and data can take place e.g. in relation to different types of radio signals or different types of cables. The Radio Establishment's signals intelligence is divided into two main areas: communications intelligence *(kommunikationsspaning, KOS*) and technical signals intelligence (*teknisk signalspaning, TES*). The data and signal collection is conducted from various locations in Sweden as well as from the Air Force Gulfstream IV (S102B) and the Navy ship M/S Orion.[77] Communication intelligence focuses on signals such as telephony, telegraphy and different kinds of transfers of data. The signals and data may concern both military and civilian communication. The collected data is analysed and processed. A report is then sent to client in question. The National Defence Radio Establishment's data processing involves e.g. forced encryption or the compilation and presentation of data in different ways. The technical signals intelligence focuses on to signals from radar, navigation and weapons-related systems. The aim is to provide a basis for electronic warfare capabilities (*telekrigsfunktioner*) and information that can be used to develop protection and countermeasures for the Swedish Armed Forces' vessels and aircrafts. The technical signals intelligence also makes it possible to monitor foreign military ships and aircraft in the vicinity.[78]

---

[75] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[76] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), official webpage Activities (*Verksamhet*), available at: www.fra.se/verksamhet.4.html

[77] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), official webpage, Signal intelligence activities (*Signalunderrättelseverksamhet*), available at: www.fra.se/verksamhet/signalunderrattelseverksamhet.68.html

[78] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), official webpage Signal intelligence activities (*Signalunderrättelseverksamhet*), available at: www.fra.se/verksamhet/signalunderrattelseverksamhet.68.html

The Armed Forces (*Försvarsmakten*) is one of the most important clients of the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*). The Radio Establishment carries out both communications intelligence and technical signals intelligence for the Armed Forces, which includes technical support, intelligence reporting and training. The assignments from the Armed Forces is mainly focused on the following areas: 1) intelligence on the military capabilities of other countries; 2) intelligence support in connection to international operations; 3) production of signals to the so-called signal reference library (*Signalreferensbiblioteket, SRB)*; 4) support to the Armed Forces air and surface intelligence; and 5) training and technical support.[79] The Signal Reference Library is a database that contains a description of various types of radar signals. The National Defence Radio Establishment is responsible for providing the signal reference library with information on these signals. The Armed Forces use the reference library as a basis to decide how to equip the radar detectors on its aircraft and ships. With the help of Signal Reference Library, the radar detectors of the Armed Forces are able to describe and identify signals from foreign targets and assist in the protection of Swedish ships and aircraft.[80]

An increasingly important task for the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) is to provide support to the Armed Forces in its international operations. The support may involve intelligence, equipment and various types of special competences needed before, during and after an operation. During some operations, the National Defence Radio Establishment has carried out signal intelligence operations together with the Armed Forces over the Adriatic Sea and outside of Libya from airplanes of type S102B (Gulfstream IV).[81] The National Defence Radio Establishment's unit for development monitors changes and technological developments linked to its intelligence areas as well as the development of signal protection. The Radio Establishment continuously develops its methods for reconnaissance and processing to meet its clients' need to manage changing threats and the security situation's demand on its intelligence services. The National Defence Radio Establishment performs mathematical assessments of cryptographic systems on behalf of the total defence services (*Totalförsvaret*). The Radio Establishment is also responsible for a pool of cryptologists (*kryptologpool*) which constitutes a national competence centre for cryptology. Furthermore, the Establishment supports the Ministry of Foreign Affairs (*Utrikesdepartementet*) and the Police Authority (*Polismyndigheten*) in cryptography issues. The National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) also carries out mathematical analyses of cryptosystems, which

[79] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), official webpage Support to the Armed Forces (*Signalunderrättelseverksamhet*), available at: www.fra.se/verksamhet/signalunderrattelseverksamhet/stodtillforsvarsmakten.72.html

[80] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), official webpage Support to the Armed Forces (*Signalunderrättelseverksamhet*), available at: www.fra.se/verksamhet/signalunderrattelseverksamhet/stodtillforsvarsmakten.72.html

[81] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), official webpage Support to the Armed Forces (*Signalunderrättelseverksamhet*), available at: www.fra.se/verksamhet/signalunderrattelseverksamhet/stodtillforsvarsmakten.72.html

are used or are intended to be used within the total defence services. The aim of the analyses is to check that the systems in question provide adequate protection.[82]

