JURIDISKA FAKULTETEN
vid Lunds universitet

Marie Tinggren Göthe

Brottsbekämpning och personlig integritet

EU-rättens inverkan på datalagring i svensk och tysk rätt

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Henrik Wenander

Termin för examen: VT2021

Innehåll

Summary

This thesis aims at providing an in-depth study of the balancing act made by the Swedish legislator between the rights to privacy and data protection on the one hand, and the retention of data generated in connection with the provision of publicly available electronic communications networks on the other hand. The latter aspect is something that is made in order to ensure that the data are available for law enforcement agencies for the purpose of the investigation of potential crime. When it comes to regulations on the so-called "E-Privacy" (i.e. privacy when using electronic communication services) the European Law mainly has precedence over national laws, hence an explanation of the national law as well as the EU law on privacy and the law on retention of certain data for the purpose of the investigation of crime, is presented in this thesis. The cardinal principles on E-Privacy within the European Union are set out in the E-Privacy Directive.

Generally, privacy is mainly protected by explicit provisions: the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (CFR), which both highlight the respect for private life. The E-Privacy Directive harmonises the provisions of the European member states required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector. Based on this directive, which is incorporated in the Swedish Data Collection Act lagen (2003:389) om elektronisk kommunikation (LEK) an analysis of the Swedish implementation process is made. Additionally, the legislative outcome and in which way it has affected law enforcement agencies, the operators and the individual are examined. The cases Tele2 and Digital Rights announced by the Court of Justice of the European Union (CJEU) and their impact on the Swedish E-Privacy legislation is studied and evaluated in a separate chapter. Within the Swedish constitutional law, privacy is protected in the regeringsformen. The Swedish protection of privacy is compared with the corresponding German constitutional rights stated in das Grundgesetz (GG). In addition, a comparison is made between Swedish and German law on E-Privacy. The latter is called das Telekommunikationsgesetz TKG. A further aim is to discuss the checks and balances between the EU-legislator and the member states and to examine which impact the separation of powers, as stated in the EU treaties, and the national sovereignty concerning issues like national security have when it comes to the above-described data retention and E-Privacy. This is made in the context of two newly announced (as of October 2020) cases from the CJEU.

The legal method used in the study is the one focusing on the investigation and systematization of contemporary law in order to establish the *lex lata*. This method is combined with the methods of comparative law. The chosen approach, and the support that is provided in the legal literature, is

elaborated in the introductory chapter. The examination is based on the above mentioned legislation, the legislative history, relevant case law, and a range of legal literature.

In conclusion, the traffic data retention prescribed in LEK is of great importance for law enforcement. At the same time the processing of information connected to electronic communications made by the national operators limits the scope of private life. Privacy is a crucial issue in the Western society, still it is elusive as a concept. It touches the foundations of society. It is the primary task of the law when it comes to traffic data retention to, on the one hand prevent abuse when dealing with sensitive information, on the other hand provide law enforcement authorities sufficient information. This thesis proves that this balancing act done by the legislator is a complex and delicate affair. Data processing will be legitimate and likely to be more accepted by the public if based on a well-founded motivation considering the interests at stake. This is important so as to prevent distrust among all those involved in the operators' data collecting process, in other words everybody using the affected electronic communications. Different aspects of this matter on a social as well as an individual level are discussed in this thesis. The government's right to obtain this information, i.e. to have a look into the processing behind someone's electronic communications, must be underpinned by the legislator, which requires clarity and transparency in legislation. According to the main rule in the E-Privacy Directive the member states must ensure confidentiality of the communications. Traffic data relating to users processed by the operator must be made anonymous or be erased when it is no longer needed for the purpose of the transmission of communications. However, the national law maker may adopt legislative measures to restrict the scope of the rights provided in the directive when such restriction constitutes a necessary and proportionate measure within a democratic society to safeguard, inter alia, national security and the prevention, investigation, detection, and prosecution of criminal offences. The implementation process of the E-Privacy Directive in the Swedish legislation LEK will be dealt with in the examination as well as the major shift in the EU approach towards traffic data retention which emerged as a result from the Data Retention Directive. This was the starting point of a vast retention of data generated or processed in connection with the provision of publicly available electronic communications services, and for this reason the Swedish LEK was also reformed, which obliged the operators to store a lot more information than before, due to law enforcement activity.

A landmark case before the CJEU was the case Digital Rights. Again, changes to the EU law on traffic data retention followed since the Court of Justice declared the Data Retention Directive to be invalid. Despite this the Swedish law stayed the same. As a consequence, a couple of years later, in the case Tele2, the Swedish regulation was declared to be too excessive and therefore violated the right to privacy according to the CFR. Since the implementation of the Data Retention Directive the national legislation

contains a dual system: one traffic data retention focusing on the so-called practical reasons such as billing (this type of processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued), one that is done exclusively for law enforcement activities. This has caused an unforeseen situation since some operators use this dual system in order to limit their traffic data retention based on practical reasons. This is a part of a selling strategy aimed at customers who want to stay away from the public eye as much as possible. Due to the case Tele2 the extent of the Swedish traffic data retention was limited. The complex balancing act on this matter made by the Swedish legislator is partly compared with German law. The comparison regards the outcome of the Swedish and the German implementation of the Data Retention Directive insofar as it affects the contemporary national legislation, LEK respectively the German TKG. A conclusion that can be drawn is that the right to respect for one's private life as declared in the CFR, as well as the rights listed in the E-Privacy Directive, have improved the national privacy legislation. Still, another effect, paradoxically, is that the Data Retention Directive curtailed the same rights as long as the directive was valid. The expanded data traffic retention was positive for law enforcement agencies but affected the individual and the net operators negatively. Therefore, it can be said that the EU legislator has had an inconsistent and ambiguous view on the law on privacy and data protection in connection with legislation concerning data retention. As a consequence of this, since the EU law is superior to national law, this inconsistent approach towards these two issues also shows in the national legislative history, the place where the balancing act made by the Swedish legislator is presented. The privacy laws of Germany are stronger than the Swedish ones. However, these differences don’t show significantly on the law of E-privacy in respective country. Some of the data categories as currently listed in LEK, due to the Swedish interpretation of the E-Privacy Directive, must be revised since they run counter to rulings made by the CJEU at the end of 2020. The impact of these cases over LEK are analysed at the end of this thesis. The division between the different categories is difficult to understand. The information provided by these are in some aspects almost the same, but still they are surrounded by different restrictions. The described balancing act, which needs to be done by the national lawmaker in accordance with EU law as well as constitutional law, is basically about balancing freedom against security. Without any data retention criminal investigations would be difficult to accomplish, and in the long run some crimes would be impossible to solve at all. The right of the individual to total freedom, which some advocators demand when using electronic communications, can therefore have a negative effect on other individuals if they happen to be a victim of crime. Fulfilling both of these objectives requires a delicate balance to be struck. Both aspects are fundamental parts in the Western society and in the social contract theory. Hence, this calls for a clear and well-motivated legislation on E-Privacy. When it comes to the time limits in LEK, improvements can be made. The reason for this is given in this analysis.

Sammanfattning

Uppsatsens syfte är att fördjupa förståelsen för den svenska lagstiftarens avvägning mellan personlig integritet och de brottsbekämpande myndigheternas behov av datalagring hos telekommunikationsbolag. Den nationella rätten styrs av EU-rätt på det här området och därför ingår i syftet att redogöra för det nationella och EU-rättsliga regelverket rörande dels datalagring av brottsbekämpande skäl, dels den lagstiftning som skyddar den personliga integriteten. I centrum står det så kallade E-Privacy-direktivet liksom det rättighetsskydd som tillkommer den enskilde i främst Europakonventionen och EU-stadgan. Det förstnämnda ska tillförsäkra att medlemsländerna har ett likvärdigt personuppgiftsskydd vid elektronisk kommunikation. Utifrån detta analyseras sedan den svenska implementeringslagstiftningen, lagen (2003:389) om elektronisk kommunikation, LEK, och vad denna innebär för teleoperatörer, brottsbekämpande myndigheter och enskilda i Sverige. Två rättsfall från EU-domstolen, Digital Rights respektive Tele2, analyseras i ett separat kapitel utifrån deras innebörd för den nämnda svenska datalagringslagstiftningen. Gällande skyddet av den personliga integriteten i regeringsformen jämförs det med motsvarande skydd i den tyska grundlagen, das Grundgesetz. Vidare betraktas den svenska LEK utifrån dess tyska motsvarighet, Telekommunikationsgesetz, TKG. Utifrån två rättsfall från EU-domstolen som meddelades under 2020 är uppsatsens vidare syfte att även diskutera vilken effekt maktdelningen mellan unionen och medlemsländerna får för den datalagring som sker mot bakgrund av att trygga nationell säkerhet.