The Annual Report of the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*)[83] goes into more detail than MUST's Annual Review, mentioned above, even though both reports are publicly available documents. According to the report, a large part of the Radio Establishment's signal intelligence is focused on monitoring the military capabilities in Sweden's immediate surroundings. This includes everything from troop movements and investments in new weapons systems to the more long-term security intentions of foreign powers. During 2016, the Radio Establishment reported on an increased tactical military presence around the Baltic Sea. As a result of the increased level of military activity in the immediate area, the National Defence Radio Establishment had added aircraft and ship-borne signal intelligence in order to remain a high standard in their input into the signal reference library (*signalreferensbiblioteket, SRB*). The National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) had also followed developments in wars and conflicts e.g. in the Middle East, which according to the report has contributed to a better knowledge level on key players' intentions and actions.[84]

The Security Service (*Säkerhetspolisen, SÄPO*) is the main client of the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) in relation to international terrorism. The tasks the National Defence Radio Establishment carries out for the Security Services includes the monitoring of international terrorist networks, their financing, organization, access to weapons etc. and the identification of potential links between these networks and Sweden. The National Defence Radio Establishment also provides general intelligence support for the Security Service. According to the report, the provision of intelligence to the Security Service remained at a consistently higher level in 2016 than before.[85] As a result the Radio Establishment had to reprioritise within its budget.[86] The overall budget of the National Defence Radio Establishment for 2017 and 2018 remain on the same level as in 2016.[87] The only changes made are to adjust

---

[82]Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), official webpage Signal intelligence development and cryptology services (*Signalutveckling och kryptologiska tjänster*), available at: www.fra.se/verksamhet/signalunderrattelseverksamhet/signalutvecklingochkrypto.80.html

[83] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[84] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[85] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[86] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[87] Sweden, Ministry of Finance (*Finansdepartementet)*, Government Budget Bill 2017, Expenditure area 6: Defence and Emergency Preparedness (*Budgetpropositionen för 2017,* Prop. 2016/17:1 *Utgiftområde 6: försvar och samhällets krisberedskap*), available at:

for the rise in prices and wages. Since the budget for 2017 remained on the same level as 2016 it appears likely that the provision of intelligence must remain on the same overall level but that the Radio Establishment must redirect or reprioritise within this budget.

Alongside these more traditional threats, the Annual report lifted the occurrence of other threats that are harder to define. During 2016 the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) observed apparent attempts by foreign powers to influence the decision-making processes outside their borders, both internationally and against Sweden. Such operations are generally referred to as influence operations (*påverkansoperationer*). According to the report, many countries carry out intelligence activities directed against Sweden and Swedish interests. The most common form of such intelligence today is advanced IT attacks. The National Defence Radio Establishment stated that Sweden is continuously and increasingly attacked through various forms of cyber-attacks. During 2016, the main goals for such attacks were research and development, defence, political bodies and institutions and government agencies with important public missions.[88] According to the National Defence Radio Establishment's report, the foreign intelligence services, which have an interest in Sweden are increasingly using cyber-attacks to obtain necessary information.[89] Skilled foreign intelligence services have access to boundless resources of staff and expertise.[90] Consequently, the Radio Establishment stated that these intelligence services are able to produce uniquely designed sophisticated methods for a cyber-attack, which are not always possible to detect by a commercially developed protection system. They may find vulnerabilities in a certain protection system and develop customized malware that allows them to enter the system in focus.[91] However, the National Defence Radio Establishment's Annual report established that the protection and security of many IT systems are so poor that an attacker may easily use known vulnerabilities and attack tools instead of more advanced methods. The conclusion of the Radio Establishment is that if a skilled attacker has decided to access a certain IT system it will almost always succeed. It is only a matter of time. According to the signal intelligence carried out by the

---

www.regeringen.se/4a6969/contentassets/e926a751d9eb4c978c4d892c659ebc8e/utgiftsomrade-6-forsvar-och-samhallets-krisberedskap According to the budget bill, the 2016 budget for the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*) was 924,926,000 SEK (96,543,700 Euro), the 2017 budget is 979,691,000 SEK (102,260,000 Euro), the 2018 budget is estimated to 1,051,750,000 SEK (109,782,000 Euro),

[88] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[89] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[90] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[91] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

National Defence Radio Establishment, shows that cyber-attacks against the Swedish government and Swedish businesses are continuous and on-going.[92] Consequently, organisations which handle information of interest for foreign countries' intelligence services must presuppose that they are vulnerable for cyber-attacks. Providers of IT services to such organisations are also interesting targets for cyber-attacks, since they may provide an easier way for a foreign signal intelligence service to reach its goal.[93]