Tillämpad metod är den rättsdogmatiska. Av metodavsnittet framgår hur denna har kombinerats med komparativ metod liksom vilket stöd för en sådan utformning som finns i den rättsvetenskapliga litteraturen. Utgångspunkten för redogörelsen utgörs av lag, förarbeten, rättspraxis och ett urval av svensk och internationell litteratur. Sammanfattningsvis visar undersökningen att den datalagring som föreskrivs i LEK är av stor betydelse för brottsbekämpningen, men innebär samtidigt en inskränkning i den personliga integriteten. Datalagringslagstiftningen måste å ena sidan borga för att de brottsbekämpande myndigheterna får tillgång till nödvändig information för att på så vis kunna fullgöra sitt uppdrag, å andra sidan ska lagstiftningen se till att känslig personlig information hos operatörerna inte kan missbrukas. Uppsatsen visar att det är en svår balansakt som lagstiftaren har stått inför. För att informationsinsamlandet hos operatörerna inte ska mötas av misstro är det såväl på individ- som samhällsnivå viktigt att det finns en tydlig motivering till varför staten ska ha insyn i enskildas privatliv. Samtidigt framgår av utredningen att begreppet personlig integritet är svårdefinierat vilket avspeglar sig i de avvägningar som lagstiftaren har gjort mellan denna och brottsbekämpningen.

Grundregeln i E-Privacy-direktivet är konfidentialitet för den enskildes uppgifter, men från detta görs undantag. För det första är datalagring tillåten då det är nödvändigt av rent tekniskt praktiska skäl för att den elektroniska kommunikationen ska kunna överföras mellan användare. Av praktiska skäl undantas även den datalagring som krävs för abonnentfakturering som får behandlas av operatörerna till dess att fordran är betald eller att preskription har inträtt och det inte längre lagligen går att göra invändningar mot faktureringen. För det andra får datalagring ske då det är nödvändigt av brottsbekämpande skäl och under förutsättning att inskränkningen kan anses vara en proportionell åtgärd i en demokrati. Hur direktivet har genomförts i LEK behandlas i undersökningen liksom vilka bakomliggande tankegångar som då fanns hos lagstiftaren. När datalagringsdirektivet ett par år senare antogs kullkastades den tidigare restriktiva datalagringslagstiftningen och en mycket omfattande lagring av uppgifter tog vid istället. LEK utvidgades därför med en ny datalagringsform enkom för brottsbekämpande ändamål. Genom den så kallade Digital Rights domen underkändes datalagringsdirektivet men svensk rätt ändrades inte efter domen. Följden blev att den svenska datalagringen i LEK underkändes i EU-domstolen i den så kallade Tele2-domen. Sammanfattningsvis kan sägas att sedan datalagringsdirektivet infördes i svensk rätt har det löpt två olika lagringsformer hos operatörerna vid sidan av varandra: en som sker av vad som benämns som ”praktiska skäl” och en av de ovan beskrivna brottsbekämpande skälen. På ett oförutsett vis har den praktiskt inriktade lagringen börjat nyttjas av vissa operatörer för att locka ”ljusskygga” kunder. Hur detta ter sig i praktiken vidareutvecklas i redogörelsen. Tele2-domen medförde att LEK fick genomgå en reform där både omfattningen av de olika uppgiftsslagen, såväl som deras lagringstid, drogs ned. En av uppsatsens kärnpunkter är det kapitel som analyserar lagstiftarens avvägning mellan brottsbekämpande myndigheters behov av trafikuppgifter mot det integritetsintrång detta innebär. I detta kapitel görs en jämförelse mellan hur utkomsten av den svenska och den tyska implementeringen av de nämnda EU-direktiven tar sig uttryck i ländernas respektive lagstiftning.

De viktigaste resultaten av undersökningen är att skyddet för den personliga integriteten i svensk rätt har stärkts av EU-rätten bland annat genom EU-stadgan och det nämnda E-Privacy-direktivet. Samtidigt har EU-rätten varit orsaken till ökade datalagringskrav för operatörerna genom datalagringsdirektivet. För de brottsbekämpande myndigheterna är detta positivt medan det får ses som en nackdel för den enskilde liksom för operatörerna. En slutsats som dras är därför att synen på den personliga integriteten kontra datalagring har varit inkonsekvent i EU-rätten. Detta visar sig även i de avvägningar som den svenska lagstiftaren har gjort i förarbetena till LEK. En annan slutsats är att Sverige och Tyskland som utgångspunkt har olika starka skydd för den personliga integriteten, men detta visar sig inte nämnvärt i hur deras datalagringslagstiftning ser ut idag.

Vidare har konstaterats att synen på vissa lagringsslag i LEK kommer att behöva revideras då behandlingen av dessa uppgifter inte följer EU-rättslig praxis från förra året. Vilka uppgifter detta gäller och hur LEK i detta

avseende avviker från de krav som ställs upp av EU-domstolen i de två aktuella rättsfallen analyseras i ett av uppsatsens senare kapitel. En effekt av den här uppgiftshanteringen är en svårbegriplig uppdelning mellan uppgiftskategorier som i stort ger samma typ av information. Datalagring av brottsbekämpande skäl bygger förenklat sagt på en avvägning mellan frihet och säkerhet och måste respektera såväl grundlag som EU-rätt på området. Utan denna datalagring skulle färre brott klaras upp, och en persons frihet går då ut över en annan persons säkerhet. I förlängningen skulle vissa brott bli omöjliga att lösa. Total frihet från datalagring vid användandet av elektronisk kommunikation har på så vis en negativ inverkan på brottsbekämpningen. Båda aspekterna, det vill säga frihet respektive säkerhet, är grundläggande i samhällskontraktet och i den västerländska rättsstaten. För lagstiftaren är det en delikat uppgift att förena dessa två samhällsbärande värden vid utarbetandet av lagstiftning som rör datalagring av elektronisk kommunikation. Höga krav ska därför ställas på lagstiftarens bakomliggande avvägning. I detta avseende behöver LEK:s lagringstider ses över och anledningen till detta utvecklas i uppsatsen.

Förkortningar

Ds	Departementsserien
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
FEK	Förordning (2003:396) om elektronisk kommunikation
FEUF	Fördraget om Europeiska unionens funktionssätt
FEU	Fördraget om Europeiska unionen
GDPR	General Data Protection Regulation
GG	Grundgesetz für die Bundesrepublik Deutschland (tysk grundlag)
IP	Internet protocol
JK	Justitiekanslern
JO	Justitieombudsmannen
LEK	Lag (2003:389) om elektronisk kommunikation
NAT	Network Address Translation (nätadressöversättning)
PTS	Post- och telestyrelsen
TKG	Telekommunikationsgesetz (tysk lag om elektronisk kommunikation)
SOU	Statens offentliga utredningar
Säpo	Säkerhetspolisen
VPN	Virtual private network

1 Inledning

1.1 Bakgrund

"Throughout the West the computer networks grow, collecting their millions of bits of data, depositing the smallest details of lives into the unforgetting memory units."

Detta skrevs år 1967 av amerikanen Alan F. Westin, i pionjärarbetet *Privacy and Freedom.*[1] Den statligt sanktionerade datalagringen och dess påverkan på individen, är som framgår, på intet sätt en ny knäckfråga för lagstiftare runt om i världen. Däremot kan sägas att omfattningen av denna lagring har intensifierats, liksom den efterföljande debatten. Det råder nämligen ett spänningsförhållande mellan å ena sidan enskildas personliga förhållanden och korrespondens, och å andra sidan lagring av telekommunikation hos teleoperatörerna för brottsbekämpande ändamål, ofta benämnt datalagring. För lagstiftaren är det således en balansakt att förena nämnda lagring och samtidigt upprätthålla ett integritetsskydd för individen som är acceptabelt i ett demokratiskt samhälle. Detta gör sig påmint i utformningen av såväl nationell rätt som EU-rätt och emanerar ur den grundläggande offentligrättsliga frågan om relationen mellan individ och stat. För svensk del kan noteras att redan 1941 uttalades, i den av Herbert Tingsten ledda utredningen, *Betänkande med förslag till ändrad lydelse av § 16 regeringsformen*, att: "regleringen av medborgerliga fri-och rättigheter får icke givas ett så absolut och ovillkorlig karaktär, att hinder uppstå för de ökade statsingripanden och de intrång i de enskildas frihet och självbestämningsrätt, som under särskilda förhållanden kunna vara erforderliga".[2] Sedan dess har väldiga tekniska framsteg gjorts vilket gör att det i dagens informationssamhälle är möjligt att kartlägga en individs kontaktmönster och vanor. En annan aspekt är att brottslighet i vissa fall har letat sig ut på internet. Tillgången till lagrade uppgifter från teleoperatörer är därför av mycket stor betydelse för de brottsbekämpande myndigheterna. Denna datalagring förutsätter samtidigt ett intrång i den enskildas personliga sfär.[3] Frågan här är därför inte om detta ska få tillåtas, utan snarare hur denna ska utformas för att skapa så lite skada som möjligt för den enskilde.

Hur avvägningen mellan upprätthållandet av den personliga integriteten gentemot tillhandahållandet av datalagring för brottsbekämpande ändamål till berörda myndigheter har gjorts i Sverige, kommer följande framställning att ta sikte på. Helt centralt är det EU-direktiv som gäller sedan 2002, E-Privacy-direktivet, som ska säkerställa den enskilda rätten till privatliv och rätten till skydd för personuppgifter inom sektorn för elektronisk

1 Westin (1968) s. 399 jfr Strömholm (1971) s. 709, 736, Strömholm (1980) s. 23–39.
2 SOU 1941:20 s. 15. Om nordisk demokratidebatt mellan Alf Ross och Herbert Tingsten se Nergelius (1996) s. 133 ff.
3 Prop. 2010/11:46, bilaga 2 s. 18.

kommunikation.[4] Där föreskrivs att medlemsstaterna är skyldiga att se till att uppgifter om elektronisk kommunikation, exempelvis en samtalsfrekvens, ska behandlas konfidentiellt liksom att de uppgifter som inte längre är i behov av användning ska avidentifieras eller raderas.[5] Det står dock medlemsstaterna fritt att göra undantag från dessa åligganden om det behövs för vissa angivna syften.[6] Undantagen utgör medlemsländernas stöd för att begränsa den enskildas integritetsskydd under förutsättning att det krävs bland annat för skydda statens säkerhet eller för att förebygga och klara upp brott. För svensk rätts vidkommande är direktivet genomfört i främst lagen (2003:389) om elektronisk kommunikation, LEK, liksom förordningen (2003:396) om elektronisk kommunikation.

E-Privacy-direktivet ska ses mot bakgrund av att EU:s medlemsstater ska garantera den enskilda två grundläggande rättigheter, dels rätten att bli fredad från kränkningar från statligt håll, dels statens skyldighet att garantera enskilda skydd mot kränkningar från andra enskilda. Det åligger det offentliga att se till att det finns ett ramverk som är förenligt med dessa principer, som i viss mån får sägas konkurrera sinsemellan. De rättigheter som främst är aktuella vid datalagring är rätten till respekt för privatlivet och den personliga integriteten, rätten till skydd för personuppgifter och rätten till yttrande-och informationsfrihet, vilka alla skyddas nationellt liksom i EU-och europarätten. År 2017, i den så kallade Tele2-domen från EU-domstolen, underkändes vissa delar av den svenska datalagringslagstiftningen i LEK då dessa inte var förenliga med E-Privacy-direktivet.[7] De paragrafer i LEK som reglerar datalagring för brottsbekämpande ändamål, var enligt EU-domstolen alltför vitt hållna vilket medförde att de inte levde upp till det EU-rättsliga integritetsskyddet.

Den del av den svenska datalagringen som underkändes av EU-domstolen var en följd av det så kallade datalagringsdirektivet[8], som var i kraft mellan 2006 och 2014. Datalagringsdirektivet ändrade förutsättningarna för E-Privacy-direktivet genom att de undantag som tillåts i E-privacy-direktivet användes för att utvidga datalagringen för brottsbekämpande ändamål i mycket stor skala. Datalagringsdirektivet underkändes 2014 då EU-domstolen, i den så kallade Digital Rights-domen[9], konstaterade att den EU-rättsliga lagstiftaren hade överskridit sina befogenheter vid dess instiftande. I Sverige bedömdes dock att de bestämmelser som grundade sig på detta underkända direktiv fortsatt skulle kunna tillämpas, vilket EU-domstolen sedermera alltså kom att hindra i Tele2-domen. Dessa olika ”turer” kommer

4 Europaparlamentets och rådets direktiv 2002/58/EG av den 12juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), hädanefter E-Privacy-direktivet.
5 Prop. 2018/19:86 s. 12 och 18.
6 Artikel 15.1 i E-Privacy-direktivet förklaras ingående nedan i kapitel 4.
7 C-203/15 och C-698/15 Tele2, EU:C:2016:970 jfr prop. 2018/19:86 s. 12.
8 Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.
9 C-293/12 och C-594/12, Digital Rights, EU:C:2014:238.

att beröras mer ingående i redogörelsen nedan. De nämnda domarna liksom datalagringsdirektivet har i hög grad påverkat hur den svenska lagstiftaren har utformat genomförandet av E-Privacy-direktivet i LEK. Tele2-domen gav upphov till debatt i EU och i Sverige fick lagstiftaren omformulera de paragrafer som EU-domstolen slog ned på för att på så vis implementera E-Privacy-direktivet på ett godtagbart vis. Dessa utgör sedan oktober 2019 gällande rätt.

Ett av de länder där Tele2-domen medförde debatt om balansen mellan statens brottsbekämpande verksamhet, utifrån behovet av datalagring hos telekommunikatörer, liksom värnandet om den personliga integriteten var Tyskland. Då landet av historiska skäl har en annan syn på integritetsfrågor och därmed ett annat konstitutionellt skydd för detta jämfört med Sverige kommer en utblick att göras på dels den tyska regleringen av datalagring för brottsbekämpande ändamål, TKG, dels hur den personliga integriteten värnas.

1.2 Syfte

Syftet med uppsatsen är att bidra med en fördjupad förståelse för den svenska lagstiftarens avvägning mellan skyddet för den personliga integriteten och de brottsbekämpande myndigheternas behov av datalagring hos telekommunikationsbolag. Undersökningen görs i ljuset av EU-rättens krav på nationell rätt och i syftet ingår därför att redogöra för det nationella och EU-rättsliga regelverket rörande dels datalagring hos teleoperatörer som kan komma de nationella brottsbekämpande myndigheterna till del, dels den lagstiftning som skyddar den personliga integriteten. Datalagring för brottsbekämpande ändamål som rör nationell säkerhet rör sig i gränslandet mellan EU:s och medlemsländernas egna maktsfärer och hur det påverkar den nationella implementeringslagstiftningen ingår i uppsatsens syfte. För att sätta den svenska lagstiftningen i ett europeiskt perspektiv görs en avgränsad utblick på tysk rätt.

Den här övergripande uppgiften delas in i följande delfrågeställningar:

1. Vad innebär datalagring hos teleoperatörer och vilka integritetskrav ställer LEK upp för den här verksamheten?
2. Hur skyddas den personliga integriteten i EU- och europarätten liksom i svensk respektive tysk rätt?
3. Hur ser det EU-rättsliga integritetsskyddet inom sektorn för elektronisk kommunikation ut?
4. Hur har den tyska och svenska lagstiftaren reglerat datalagring för brottsbekämpande ändamål i TKG och LEK sedan datalagringsdirektivet genomfördes i länderna?
5. Hur har den EU-rättsliga rättsutvecklingen som har följt efter datalagringsdirektivet påverkat Sverige och Tyskland?
6. Vilka slutsatser om personlig integritet i förhållande till datalagring för brottsbekämpande ändamål kan dras utifrån undersökningen?

1.3 Avgränsningar

Uppsatsen behandlar regleringen av datalagring hos teleoperatörer och inte den efterföljande inhämtningen av uppgifterna till myndigheterna. I den mån inhämtningen berörs är det för att det krävs för förståelsen och systematiken bakom lagringsmomentet. Ett skäl till uppdelningen är att inhämtningen är en fråga som hör till straffrätten. Gällande avsnittet om personlig integritet är det avgränsat till att ge en grundförståelse för den svenska synen på personlig integritet liksom vilka folkrättsliga och nationella regler som ska beaktas på området. Detta enbart utifrån de aspekter av den personliga integriteten som ankommer på berörd datalagring. LEK:s förordning berörs i de fall som det tillför lagringsmomentet i LEK relevant information, däremot ska detta inte ses som att förordningen på ett genomgående vis behandlas och rena tekniska specifikationer utelämnas. Teknisk indelning av lagrade uppgifter styr dock integritetsskyddet. Avgränsningen av lagstiftningens tekniska aspekter har utgått från i vilken grad informationen krävs för att förstå dess påverkan på integritetsskyddet. Gällande avgränsningen av den tyska rätten är detta en följd av metoden och detta behandlas därför under nästa rubrik i sitt sammanhang.

1.4 Metod och material

Redogörelsen för svensk rätt följer rättsdogmatisk metod och därtill knutna rättskällor (lag, förarbeten, prejudikat och doktrin). Huvudsyftet med den rättsdogmatiska metoden är att fastställa gällande rätt (*lex lata*) vilket innefattar att beskriva och systematisera denna.[10] Kritisk rättsdogmatisk forskning går vidare med resultatet av denna rekonstruktionsuppgift och kan utifrån fristående ändamålsargument påvisa att rättsläget är otillfredsställande, om detta visar sig vara fallet.[11] Det senare har använts som ett tillvägagångssätt för att bedöma hur den nationella rätten förhåller sig till EU-rätten. Claes Sandgren respektive Jan Kleineman framhåller båda att den rättsdogmatiska metoden inte utesluter användning av annat än det klassiskt rättsdogmatiska materialet för att på så vis berika analysen. Detta eftersom utländsk rätt kan vara användbar för att peka på svagheter i analysen av inhemsk gällande rätt. En landvinning som uppnås med jämförande studier är att ett främmande lands reglering av en fråga kan kasta nytt ljus över den egna rättens synsätt vilket därmed ökar förståelsen för inhemsk rätt. Helt avgörande i den komparativa metoden är att syftet med jämförelsen tydligt framgår för läsaren.[12] Av denna anledning ska användningen av den tyska rätten förklaras i det följande.