According the National Defence Radio Establishment's Annual Report the following information may be of interest for a foreign state's intelligence service: 1) Sweden's defence ability and defence planning (*försvarsförmåga och försvarsplanering*); 2) Swedish security policy intentions (*svenska säkerhetspolitiska avsikter*); 3) State secrets (*statshemligheter*); 4) Industry secrets (*industrihemligheter*); and 5) Research results (*forskningsresultat*).[94]

On 23 February 2017, the Parliamentary Commission of Defence (*Försvarsutskottet*) presented its concluding report[95] concerning the Government's yearly report/communication (*skrivelse*) presented to Parliament in December 2015.[96] The Commission's report treated six areas: 1) the protection of personal integrity in relation to signals intelligence in defence intelligence; 2) the Swedish Foreign Intelligence Inspectorate (*Statens inspektion av försvarsunderrättelseverksamhet, SIUN*); 3) Signal intelligency and weapons of mass destruction; 4) the Armed Forces' reconaissance aviation; 5) Land purchase as security threats; and 7) the State's ability to protect the interests of the total defence services.[97]

---

[92] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[93] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[94] Sweden, National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), Annual Report 2016 (*Annual Report 2016*), available at: www.fra.se/download/18.4380e2fb15a3d2f3f3e4f/1488204590345/FRA-arsrapport-2016.pdf

[95] Sweden, Parliamentary Commission of Defence (*Försvarsutskottet*), Privacy in signals intelligence in defence intelligence, Commission report 2016/17:FöU5 (*Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet, Försvarsutskottets betänkande 2016/17:FöU5*), available at: https://data.riksdagen.se/fil/C552423E-8AF8-414D-B855-A8C2545CF252

[96] Sweden, Government Communication: Protection of integrity in relation to signals intelligence in defence intelligence" (*Regeringens skrivelse: integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet, Skr 2015/16:70*), available at: https://data.riksdagen.se/fil/9DAC5F77-C1E5-463E-B168-E2D116006E50 The Government is required by parliament to present an annual report on signal intelligence. The 2016 Government Communication concerning the same area, (*Regeringens skrivelse: integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet, Skr 2016/:70*) was presented to parliament on 8 December 2016 and is available at: https://data.riksdagen.se/fil/85636C7B-57D5-4BBA-89A5-5E90C0CA8BE4

[97] The total defence services (*totalförsvaret*) includes both the Armed Forces (*försvarsmakten*) and civilian services connected to the defence of the country.

According to the report, the Parliamentary Commission of Defence (*Försvarsutskottet*) understood signal intelligence as an important tool in the implementation of defence intelligence. Simultaneously, the commission attached great importance to a system that protects personal integrity in relation to signal intelligence in accordance to Swedish laws and regulations. The Commission noted that besides the 31 audits carried out by the Swedish Foreign Intelligence Inspectorate (*Statens inspektion för försvars-underrättelseverksamheten, SIUN*), and included in SIUN's Annual Report for 2015, the Inspectorate had carried out two additional audits that will be included in the annual report for 2016. The Commission had been informed that the Swedish Foreign Intelligence Inspectorate have submitted comments to the National Defence Radio Establishment in relation to both audits. The Commission assumed that the government will present its conclusions on the comments made by SIUN and that the government in its appointments of members to the Radio Establishment's internal Council for the Protection of Personal Integrity (*Integritetsskyddsrådet*)[98] whose task is to ensure the protection of privacy in the electronic reconnaissance carefully considering how the Council's possibilities to contribute to the protection of personal integrity can be further enhanced. However, at the moment the Commission finds no reason to follow the suggestions of member bill (*motion*) 2016/17: 3570 by Mr. Stig Henriksson et al. of the Left Party (*Vänsterpartiet, V*), which was consequently rejected. The member bill suggested that the government should come back to Parliament with proposals on measures to ensure that the control functions and information to Parliament really work as they should.

The Board of the Swedish Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten, SIUN*) consists of seven board members, including two judges or former judges. In accordance with its previous positions on this issue (the reports 2014/15: FöU5, and 2015/16: FöU5), the Parliamentary Commission of Defence (*Försvarsutskottet*) noted that the composition of the Board meets the statutory regulations and that the government has appointed members from the nominations of the party groups. These represent both the government and the opposition parties. The Commission saw no reason to further regulate the composition and constitution of the board. Consequently, it rejected member bills 2016/17:3575 and 2016/17:2899 both by Mr. Mikael Jansson et al. of the Sweden Democrats (*Sverigedemokraterna, SD*). The member bills suggested that the number of members of the Swedish Foreign Intelligence Inspectorate should be extended so that all parties represented in parliament (including their own) may have at least one member.