Inledningsvis i denna del ska sägas att Jaakko Husa framhåller att den komparativa rätten och dess metod spänner över ett mycket brett område

[10] Sandgren (2015) s. 43 jfr Kleineman (2013) s. 26, Sandgren (2009) s. 117–125.
[11] Kleineman (2013) s. 34, 37, 39.
[12] Sandgren (2015) s. 44, 55, Kleineman (2013) sid 40–42 jfr Bogdan (2003) sid 57.

med olika vetenskapliga inriktningar.[13] Utgångspunkten för den så kallade klassiska formen av komparation, som starkt förknippas med Konrad Zweigert och Hein Kötz[14], är att jämföra rättsregler som fyller samma funktion i sina respektive rättssystem.[15] Syftet med uppsatsen komparativa delar är att ge en utblick på den tyska synen på dels personlig integritet, dels implementeringen av de EU-rättsliga reglerna avseende datalagring för brottsbekämpande ändamål.[16] Vad gäller neutraliteten vid utformningen av jämförelsen är denna av avgörande betydelse för att denna ska kunna tillskrivas något värde överhuvudtaget. Kischel framhåller svårigheten med att ha en objektiv inställning till jämförelseobjekten.[17] Med detta sagt har utgångspunkten ändå varit att inte plocka ”tyska russin ur kakan” där det tycks passa för att styrka ett argument, utan såväl den svenska som den tyska rätten har behandlats likvärdigt och med iakttagande av rättskällehierarkin i de delar som jämförs. Vad gäller avgränsningen i de jämförande avsnitten redogörs det för nedan.

För att inte hamna i det Sandgren benämner som ett ”mellanläge”, det vill säga där den utländska rätten inte behandlas på ett vedertaget vis alternativt upptar ett oproportionerligt stort utrymme, har jämförelsen utgått från att de regler som har redogjorts för i den svenska rätten gällande personlig integritet har ett korrelerande tyskt avsnitt.[18] Målet har varit att vika ungefär lika mycket utrymme åt de båda länderna i denna del. Utifrån redogörelsen av den tyska regleringen av den personliga integriteten sätts RF:s rättighetsskydd i ett tyskt perspektiv. På motsvarande vis behandlas de paragrafer som reglerar datalagring av rent brottsbekämpande ändamål i LEK respektive den tyska TKG. I denna del sätts den svenska implementeringen av det berörda EU-rättsliga datalagringsregelverket i ljuset av den tyska regleringen. Som framgår av uppsatsens syfte är det dock den svenska rätten som är i huvudfokus. Det som ska utredas är hur den svenska lagstiftaren har vägt skyddet för den personliga integriteten mot de brottsbekämpande myndigheternas behov av datalagring hos telekommunikationsbolag i ljuset av EU-rättens krav på nationell rätt. Gällande den utblick som görs på den tyska datalagringen för brottsbekämpande ändamål ska ett par förtydliganden göras i det följande, detta för att läsaren ska förstå komparationens angreppssätt i denna del.

Beskrivningen av svensk rätt utgår från införandet av LEK och undersöker hur den svenska lagstiftaren vid tiden såg på brottsbekämpande myndigheters behov av datalagring i förhållande till den personliga integriteten. Detta innebär att den svenska rättsutredningen går längre tillbaka i tiden jämfört med den tyska och det beror på att datalagringsdirektivet är en senare tillkommen EU-lagstiftning. Som framkommer är jämförelsen länderna emellan inriktad på att undersöka hur

[13] Husa (2017a) s. 53. Se även Kischel (2019) s. 88.
[14] Se Zweigert & Kötz (1998) s. 34–47.
[15] Kischel (2019) s. 88–89.
[16] Gällande komparativa utblickar se Sandgren (2015) s. 54.
[17] Kischel (2019) s. 92–94.
[18] Sandgren (2015) s. 54.

de har implementerat detta direktiv. Kort sagt: innan denna rent brottsbekämpande lagring tillkom via datalagringsdirektivet skedde redan en datalagring i Sverige utifrån LEK. Analysen av denna äldre svenska datalagring som sker parallellt med den rent brottsbekämpande lagringen (och som nyttjas av de brottsbekämpande myndigheterna) har på grund av just beskrivna komparativa avgränsning inte ett korrelerande tyskt avsnitt. För att läsaren ska kunna förstå den gällande tyska telekommunikationslagstiftningen i sitt sammanhang liksom hur den förhåller sig till den tyska integritetslagstiftningen görs en genomgång av den tyska rättsutvecklingen på området från och med datalagringsdirektivets genomförande. För att sammanfatta komparationens avgränsning: rättsjämförelsen görs enbart utifrån ländernas reglering av den personliga integriteten, liksom utkomsten av de båda ländernas implementering av datalagringsdirektivet så som den tar sig uttryck i nuvarande nationell lagtext i LEK och TKG. Därtill undersöks vilken inverkan Digital Rights-domen respektive Tele2-domen har haft på nämnda nationella lagstiftningar. Detta är också förklaringen till att den svenska rätten tar mest utrymme i anspråk till hela arbetet sett. Koncentrationen ligger således på svensk rätt, därtill görs de just beskrivna avgränsade utblickarna på tysk rätt.[19]

Skälet till att Tyskland valdes är att tysk rätt innefattar en mycket bred rättsdogmatisk forskning. I metodlitteratur uttrycks även att det är att föredra att uppsatsförfattaren kan ta till sig landets primärkällor på originalspråk och studera dessa i kombination med sekundära källor. Även om engelskspråkig och svensk litteratur har använts har studiet av den tyska telekommunikationslagstiftningen, liksom fördjupande artiklar om denna förutsatt kunskaper i tyska.[20] Gällande den komparativa metoden rent generellt har det framhållits i litteraturen att det inom rättsområden där unionsrätt och internationella överenskommelser har en avgörande betydelse, kan det vara angeläget att jämföra medlemsländer. Michael Bogdan varnar för att det vid en jämförelse mellan två rättsordningar är lätt att utgå från att det egna landets lagstiftare har samma mål som den utländska. Just med tanke på denna fälla har just ett EU-direktiv rörande integritetsskydd inom sektorn för elektronisk kommunikation valts som utgångspunkt, vilket innebär att det går att säga att målen med den nationella lagstiftningen ska vara desamma för den tyska och svenska lagstiftaren då detta är dikterat av EU. Bogdan framhåller vidare att det svenska medlemskapet har ”förstärkt behovet hos de svenska juristerna av kunskaper om de ”tunga” medlemsstaternas rätt.” Jämförelser mellan EU-medlemmars rättssystem är ett viktigt inslag i EU:s löpande arbete vid utarbetande och tolkning av sekundärrätten.[21] Vad gäller det tyska materialet utgår det främst från den tyska lagstiftningen på området liksom material från Beck-Online vid sidan om engelskspråkiga standardverk och

[19] Metod och upplägg se vidare i Sandgren (2015) s. 44, 55 och Kleineman (2013) s. 40–42 jfr Bogdan (2003) s. 57.
[20] Kleineman (2013) s. 40. Om språkets betydelse se Bogdan (2003) s. 41–43. Se även Husa (2017b) s. 32–39, Husa (2015) s. 125–127.
[21] Bogdan (2003) s. 20, 34, 75 jfr Jonsson Cornell (2015a) s. 19 ff. som varnar för feltolkningar om författaren inte är metodiskt medveten om fällor i den utländska rätten.

konstitutionella avhandlingar. Utgångspunkten för komparationen har utgjorts av Vera Hillers avhandling, *Der Konflikt zwischen Persönlichkeitsschutz und Pressefreiheit im deutschen und schwedischen Recht* och Joakim Nergelius komparativa avhandling *Konstitutionellt rättighetsskydd.* Det senare verket börjar bli till åren, men har trots detta varit värdefull för förståelsen av tysk grundlag, vid sidan av nyare litteratur. Gällande avsnittet om den tyska datalagringen är SOU 2017:75 *Datalagring – brottsbekämpning och integritet*, anledningen till jämförelsen från första början. Med ledning av utredningens internationella avsnitt kunde jag med säkerhet förvissa mig om att jag jämförde svenska LEK:s korrelerande tyska lagstiftning. Därtill tillhandahölls en svensk sammanfattning av den tyska lagstiftningen vilket har varit till stor hjälp vid det fortsatta arbetet liksom vid översättandet av den tyska lagstiftningen.

Den svenska delen och redogörelsen för gällande rätt har i enlighet med den rättsdogmatiska metoden utgått från RF och LEK liksom relevanta delar av förarbeten till dessa.[22] Bertil Bengtsson menar att även om SOU:er inte leder till lagstiftning kan redogörelsen för gällande rätt respektive analysen av principiella frågor liksom lagens innebörd som där förekommer få betydelse för rättstillämpningen. Bengtsson fastslår att i detta hänseende ”håller de ofta högre klass än propositioner...” Detta eftersom propositionen oftast syftar till att argumentera för den föreslagna lagstiftningen. Även med beaktande av Bengtssons brasklapp om att tillsatta utredningar utgår från olika typer av uppdrag, vilket avspeglar sig i deras inneboende värde som rättskälla, ska inte de teoretiska utläggningarna och den juridiska problematiken i dessa underskattas. En annan sak är att de politiska problemen framträder först vid läsning av propositionen. Även om ett stort mått av utredningar har använts har ambitionen varit att vara medveten om det Bengtsson påpekar när materialet har valts ut. Gällande de remissvar som är med i redogörelsen har detta gjorts med målsättningen att ge en allsidig och nyanserad bild av de synpunkter som har kommit in på lagstiftarens förslag. Samma förhållningssätt har använts vid urvalet av rättspolitiska åsikter. Detta för att kunna sätta ett perspektiv på de avvägningar som lagstiftaren har gjort i förarbetena. Det som har styrt i denna del är därför argumentationens inneboende tyngd.[23] Bland doktrin ska särskilt lyftas fram Markus Naarttijärvis avhandling *För din och andras säkerhet* som har varit till stor hjälp under hela arbetet, inte minst för att förstå datalagringen ur ett bredare rättssäkerhetsperspektiv. Därtill har denna sörjt för tips till referenslitteratur. Utöver detta har rättspolitiska synpunkter från främst Jane Reichel och Thomas Bull bidragit till framställningen av den svenska rätten. Gällande litteraturen om den EU-rättsliga datalagringslagstiftningen som har använts kommenteras den nedan under rubriken forskningsläge. Målsättningen har varit att ge en allsidig belysning inom syftets satta ramar.

[22] Gällande LEK: prop. 2018/19:86, prop. 2010/11:46 och SOU 2017:75. Avseende RF: främst prop. 2009 /10:80, liksom utredningar som föregick reformeringen av RF: SOU 2007:22, SOU 2008:3 och SOU 2008:125.
[23] Bengtsson (2011) s. 777–785 jfr Trolle Önnerfors & Wenander (2019) s. 20, Kleineman (2013) s. 28, 32–33, 35 om det hierarkiska förhållandet mellan förarbeten och doktrin.

Till sist ett förtydligande. Som Ulf Bernitz påpekar inbegriper termen europarätt rättssystem som nära anknyter till EU varav Europakonventionen, EKMR[24], är särskilt viktig. Europarätten är därmed vidare än EU-rätten och Jane Reichel framhåller att EU-rätten kan betraktas som en autonom rättsordning för sig själv. Med detta som utgångspunkt behandlas därför EU-rätten för sig och EKMR behandlas under Europarådets bestämmelser.[25]

1.5 Disposition

Uppsatsen utgår från en sammanhangsdisposition vilket innebär att materialet i möjligaste mån följer ett orsak-verkan-resonemang.[26] Kärnpunkterna i framställningen är de två avvägningsaspekterna personlig integritet och myndigheternas behov av datalagring från teleoperatörer, varför kapitel 2 och 3 behandlar dessa två områden. Kapitel 3 behandlar allmänna regler som skyddar den personliga integriteten i svensk och tysk rätt liksom utifrån EU-och europarätt. Integritetsskydd vid elektronisk kommunikation behandlas separat i kapitel 4. Anledningen till att den personliga integriteten inte behandlas redan i kapitel 2 är för att läsaren först ska få en förståelse för vad datalagring är och på vilket sätt den påverkar den personliga integriteten. Kapitel 2 tillhandahåller en introduktion till LEK och förklarar begrepp som krävs för förståelse av den resterande läsningen. Denna del följs av med en fördjupande del om LEK:s integritetsskydd vid datalagring i kapitel 4. Som beskrevs i inledningen har dessa bestämmelser successivt förändrats i takt med en förändrad EU-rätt på området. Den personliga integriteten vid datalagring behandlas därför, i enlighet med sammanhangsdispositionen, löpande i kapitel 4 till 6, varav kapitel 5 är helt inriktat på EU-domstolens domar Digital Rights och Tele2 som båda har haft ett stort inflytande på LEK:s utformning. Kapitel 6 behandlar lagstiftarens reformarbete som följde i kölvattnet av Tele2-domen. I samma kapitel berörs också nya försvarspolitiska ställningstaganden som EU-domstolen har gjort, vilka ännu inte speglas i den nationella lagstiftningen men som framgent kommer att få betydelse på nationell lagstiftning.

Att den tyska datalagringsregleringen presenteras först i kapitel 6 beror på att det är först där som läsaren har fått en klar bild av såväl den svenska datalagringsregleringen som vilka krav EU-rätten ställer upp. Detta är en förutsättning för att kunna ta till sig en rättsjämförelse länderna emellan. Till sist följer sammanfattande synpunkter i kapitel 7. Jensen med flera betonar att uttryck för egna värderingar ska ske löpande och målet har varit att få till detta utöver uppsatsen avslutande del.[27]

[24] Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, Rom 4 november 1950, SÖ 1952:35, jfr avsnitt 3.3.3.1 om svensk inkorporering.
[25] Bernitz m. fl. (2010) s. 62, Reichel (2013) s. 109 ff.
[26] Jensen m.fl. (2018) s. 24–26, 108–110, Trolle Önnerfors & Wenander (2016) s. 38–44.
[27] Jensen m.fl. (2018) s.113 jfr Trolle Önnerfors & Wenander (2016) s 40.

1.6 Forskningsläge

Rättsfilosofiska aspekter av datalagring har det forskats mycket om. Här kan bland annat Serge Gutwirths *Privacy and the Information Age* och Daniel J Soloves *Nothing to Hide: the False Tradeoff between Privacy and Security* nämnas.[28] I dessa behandlar de båda författarna informationsteknologi och personlig integritet. Orla Lynskey har forskat kring det EU-rättsliga skyddet för personlig integritet i förhållande till unionens dataskyddslagstiftning. Christopher Kuner, Lee A. Bygrave och Christopher Docksey har i sin omfattande kommentar från 2020, *The EU General Data Protection Regulation (GDPR),* behandlat förordningen liksom hur den förhåller sig till andra rättsakter på området. Här kan även nämnas *EU Data Protection Law av* Denis Kelleher och Karen Murray. Tysk dataskyddslagstiftning och EU-rätt på området har Jochen Schneider skrivit om i sin *Datenschutz nach der EU-Datenschutz-Grundverordnung.*

Gällande konstitutionella aspekter på lagring och inhämtning av uppgifter om elektronisk kommunikation i myndigheternas underrättelseverksamhet (preventiva tvångsmedel) i Sverige märks främst Markus Naarttijärvi och hans avhandling *För din och andras säkerhet* från 2013. Även om LEK liksom tekniken har förändrats är avhandlingens rättsstatliga aspekter aktuella. Gällande själva lagringsmomentet i LEK har inte mycket skrivits på senare år, dock har Per G. Andersson bidragit till området genom lagkommentaren till LEK på Juno. Avsaknaden av nyare redogörelser för den svenska datalagringen hos teleoperatörer i litteraturen gör att uppsatsen har ett nyhetsvärde. Bredare perspektiv om informationssamhällets utmaningar behandlas av bland andra Anna-Sara Lind, Jane Reichel och Inger Österdahl i antologierna *Information and Law in Transition – Freedom of Speech, the Internet, Privacy and Democracy in the 21st Century* från 2015, liksom *Transparency in the future – Swedish openness 250 years* från 2017. Gällande forskning om integritetsskyddet nationellt såväl som internationellt ska främst Stig Strömholms forskargärning lyftas fram här, artiklarna *Integritetsskyddet* från 1971 liksom *Individens skyddade personlighetssfär* från 1980 har båda bidragit till en fördjupad förståelse för integritetsskyddets komplexitet i mötet med datateknik.[29] Till sist ska sägas att vad gäller regeringsformens integritetsskydd har mycket skrivits av Thomas Bull, Fredrik Sterzel, Johan Hirschfeldt och Henrik Jermsten.

[28] Aspekter av GDPR se även Gutwirth m.fl. red. (2017) *Data Protection and Privacy: (In)visibilities and Infrastructures.*
[29] Strömholm (1971) respektive Strömholm (1980), se även "Right of Privacy and Rights of the Personality" Strömholm (1967).

2 Brottsbekämpande verksamhet och datalagring i Sverige

2.1 Nationell säkerhet – ett tvetydigt begrepp

”Allas kamp mot alla.” Så ter sig det mänskliga naturtillståndet såvida inte staten, genom samhällsfördraget, träder in och skipar lag och ordning. Denna naturrättsligt präglade tanke, presenterad av Hobbes i *Leviathan* 1651 har bidragit till att säkerhet för medborgaren har spelat en central roll i den konstitutionella debatten.[30] Konceptet med en så kallad nationell säkerhet går således tillbaka till framväxten av nationalstaten, och även om de lärde alltjämt tvistar om vad denna säkerhet ska bestå i mer specifikt så anses tillhandahållandet av en fungerande säkerhetsapparat utgöra en av statens mest grundläggande uppgifter.[31] Såväl Iain Cameron som Markus Naarttijärvi pekar på svårigheterna med att definiera begreppet och att det inte går att ge ett entydigt svar utan en kontext. Innebörden av nationell säkerhet i ett internationellt perspektiv sammanfaller nämligen inte nödvändigtvis med den rent inhemska definitionen av begreppet.[32] Det råder alltså ett spänningsförhållande mellan detta ”trubbiga” begrepp och bibehållandet av rättsstatliga värden, varav den personliga integriteteten utgör ett av dessa. För att citera Iain Cameron;” the weaker the state, the more ambiguous the concept of national security becomes in relation to it.”[33] Flexibiliteten i begreppet kan således medföra visa risker eftersom hänsyn till allmän säkerhet kan rättfärdiga åtgärder som i andra fall hade setts som otänkbara i en demokratisk stat. Begreppet innebär därför en laddning liksom ett potentiellt hot mot grundlagsskyddade rättigheter.[34]