The Parliamentary Commission of Defence (*Försvarsutskottet*) attached great importance to an efficient inter-agency cooperation both in the defence intelligence as a whole, and in the efforts to prevent the proliferation of weapons of mass destruction. The focus of the signal intelligence in defence intelligence may currently only be specified by the Government, the Government

---

[98] According to section 11 of the Act on Signal intelligence in the Defence Intelligence (*Lag [2008:717] om signalspaning i försvarsunderrättelseverksamheten*), 1 December 2009, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717 the National Defence Radio Establisment (*Försvarets radioanstalt, FRA*) must have a Council for the Protection of Personal Integrity (*Integritetsskyddsrådet*). The task of the Council is to ensure the protection of personal integrity in the electronic intelligence services.

Offices (*Regeringskansliet*), the Armed Forces (*Försvarsmakten*), the Security Service (*Säkerhetspolisen, SÄPO*) and the National Operations Department of the Police Authority (*Nationella operativa avdelningen, NOA vid Polismyndigheten*). Non-proliferation issues are today conducted through a coordinating council, which is linked to the Inspectorate of Strategic Products (*Inspektionen för strategiska produkter, ISP*).[99] The co-operating agencies that provide support to the ISP are the Research Institute of the Total Defence Services (*Totalförsvarets forskningsinstitut, FOI*), the National Defence Radio Establishment, (*Försvarets radioanstalt, FRA*), the Secret Service *(Säkerhetspolisen, SÄPO*) and the Military Intelligence and Security Service (*Militärens underrättelse- och säkerhetstjänst, MUST*). The Commission points out that the cooperation between the relevant authorities continued to evolve, according to the ISP, which is a positive development. Furthermore, the Commission notes that the decision to change the Act on signals intelligence so that the Security Service and the then National Police Authority should be allowed to use the signal intelligence of the defence intelligence was a long process with many considerations. Consequently, the Commission did not see any reason to include more authorities in the Act and rejected member bill 2016/17: 3584 by Mr. Hans Wallmark et al. of the Moderate Party (*Moderaterna, M*), the Liberal Party (*Liberalerna, L*) and the Christian Democrats (*Kristdemokraterna, KD*). The member bill suggested a review of the possibilities to allow the Inspectorate of Strategic Products (*Inspektionen för strategiska produkter, ISP*) to specify the signal intelligence carried out by the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*). The Commission also rejected member bill 2016/17: 2497 by Mikael Oscarsson et al. of the Christian Democrats (*Kristdemokraterna, KD*). The member bill suggested the initiation of a government inquiry (*statlig utredning*) tasked with analysing if any changes should be made in the structure of the Swedish intelligence services.

The Parliamentary Commission on Defence (*Försvarsutskottet*) shared the Government's view that it is necessary to continue the dialogue on arms control in a situation where the Russian military is developing its abilities and the country's military activities continue to challenge its neighbouring countries. The Commission noted with concern that the Organisation for Security and Co-operation in Europe (OSCE) has difficulties in finding ways forward in the politico-military (*militärpolitiska*) field. However, the Commission found the co-operation on observation flights (*observationsflygningar*) between the Armed Forces and other treaty states a positive development. The Armed Forces do not only conduct observation flights but also make its reconnaissance airplanes (*spaningsflygplan*) available to other treaty states. Under the current conditions in Sweden's neighbouring area, the Commission assumed that the government will continue to work actively in this field. Consequently, it found no reason to approve member bill 2016/17: 159 by Mr. Jonas Sjöstedt et al. of the Left Party (*Vänsterpartiet, V*). The member bill

[99] The Inspectorate of Strategic Products (*Inspektionen för strategiska produkter, ISP***)**, works with control and compliance of defence material and dual-use products. ISP is also the National Authority for the Chemical Weapons Convention and handle cases concerning targeted sanctions. ISP is also the National Authority for the Chemical Weapons Convention and handle cases concerning targeted sanctions.

suggested that the government should expand the possibilities to reconnaissance flights (*spaningsflygningar*) in the neighbouring area together with other countries.

The Parliamentary Commission on Defence (*Försvarsutskottet*) referred to a meeting with General Anders Thornberg of the Security Service (*Säkerhetspolisen, SÄPO*) on 7 June 2016. At the meeting the General informed the Commission about land purchases as a potential security threat. The Commission noted that measures are taken to counteract any instance of foreign intelligence which may constitute a security threat. Consequently, it saw no reason to require any additional measures as suggested by the member bill 2016/17: 3205 by Mr. Hans Wallmark et al. of the Moderate Party (*Moderaterna, M*). Consequently, the member bill, which suggested that a survey of certain land purchases with potential security interest should be conducted was rejected.

The government had expressed its intention to review the need for legislative changes to accommodate the protection of certain objects, which warrant special protection. According to the Commission, it is important that the issue is subjected to a broad and thorough investigation without any further delay. The aim of this investigation should be to find common solutions to various situations when different interests of the total defence services require special protection. The Commission required that the government urgently come back to parliament with a proposal for such solutions. Furthermore, the government should also come back to parliament with a report on how the government intends to handle the issues during the period before the government can present its proposal on permanent solutions to Parliament. With the support of section 16, chapter 9 of the Parliament Act (*Riksdagsordning [2014:801]*)[100] the Parliamentary Commission of Defence (*Försvarsutskottet*) proposes that Parliament endorses the Committee's report concerning the government's ability to protect the total defence services (*totalförsvarsintressen*) and notify the government of its decision. With the support of section 16, chapter 9 of the Parliament Act (*Riksdagsordning [2014:801]*)[101] the Parliamentary Commission of Defence (*Försvarsutskottet*) proposed that the Parliament endorses its report concerning the government's ability to protect the total defence services (*totalförsvarsintressen*) and notify the government of its decision.

The report was discussed in Parliament on 2 March 2017.[102] The discussion consisted of an oral argumentation of the contents of the Committee's report by members of Parliament from the Liberal Party (*Liberalerna, L*), the Moderate Party (*Moderaterna, M*), the Social Democratic Party (*Socialdemokraterna, S*), the Left Party (*Vänsterpartiet, V*), the Green Party (Miljöpartiet), the Centre Party (Centerpartiet) and the Sweden Democrats (*Sverigedemokraterna, SD*). The persons, who had submitted the member bills on defence issues that were rejected by the

[100] Sweden, Parliament Act (*Riksdagsordning [2014:801]*), 19 June 2014, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/riksdagsordning-2014801_sfs-2014-801

[101] Sweden, Parliament Act (*Riksdagsordning [2014:801]*), 19 June 2014, available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/riksdagsordning-2014801_sfs-2014-801

[102] Sweden, Swedish Parliament, Parliament's protocol (*Riksdagens protokoll 2016/17:77 Torsdagen den 2 mars*) https://data.riksdagen.se/fil/91231FC2-9F91-49F5-86E4-6A31E8F37C04

Parliamentary Commission of Defence argued that their motions should be supported by Parliament.[103] The Parliament decided to endorse the report on 15 March 2017.[104]

3. **Work of non-governmental organisations and academia**

The preliminary ruling of the Court of Justice of the European Union from 21 December 2016, mentioned above, launched a series of opinion articles, Tweets and blogs mainly written by persons from the legal profession. Four district prosecutors (*kammaråklagare*) expressed their strong concerns for the potential effects of the ruling of the Court of Justice and the following ruling of the Stockholm Court of Appeal *(*K*ammarrätten i Stockholm*) in an opinion article (*debattartikel*) in Svenska Dagbladet on 28 December 2016. According to the district prosecutors, paedophiles, robbers and murderers will go free if the prosecution can no longer access information about data traffic as it is used to. They argued that it is unreasonable that Swedish law enforcement is limited by EU law and demanded that the Swedish government should act.[105]

An opinion article published in the online journal Dagens juridik (appr. Contemporary Law) on 10 January 2017 by the Deputy Chief Prosecutor at the International Public Prosecution Office in Gothenburg stated that the European Court of Justice's ruling is very strange and unfortunately, pretty much based on emotional arguments without support either in earlier practice or conventions.[106] According to the author the preliminary ruling had removed an important tool for combating terrorism and serious crime. He argued that for the Police to able to access the data it needs, the data must be available in the first place – if they are erased, they are not. The article ended with a question: What should we, who think that crimes should be combated and punished and terrorism prevented, do? The author suggested to: 1) ignore the Court's ruling since it is badly motivated; 2) change the Data Collection Act a bit, so as to shorten the retention time; 3) work within the EU for a clarification of the EU Charter of Fundamental Rights; or 4) all three suggestions together.