När det gäller den brottsbekämpande verksamheten, innefattar den huvudsakligen utredande – samt underrättelseverksamhet. Den senare är främst inriktad mot att avslöja om en ”viss inte närmare specificerad brottslighet har ägt rum, pågår eller kan antas komma att begås”[35] . Det övergripande målet med underrättelseverksamhet är att förse brottsbekämpande myndigheter med information som kan nyttjas i den operativa verksamheten.[36] Brottsutredningar av redan begångna handlingar sker vanligtvis inom en förundersökning, där man undersöker om ett brott

[30] Hobbes (1651) kapitel XVIII punkt 8, Häthén (2014) s. 64, Robinson (2000) s. 218.
[31] Mill (1960) s. 50, Cameron (2000) s. 39 och Naarttijärvi (2013) s. 114–115.
[32] Naarttijärvi (2013) s. 119 och 121–122 och Cameron (2000) s. 40–49 och 56.
[33] Cameron (2000) s. 41.
[34] Cameron (2000) s. 62–63 och Naarttijärvi (2013) s. 122. Även Prölss-Peter (1986) s. 65–66 och Bull (2009) s. 13–14.
[35] Prop. 2018/19:86 s. 13.
[36] Prop. 2018/19:86 s. 13, prop. 2019/20:64 s. 32 och SOU 2017:75 s. 18.

har begåtts genom handlingen, vem som då kan vara skäligen misstänkt och se till att det finns tillräckligt underlag för att kunna bedöma om åtal ska väckas. Här kommer datalagring in, eftersom den hjälper polisen att ”lägga pussel” och klarlägga händelseförlopp liksom att ringa in misstänkta personer. En viktig hörnsten i detta arbete är att ta reda på när, hur och med vem som en misstänkt har kommunicerat, liksom var personerna som har kontaktat varandra har befunnit sig. Likväl som att hjälpa till att fälla en brottsling kan uppgifterna också leda till att misstänkta personer avförs från vidare utredning.[37] För att få tillgång till denna nödvändiga information är både Säkerhetspolisen (Säpo) och den öppna polisen i behov av medverkan från teleoperatörer som hanterar elektronisk kommunikation. Mot bakgrund av detta föreskrivs i LEK att vissa uppgifter om bl.a. telefoni, meddelandehantering och internettrafik måste lagras under vissa förutsättningar av teleoperatörer.[38]

Ökad internationalisering liksom snabb teknisk utveckling har inneburit att även kriminaliteten har förändrats i vissa avseenden; alltfler internetanvändare möjliggör att brottsplanering kan fortgå såväl inom som utom Sverige, och med detta i åtanke har regeringen beskrivit internet som ”en etablerad plattform för våldsbejakande extremism och terrorismpropaganda.”[39] Även den tilltagande webbaserade narkotikahandeln och barnpornografibrott är gärningar som oftast begås med hjälp av elektronisk kommunikation. Gällande det senare har staten en plikt att bekämpa detta i enlighet med artikel 20 i Europarådets konvention om skydd för barn mot sexuell exploatering och sexuella övergrepp. Därtill stadgar artikel 30.1 att landet ska vidta nödvändiga åtgärder för att säkerställa en effektiv utredning och åtal av brottstypen. I förarbeten till LEK har framhållits att utan effektiva utredningsverktyg är det inte möjligt för Sverige att leva upp till konventionsåtagandena.[40]

Därtill konstaterade Beredningen för rättsväsendets utveckling (BRU), redan år 2005, att datalagring i många fall bidrog med den viktigaste informationen för att driva utredningar om grövre brottslighet framåt. Speciellt vad gäller internetrelaterad brottslighet är tillgången till lagrade uppgifter om elektronisk kommunikation ofta det enda som polisen har att gå på för att komma en misstänkt på spåren.[41] Det finns flertalet konkreta exempel på fall där elektroniska uppgifter har varit av avgörande betydelse i utredningar rörande allvarliga vålds- och sexualbrott. Rörande denna brottstyp, liksom för terroristbrott, är det mycket vanligt att elektroniska uppgifter hämtas in i utredningsskedet.[42] Säpo vittnar om att uppgifter om elektronisk kommunikation är avgörande i deras underrättelsearbete. Kort sagt är datalagringen viktig för att säkra bevisning och förhindra att brott

[37] Prop. 2018/19:86 s. 15, 32–33, 40, SOU 2017:75 s. 18, prop. 2010/11:46 s. 17–18 och SOU 2007:76 s. 133 ff., SOU 2005:38 s. 322–325.
[38] Se 1 kap. 1 och 7 §§ LEK, SOU 2015:31 s. 15 och Naarttijärvi (2013) s. 243.
[39] Prop. 2018/19:86 s. 26.
[40] SÖ 2013:16 jfr prop. 2018/19:86 s. 28.
[41] SOU 2005:38 s. 322–324 och prop. 2018/19:86 s. 14.
[42] SOU 2007:76 s. 133 ff. och prop. 2010/11:46 s. 17–18 och prop. 2018/19:86 s. 14.

begås. I praktiken innebär bristande utredningsverktyg straffrihet för vissa brottstyper.[43] Nedan förklaras närmare vad begreppet datalagring innebär.

2.2 Lagring av elektronisk kommunikation

LEK trädde i kraft i juli 2003 och ersatte då telelag (1993:597) och lag (1993:599) om radiokommunikation. Ett av skälen bakom införandet var att säkra data som har lagrats av de företag som tillhandahåller elektronisk kommunikation så att brottsbekämpande myndigheterna under vissa förutsättningar kan få tillgång till dessa uppgifter.[44] Vissa teleoperatörer måste därför lagra uppgifter om bland annat telefonsamtal och internettrafik som har behandlats i deras verksamhet.[45] Det bredare syftet med lagen framgår av 1 kap. 1 § och består förenklat i att enskilda och myndigheter skall få tillgång till säkra och effektiva elektroniska kommunikationer, med största möjliga urval av kommunikationstjänster liksom ett konkurrensutsatt pris för dessa. Internationell harmonisering och konkurrens ska därför främjas. Enligt 1 kap. 2 § får åtgärderna i lagen inte vara mer ingripande än vad som framstår som rimligt och dessa ska stå i proportion till lagens syfte. LEK är enligt 1 kap. 4 § tillämplig på elektroniska kommunikationsnät och kommunikationstjänster, dock är det inte själva innehållet som överförs i elektroniska kommunikationsnät med hjälp av elektroniska kommunikationstjänster som avses utan det är alltså bara de elektroniska signaler som överför information som omfattas av lagring. Ett elektroniskt kommunikationsnät definieras i 1 kap. 7 § LEK och mycket förenklat innebär det ett system för överföring av signaler med hjälp av olika tekniska metoder. Den här typen av signalöverföring i ett elektroniskt kommunikationsnät sker i det så kallade allmänna kommunikationsnätet, som syftar till att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster mot ersättning, vad som i vanligt tal innebär att man har ett telefonabonnemang. Med detta sagt är således kommunikationsnät ett vidare begrepp i lagen jämfört med kommunikationstjänst och en leverantör av det senare behöver inte samtidigt leverera ett nät för att ändå omfattas av en lagringsskyldighet.[46]

För den som vill tillhandahålla allmänna kommunikationsnät eller elektroniska kommunikationstjänster mot ersättning krävs en anmälan till tillsynsmyndigheten som är Post-och telestyrelsen, förkortad PTS. Detta framgår av 2 kap. 1 § i förening med lagens förordnings 2 §. Lagringen i dessa nät bygger alltså på tanken att operatörerna har ett samhällsansvar att bistå de brottsbekämpande myndigheterna.[47] De insamlade uppgifterna delas in i olika kategorier och förklaras i nästa stycke. Några exakta gränserna mellan dessa är svåra att dra vilket renderar en viss överlappning

[43] Skr. 2017/18:69 s. 30–31, SOU 2015:31 s. 87, prop. 2018/19:86 s. 15, 27.
[44] Prop. 2002/03:110 s. 1 och prop. 2018/19:86 s. 13.
[45] SOU 2017:75 s. 19.
[46] Prop. 2019/20:15 s. 15 och prop. 2010/11:46 s. 43.
[47] Prop. 2019/20:64 s. 178 och prop. 2018/19:86 s. 110.

kategorierna emellan.[48] Iain Cameron framhåller att i Sverige, precis som i många andra europeiska länder, har datalagring vid telekommunikation fram till relativt nyligen setts som ett mindre hot mot den personliga integriteten jämfört med lagring av innehållet i kommunikationen. Framväxten av internet och speciellt smart phones har dock förändrat detta.[49] Nedan följer de tre uppgiftkategorierna.