---

[103] Sweden, Swedish Parliament, (*Riksdagen*), Parliament's protocol (*Riksdagens protokoll 2016/17:77 Torsdagen den 2 mars*), available at: https://data.riksdagen.se/fil/91231FC2-9F91-49F5-86E4-6A31E8F37C04

[104] Sweden, Swedish Parliament, (*Riksdagen*), Parliament's protocol (*Riksdagens protokoll 2016/17:80 Onsdagen den 15 mars*), available at: https://data.riksdagen.se/fil/6E8F86B7-CA7B-4FC1-8359-2DF050520506

[105] Bälter Nordenman, T., Asplund, J., Svanfeldt, J. and Larson, D. Data retention, a requirement for finding serious criminals (*Datalagring krav för att hitta grova brottslingar*) in *Svenska Dagbladet*, 28 December 2016, available at: www.svd.se/datalagring-kravs-for-att-hitta-grova-brottslingar/om/debatt

[106] Ahlstrand, T. The ruling on data storage is only opinions based on the Court's own point of view rather than an interpretation of the law *(Domen om datalagring är ett tyckande grundat i egna åsikter – inte en tolkning av gällande rätt)* in Dagens juridik, 10 January 2017, available at: www.dagensjuridik.se/2017/01/domen-om-datalagring-ar-ett-tyckande-grundat-i-egna-asikter-inte-en-tolkning-av-gallande-rat

In her blog[107] the secretary general of the Swedish Bar Association (*Svenska advokatsamfundet*) argued that the ruling of the Court of Justice underlined the lack of proportionality between the violation of personal integrity and law enforcement & security – also legitimate interests in their own right. The secretary general, Ms. Anne Ramberg, pointed out that the increasing influential technology leads to a shift of power from the parliament to the government and the legal practitioners. Consequently, the extent of the violation of personal integrity may easily increase without a change in the legislation. The secretary general welcomed that the Court of Justice once again had decided that EU law does not always allow invasion of privacy – even if the aim may be acceptable. According to her, the Court of Justice seemed to be the only cure for an increasingly audacious legislation.

The most influential opinion article was published on 14 February by the general directors (heads) of Sweden's five main law enforcement authorities – the Swedish Police Authority (*Polismyndigheten)*, the Swedish Economic Crimes Authority (*Ekobrottsmyndigheten*), the Swedish Customs (*Tullverket*), the Swedish Prosecution Authority (*Åklagarmyndigheten*) and the Swedish Security Service (*Säkerhetspolisen, SÄPO*).[108] In the article the five general directors expressed their strong concerns for the potential effects of the ruling of the Court of Justice and the upcoming ruling of the Stockholm administrative Court of Appeal (*Kammarrätten i Stockholm*). They emphasised that there is an urgent need to find a legally secure solution. They pointed out that the law enforcement authorities do not have free access to private telecommunications data – it is the telecommunications operators. The authorities in question may only demand access to them when there are suspicions of serious crimes or when there is danger to life and health. It is the court that decides if access should be granted and the Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden, SIN*) that reviews these decisions.[109] Furthermore, the authors underlined that "[m]ost people never get their telecommunication traffic controlled by an authority. Their data remains with the operators. It is only "[…] a tiny part of the Swedish population, one per mille, which gets its telecommunications data handed over to the authorities for control every year.[110] Furthermore, the general directors claimed that it has already gone so far so "[…] criminals seek out operators

[107] Ramberg, A. The legislature wrong – again! (*Lagstiftaren fel på det – igen!*), blog published on 8 January 2017, available at: https://annerambergs.wordpress.com/2017/01/08/lagstiftaren-fel-pa-det-igen/

[108] Eliasson, D., Håkansson, E. Mattson, T., Perklev, A. and Thornberg A. Data retension essential to prevent and investigate crime (*Datalagring avgörande för att hindra och utreda brott),* opinion article published in *Dagens Nyheter* (daily newspaper) 14 February 2017, available at: www.dn.se/debatt/datalagring-avgorande-for-att-hindra-och-utreda-brott/

[109] Eliasson, D., Håkansson, E. Mattson, T., Perklev, A. and Thornberg A. Data retension essential to prevent and investigate crime (*Datalagring avgörande för att hindra och utreda brott*), opinion article published in *Dagens Nyheter* (daily newspaper) 14 February 2017, available at: www.dn.se/debatt/datalagring-avgorande-for-att-hindra-och-utreda-brott/