- Abonnemangsuppgift är ett omdiskuterat begrepp. Ursprungligen härstammar definitionen från den gamla telelagen och tanken var att dessa uppgifter skulle motsvara de som fanns i dåtidens telefonkataloger.[50] Då EU-rätten inte ger ledning i frågan är abonnemangsuppgiften definierad utifrån den nationella rätten.[51] Kammarrätten i Stockholm har i en dom från 2018 konstaterat att abonnemangsuppgifter, utifrån 6 kap. 20 § första stycket 1 LEK utgörs av bland annat uppgifter om namn, adress och abonnentnummer.[52] Till abonnemangsuppgifter brukar även räknas information om fakturering och avtal, uppgift om vem som har använt en fast eller dynamisk IP-adress, (ett nummer som används som en enhetsadress på internet då data sänds genom den tekniska standarden Internet Protocol) eller ett så kallat IMSI-nummer (ett nummer kopplat till en abonnents sim-kort). Dock omfattas inte uppgifter om vilka IP-adresser som har kommunicerat med varandra eller vilka hemsidor som har besökts. Då IP-adressen alltså hänför sig till en internetuppkoppling anses dess huvudsakliga syfte vara att identifiera en abonnent och i förarbetena liknas dessa därför med en postadress för vanliga brevförsändelser.[53]

- Trafikuppgifter eller trafikdata avser de uppgifter som behandlas för att förmedla ett elektroniskt meddelande i ett elektroniskt kommunikationsnät eller av praktiska skäl för att fakturera ett sådant meddelande vilket framgår av 6 kap. 1 § LEK.[54] Trafikdata avser således, något förenklat, uppgifter som behandlas i tekniska system som överför kommunikation. Identitetsuppgifter för innehavare av SIM-kort är ett exempel på en trafikuppgift.[55] Dessa fyller flera syften i underrättelseverksamhet och kan vara lika värdefull för myndigheterna som själva innehållet i kommunikationen. Trafikdata kan nämligen skapa en bild för myndigheterna över nätverk av

[48] Prop. 2018/19:86 s. 13 jfr artikel 2 och 6 i E-Privacy-direktivet.
[49] Cameron (2015) s. 136, jfr Cameron (2010) s. 477.
[50] Prop. 2018/19:86 s. 92–94, prop. 2002/03:110 s. 271, prop.1992/93:200 s. 164, 310.
[51] Prop. 2018/19:86 s. 93–94. Dock har definitionen av IP-adresser tydliggjorts genom EU-domstolens dom C-511/18, C-512/18 och C-520/18, 2020-10-06, vilket behandlas i kap. 6.
[52] Kammarrätten i Stockholm mål 2471–18, dom 2018-12-14. Jfr motsvarande resonemang i prop. 2011/12:55 s. 101–102, prop. 2018/19:86 s. 12–13, 93 ff. och SOU 2017:75 s. 19.
[53] Prop. 2018/19:86 s. 12–13, 93–94 och SOU 2017:75 s. 19.
[54] Prop. 2018/19:86 s. 12, Naarttijärvi (2013) s. 269, Kelleher m.fl. (2018) s. 481–486.
[55] Naarttijärvi (2013) s. 269, 271 & C-207/16, Ministerio Fiscal, EU:C:2018:788, p. 41–42.

individer liksom deras kommunikationsmönster och analyser över tid kan skapa en uppfattning om hierarkin inom ett nätverk. En ökad samtalsfrekevens kan vara ett indicium om en stundande planering av en gärning och ett stort antal samtal till en viss person kan tyda på att denna person utgör en central figur inom organisationen. Genom lagring kan därför okända men intressanta individer identifieras och detta kan vara ett första steg till ett senare eventuellt inhämtningsbeslut, vilket innebär att data ska lämnas ut till de brottsbekämpande myndigheterna. Teknikkunniga kriminella grupperingar försöker många gånger dölja sina ”elektroniska fotspår” genom byte av utrustning och nummer, men trots detta så kan insamlade trafikuppgifter alltså vara värdefullt för att hitta tillbaka till de individer som har varit föremål för spaning.[56]

- Lokaliseringsuppgift är en uppgift om var en viss teknisk utrustning befinner eller har befunnit sig och definieras mer ingående i 1 kap. 7 § LEK. Det kan till exempel röra sig om vilken antenn på en så kallad basstation som utrustningen har kopplat upp sig mot. Polisen kan på så vis lokalisera var en okänd användare av en telefon har kommunicerat med andra telefoner, och detta tillsammans med annan information, som exempelvis bilder från övervakningskameror, kan hjälpa till att identifiera telefonens innehavare. Uppgifterna kan även bevisa eller vederlägga vittnesmål och kartläggningen av rörelsemönster kan ligga till grund för användning av tvångsmedel som husrannsakan, liksom eventuellt koppla en person till andra platser och händelser som rör gärningen, exempelvis stöld av en flyktbil eller inköp av ett vapen.[57] Avigsidan med lokaliseringsuppgifter är att en användning av dessa förutsätter att telefonen är påslagen, och Säpo påpekar att så är sällan fallet precis då ett brott utförs. En annan aspekt är kvalitén på de uppgifter som lagras. I flera av Säpos utredningar har lokaliseringsuppgifterna varit för oprecisa för att vara avgörande när det gäller att knyta en person till ett visst område.[58] Trots dessa aspekter värderas uppgifterna mycket högt av de brottsbekämpande myndigheterna.

I detta sammanhang ska ett förtydligande gentemot en närliggande, i dagarna omtalad, författning göras. Den tekniska utvecklingen har nämligen medfört nya hinder för de brottsbekämpande myndigheterna, och hit hör bland annat kryptering som innebär att innehållet i meddelanden är oåtkomligt för utomstående.[59] Sedan 1 april 2020 finns därför regler i lag (2020:62) om hemlig dataavläsning som gör det möjligt för de brottsbekämpande myndigheterna att ta sig in i teknisk utrustning avsedd för elektronisk kommunikation, exempelvis mobiltelefoner. Detta får användas

[56] Naarttijärvi (2013) s. 269. Se även Ogorek (2021), NJW 2021, 531 s. 547–548.
[57] Prop. 2018/19:86 s. 12–13, 41, Naarttijärvi (2013) s. 277, SOU 2017:75 s. 19 och prop. 2019/20:64 s. 72.
[58] Prop. 2019/20:64 s. 72.
[59] SOU 2015:31 s. 85 och prop. 2018/19:86 s. 16.

i vissa förundersökningar, i underrättelseverksamhet samt vid särskild utlänningskontroll och enbart vid särskilt grov brottslighet. Vid sidan av de ovan beskrivna lokaliseringsuppgifterna finns positioneringsinformation många gånger i själva utrustningen, såsom exempelvis i en mobiltelefon och det är för att ta del av det senare som hemlig dataavläsning används. Fördelen är att dessa positioneringsuppgifter många gånger är mycket mer precisa än de lokaliseringsuppgifter som hämtas in från teleoperatören. Samtidigt har regeringen framhållit att varken hemlig dataavläsning, eller andra nämnda hemliga tvångsmedel eller polisiära metoder såsom fysisk spaning, kan ersätta teleoperatörernas datalagring, utan menar istället att de olika metoderna ska ses som komplement till varandra.[60]

2.3 Tillgång till lagrade uppgifter

Som nämnt under avgränsningar kommer den fortsatta redogörelsen inte att fördjupa sig i lagringens andra steg, myndigheternas tillgång till uppgifter, såvida det inte krävs för att förstå lagringsmomentet i sitt sammanhang. Här ska därför ett förtydligande om systematiken bakom lagring respektive tillgång göras. Vissa av de ovan listade uppgifterna medger tillgång direkt för de brottsbekämpande myndigheterna medan andra kräver domstolsbeslut. Detta speglar sig i hur mycket information som själva lagringen ger. Tillgången är därför beroende av vilken typ av uppgift det rör sig om och i vilket syfte som denna har begärts av myndigheten. Inom både underrättelse- och brottsbekämpande verksamhet används hemliga tvångsmedel och tillgång till datalagring kan ges med stöd av reglerna om hemlig övervakning av elektronisk kommunikation i enlighet med 27. kap rättegångsbalken. Gällande tillgången till trafik-och lokaliseringsuppgifter regleras detta i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Dessutom finns bestämmelser i lagen (1991:572) om särskild utlänningskontroll och i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, som båda hänvisar till rättegångsbalkens bestämmelser. Vid brottsutredande verksamhet krävs domstolsbeslut för att tillgå trafik-och lokaliseringsuppgifter och detta beviljas endast vid allvarlig brottslighet. Huvudregeln gällande underrättelseverksamhet däremot är att domstolsbeslut inte fordras i inhämtningslagen, dock medför detta att tillgången till trafikuppgifter är mer begränsad.[61] Att inhämtningen av trafikuppgifter kräver lagstöd framgår även av Europadomstolens praxis.[62]

Rörande abonnemangsuppgifter har möjligheten att tillgå dessa funnits under en lång tid vilket har motiverats med att de brottsbekämpande

[60] Prop. 2019/20:64 s. 55, 72, prop. 2018/19:86 s. 15.
[61] Prop. 2018/19:86 s. 13–14, 97, SOU 2017:75 s. 18, 20 och JUNO internet, lag (2003:389) om elektronisk kommunikation 6 kap. 16 a § JUNO, not 290, 2021-02-20.
[62] Malone v. the United Kingdom, no 8691/79, ECHR 1984-VIII p. 63 ff, angående internettrafik se Copland v. United Kingdom, no 62617/00, ECHR 2007-IV, p. 29 ff, gällande lokaliseringsuppgifter se Uzun v. Germany, no 35623/05, ECHR 2010-IX p. 33 ff.