[110] Eliasson, D., Håkansson, E. Mattson, T., Perklev, A. and Thornberg A. Data retension essential to prevent and investigate crime (*Datalagring avgörande för att hindra och utreda brott*), opinion article published in *Dagens Nyheter* (daily newspaper) 14 February 2017, available at: www.dn.se/debatt/datalagring-avgorande-for-att-hindra-och-utreda-brott/

that have restrictiveness as their selling point,"[111] that is, that they use the operators that have stopped storing data. The article continued to argue that the telecom operators were still required to keep a record of telephone traffic for six months for law enforcement needs in accordance with the current Swedish legislation. According to the general directors, the "[…] subscription, contact and location information are often crucial to prevent, detect, investigate and prove violations" [112] and that the Court of Justice of the EU preliminary ruling of 21 December 2016 was "[…] a major blow to law enforcement activities, and. in practice a success for the criminals." [113] The authors pointed out that the consequences of the preliminary ruling may be very grave. What if a terrorist attack occurs, which could have been prevented by the retention of telecommunications data information? They ended the article by once again announcing the urgency for the government to find a durable solution. [114]

It must be noted that the ruling of the Stockholm Administrative Court of Appeal (*Kammarrätten i Stockholm*) on 8 March 2017, mentioned above, did not led to any further public debate on the subject.

During 2016, eight Swedish scientists and three heads of security operations (in public and private sector) authored an anthology on commission by the Swedish Civil Contingencies Agency (*Myndigheten för samhällsberedskap, MSB*) entitled Surveillance and Integrity (*Övervakning och integritet*).[115] This report was later revised by the authors and published as a book with the title

---

[111] Eliasson, D., Håkansson, E. Mattson, T., Perklev, A. and Thornberg A. Data retension essential to prevent and investigate crime (*Datalagring avgörande för att hindra och utreda brott*), opinion article published in *Dagens Nyheter* (daily newspaper) 14 February 2017, available at: www.dn.se/debatt/datalagring-avgorande-for-att-hindra-och-utreda-brott/

[112] Eliasson, D., Håkansson, E. Mattson, T., Perklev, A. and Thornberg A. Data retension essential to prevent and investigate crime (*Datalagring avgörande för att hindra och utreda brott),* opinion article published in *Dagens Nyheter* (daily newspaper) 14 February 2017, available at: www.dn.se/debatt/datalagring-avgorande-for-att-hindra-och-utreda-brott/

[113] Eliasson, D., Håkansson, E. Mattson, T., Perklev, A. and Thornberg A. Data retension essential to prevent and investigate crime (*Datalagring avgörande för att hindra och utreda brott),* opinion article published in *Dagens Nyheter* (daily newspaper) 14 February 2017, available at: www.dn.se/debatt/datalagring-avgorande-for-att-hindra-och-utreda-brott/

[114] Eliasson, D., Håkansson, E. Mattson, T., Perklev, A. and Thornberg A. Data retension essential to prevent and investigate crime (*Datalagring avgörande för att hindra och utreda brott*), opinion article published in *Dagens Nyheter* (daily newspaper) 14 February 2017, available at: www.dn.se/debatt/datalagring-avgorande-for-att-hindra-och-utreda-brott/

[115] Sweden, Swedish Civil Contingencies Agency (*Myndigheten för samhällsberedskap, MSB*), Surveillance and Integrity (*Övervakning och integritet*) 11 May 2016, available at: https://www.msb.se/Upload/konferenser/%C3%96vervakning%20och%20integritet%202015/Rapport%20till%20MSB.pdf The authors are Mr. Håkan Hydén, professor emeritus in Sociology of Law at Lund University; Mr. Janne Flyghed, professor in Criminology at the University of Stockholm; Ms. Julia Branting, former lead strategist in the city of Malmö; Mr. Marcin de Kaminskin, Ph.D. student in Sociology of Law and researcher at the Internet institute and Mr. Per Gustafson, Head of Security and Ph.D. in security processing (*sekuritetshantering*) both at Lund University; Mr. Petrus Bolin, Head of Security at the Handelsbanken concern, former police officer; Mr. Markus Lahtinen and Mr. Benjamin

Surveillance and integrity: technology, protection and actors in the new control era. (*Övervakning och integritet: teknik, skydd och aktörer i det nya kontrollandskapet*).[116] The book chapters deal with contextual integrity, the monitoring of metadata, new actors and new control technology, and the effects of CCTV surveillance. The book ends with a concluding discussion on surveillance asking if surveillance should be seen as the protection or destruction of democracy.

No other academic papers or articles have been published during the period in question that relates to the subjects in focus. The same applies to reports on surveillance and/or intelligence issued by any non-governmental organisations. In fact, there are hardly any NGOs focusing on these issues in Sweden. The Pirate party (*Piratpartiet)* is at the moment primarily concerned with the ruling of the Supreme Patent and Market Court (*Patent- och marknadsöverdomstolen*) of 13 February 2017.[117] The ruling changed the previous ruling of the district court. Consequently, the internet service provider in question, Bredbandsbolaget, must apply the technical measures necessary to prevent its customers' access to the Pirate Bay and Swefilmer through different domain names and URLs. The ruling will likely lead to a situation where all international service providers must block the Pirate Bay.

ANNEX – Court decisions

Thematic area	Please provide the most relevant high court decision relating to the use of s NO SWEDISH COURT HAS TAKEN ANY DECISION OF A PRECEDENTIAL NATUF SURVEILLANCE MEASURE DURING THE PERIOD 1 AUGUST 2016 – 31 MARCH A thorough search in the data base www.rattsinfosok.dom.se/lagrummet/i decisions taken by: • 48 District Courts (*Tingsrätter*) • Svea Court of Appeal (*Svea Hovrätt*) • Göta Court of Appeal (*Göta Hovrätt*)

Weaver, both researchers at the Institute for economic research at Lund University; Mr. Markus Naarttijärvi, Dr. in Law and Senior Lecturer at the Law Department at the University of Umeå; Mr. Tobbe Petterson, researcher in Intelligence Analysis at Lund University and Mr. Wilhelm Agrell, professor in Intelligence Analysis at Lund University.

[116] Agrell, W., Petterson, T. (eds.) (2016) Surveillance and integrity: technology, protection and actors in the new in the control environment (*Övervakning och iintegritet: teknik, skydd och aktörer i det nya kontrollandskapet*), Stockholm: Carlsson.

[117] Sweden, Pirate party *(Piratpartiet)*, Swedish court opens Pandora's box *(Svensk domstol öppnar Pandoras ask),* 13 February 2017, available at: www.piratpartiet.se/svensk-domstol-oppnar-pandoras-ask/

Sweden, Supreme Patent and Market Court (*Patent- och marknadsöverdomstolen*)*, Press* Release, ISP ordered to block its customers' access to certain so-called pirate sites (*Pressmeddelande, Internetleverantör åläggs att blockera sina kunders tillgång till vissa s.k. piratsajter*), 13 February 2017, available at: www.svea.se/Om-Svea-hovratt/Nyheter-fran-Svea-hovratt/Internetleverantor-alaggs-att-blockera-sina-kunders-tillgang-till-vissa-sk-piratsajter/

	• Scania and Blekinge Court of Appeal (*Hovrätten över Skåne och Blek* • Court of Appeal for Western Sweden (*Hovrätten för Västra Sverige*) • Court of Appeal for Southern Norrland (*Hovrätten för Nedre Norrla* • Court of Appeal for Northern Norrland (*Hovrätten för Övre Norrland* • Supreme Court (*Högsta domstolen*) • 12 Adminstrative Courts (*Förvaltningsdomstolar*) • Stockholm Adminstrative Court of Appeal (*Kammarrätten i Stockho* • Gothenburg Adminstrative Court of Appeal (*Kammarrätten i Gothe* • Sundsvall Adminstrative Court of Appeal (*Kammarrätten i Sundsval* • Jönköping Adminstrative Court of Appeal (*Kammarrätten i Jönköpi* • Supreme Administrative Court (*Högsta förvaltningsdomstolen*) • Labour Court (*Arbetsdomstolen*) • Supreme Land and Environmental Court (*Mark- och miljööverdoms* • Supreme Migration Court (*Migrationsöverdomstol*) • Supreme Patent and Market Court (*Patent- och marknadsöverdoms* • *Etc.* During 1 August 2016 – 31 January 2017 only 110 decisions have been mad precedential nature. After a review of these decisions we can state that no surveillance measures, as defined by the FRA 2015 report. One decision by (*Högsta förvaltningsdomstolen*)*,* 21 October 2016 (HFD 2016 ref. 71), conce be considered as an instance of illegal camera surveillance. Consequently, t Surveillance (*Kameraövervakningslag [2013:460]*)[118] A complementary information request was sent via e-mail to the District Co *tingsrätt)*, that has a special responsibility for cases on surveillance. The req 2017. It was stated that the Court was not able to disclose any information of any cases, due to its secrecy regulations. The ruling of the Administrative Court of Appeal in Stockholm (*Kammarrätt* not considered to be of a precedential nature.
Decision date	
Reference details	
Key facts of the case (max. 500 chars)	

[118] Sweden, Act on Camera Surveillance *(Kameraövervakningslag [2013:460])*, 30 May 2013, available at: www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/kameraovervakningslag-2013460_sfs-2013-460

Main reasoning/argumentation (max. 500 chars)	
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	
Key quotation in original language and translated into English with reference details (max. 500 chars)	