myndigheterna av utredningsskäl är i stort behov av uppgifterna.[63] Tillgång till dessa har inte bedömts utgöra ett hemligt tvångsmedel och därför regleras frågan direkt i LEK. Det krävs alltså inte domstolsbeslut för att tillgå abonnemangsuppgifter utan dessa får den brottsbekämpande myndigheten besluta om på egen hand.[64] Tillgången regleras i 6 kap. 22 § första stycket 2 LEK, och sedan en lagändring 2012 krävs inte längre att fängelse ska vara föreskrivet för brottet i fråga, utan numera räcker det att det föreligger misstanke om brott.[65] Eftersom det är lättare för de brottsbekämpande myndigheterna att få tillgång till abonnemangsuppgifter jämfört med övriga uppgifter, blir därför definitionen av vad som ska innefattas av begreppet, ur en integritetsaspekt, avgörande. Kritik har riktats mot att definitionen av abonnemangsuppgifter härstammar från den daterade föregångaren till LEK. Detta eftersom de uppgifter som sorteras under abonnemangsuppgifter idag, på grund av nuvarande teknik, är mer omfattande och integritetskänsliga jämfört med vad som innefattades i uppgiftstypen vid införandet av begreppet i 1993 års lag.[66]

2.4 Komparativ utblick – brottsbekämpning och elektronisk kommunikation i Tyskland

Precis som i Sverige är de brottsbekämpande myndigheterna i Tyskland i stort behov av information för att kunna fullgöra sina uppgifter.[67] Enligt en grundläggande organisatorisk princip, das Trennungsgebot, görs en uppdelning mellan de olika förbundsstaternas polisväsende och den federala polisiära verksamheten respektive underrättelse-och militärväsendet. Hans Peter Bull menar att åtskillnaden mellan underrättelse- och polisverksamhet ska förhindra framväxten av en ”övermäktig stat” och ett nytt Gestapo. En följd av nämnda princip är att respektive myndighet, som huvudregel, enbart ska samla in så pass mycket information som den behöver, även om ett visst informationsutbyte dessa emellan måste ske. Gällande datalagring, Vorratsdatenspeicherung (VDS), hos teleoperatörer regleras denna federalt genom Telekommunikationsgesetz, TKG.[68] Detta kommer att beskrivas tillsammans med den svenska gällande rätten i kapitel 6.

2.5 Datalagringens påverkan på privatlivet

Som beskrivet i det här kapitlet är de brottsbekämpande myndigheterna i behov av lagrade uppgifter. Samtidigt inkräktar lagringen på den enskildes

[63] Kammarrätten i Stockholm mål 2471–18, dom 2018-12-14.
[64] SOU 2017:75 s. 20, prop. 2018/19:86 s. 14 och 95, prop. 2011/12:55 s. 102–103.
[65] Kammarrätten i Stockholm mål 2471–18, dom 2018-12-14, prop. 2011/12:55 s. 144–145.
[66] Prop. 2018/19:86 s. 92.
[67] Bull (2009) s. 81 ff.
[68] Kutscha (2006) s. 337–338, Bull (2009) s. 100–103, Ipsen (2019) s. 17.

rätt till att få kommunicera privat.[69] Integritetsskyddskommittén[70] menade att polisverksamheten per definition är kränkande för den personliga integriteten hos dem som utsätts för polisiära åtgärder och detta är i synnerhet fallet då behandlingen sker på grund av felaktiga misstankar. Vidare framhölls vikten av ett tydligt regelverk så att både den enskilde och polisen i sin praktiska verksamhet är medvetna om hur personuppgifter får användas.[71] Integritetsskyddskommittén har framhållit att det utifrån flera undersökningar har framkommit att den enskilde tycker att det är viktigt hur personuppgifter hanteras. I en europeisk undersökning rörande inställningen till personlig integritet genomförd år 2015, tog 52 procent av de svenska deltagarna avstånd från påståendet ”att lämna ut personlig information är inget problem för dig”.[72]

En annan aspekt är att lagstiftning som medför inskränkningar i integritetsskyddet till förmån för bland annat nya spaningsmetoder riskerar att mötas av misstro hos allmänheten om den inte motiveras på ett övertygande vis. Generella övervakningsmetoder, som exempelvis lagringsskyldighet av teletrafikuppgifter, anses ur integritetshänseende vara allvarligare än riktade åtgärder mot utpekbara grupperingar. Detta eftersom generella åtgärder i större utsträckning ”riskerar att hos befolkningen inge en föreställning om att leva i ett kontrollsamhälle” och kan innebära ett ändrat beteendemönster.[73] Här kan en parallell dras till de olika regler som råder för trafik-och lokaliseringsuppgifterna å ena sidan, respektive abonnemangsuppgifterna å andra sidan, det vill säga att riktade åtgärder som hemliga tvångsmedel föregås av en domstolsprövning, och bara sker vid misstanke om att brott av en viss svårighetsgrad planeras eller har utförts. Detta gör att den berörda gruppen är mycket snävare jämfört med de som omfattas av en generell lagring som utgörs av alla abonnenter.

I nästföljande kapitel redogörs för skyddet av den personliga integriteten som bärs upp av de ”tre benen”: det nationella konstitutionella systemet liksom det EU- och europarättsliga med därtill knuten rättspraxis.[74] Utgångspunkten är att såväl regeringsformen som Europakonventionen och EU:s rättighetsstadga sätter upp krav för vad som kan anses vara godtagbara åtgärder trots att dessa inkräktar på skyddet av den personliga integriteten. Åtgärden måste då vidtas för ett ändamål som är godtagbart i ett demokratiskt samhälle, vara objektivt sett ägnad att uppnå syftet med åtgärden och vara proportionerlig. Det ska visas vilken betydelse en åtgärd som medför intrång i integriteten kan ha för att nå målet att stävja och lagföra brott.[75] Då den elektroniska kommunikationen idag har en så pass

[69] Jfr prop. 2018/19:46 s. 40 och Prölss-Peter (1986) s. 65–82.
[70] Tillsattes år 2004, dir. 2004:51 med uppdraget att bland annat kartlägga och analysera lagstiftning rörande den personliga integriteten samt föreslå ny grundlagsreglering. Se SOU 2007:22, SOU 2008:3. Kommitténs förslag inarbetas i SOU 2008:125.
[71] SOU 2007:22 s. 211.
[72] Special Eurobarometer 431, Data Protection, se vidare analys i SOU 2016:41 s. 55.
[73] SOU 2007:22 s. 469 och s. 477 jfr SOU 2017:52 s. 19 ff.
[74] Bull (2013a) s. 295.
[75] Prop. 2018/19:86 s. 13–14.

central plats i samhället utgör den en scen där principiella konflikter mellan staten och den enskilde utspelar sig.[76]

[76] Derlén m.fl. (2016) s. 315.

3 Regler till skydd för den personliga integriteten

3.1 Begreppet personlig integritet

Personlig integritet betyder okränkbarhet och det som utmärker begreppet är att rätten till denna inte upphör bara för att en individ inte förmår hävda denna rättighet på egen hand.[77] Integritetsskyddskommittén anförde att en utredning av *vad* som avses med begreppet personlig integritet har sina begränsningar eftersom en sådan begreppsanalytisk infallsvinkel faller på att det är nästintill omöjligt att ge ett allmänt accepterat svar på vad som avses med begreppet. Att definiera innebörden är svårt utan att samtidigt ta ställning till ”omfattningen och tyngden av de motstående legitima intressen som kan finnas, såsom intresset av offentlighet och brottsbekämpning.” [78] Förenklat sagt är definitionen inte entydig och på området finns det material nog för att skriva en avhandling.[79] Följande kapitel ämnar till att ge en bakgrundsbild och en förståelse av begreppets komplexitet, detta eftersom det utgör en väsentlig avvägningsaspekt vid datalagring.

I skymundan av just frågan om *vad* som avses med begreppet personlig integritet, har frågan om *varför* detta är skyddsvärt hamnat.[80] En anledning kan vara att det idag betraktas som en självklarhet att rätten till personlig integritet är en grundläggande rätt i en demokrati. Detta skulle kunna förklara varför motiven till varför denna rätt föreligger inte har beskrivits på något fullständigt vis i förarbeten eller grundlag. I motiven till den reformerade regeringsformen konstaterades kort och gott att en utredning av begreppet inte har något egenvärde.[81] Utgångspunkten har varit att försöka “förbjuda sådana företeelser som inte ansetts försvarbara med hänsyn till dels den skada de skulle innebära för den personliga integriteten, dels den skada som ett upprätthållande av integriteten skulle åsamka andra beaktansvärda intressen.”[82] Även om konturerna är suddiga kan konstateras att en central del av begreppet är att den enskilde ska kunna ha en avgränsad och skyddad kommunikation. Detta inbegriper bland annat att individen själv ska kunna styra över vad denne väljer att delge sin omgivning.[83] Ett sådant skydd har givetvis ett värde för individen som sådan, men i takt med IT-samhällets frammarsch har även andra aspekter lyfts fram och detta genom att påtala dess koppling till andra samhälleliga skyddsvärden. Rätten till personlig integritet har därför inte enbart kommit att betraktas som en individuell rättighet, utan även som en rättighet som reglerar förhållandet

[77] Prop. 2005/06:64 s. 35 och SOU 2008:3 s. 208.
[78] SOU 2007:22 s. 52.
[79] Se bl.a. SOU 2007:22 s. 63, prop. 2009/10:80 s. 175 och Strömholm (1980) s. 30 ff.
[80] Naarttijärvi (2013) s. 222–223.
[81] Prop. 2009/10:80 s. 175 och 185. SOU 2008:3 s. 97, 204–206. Jfr SOU 2016:41 s. 39.
[82] SOU 2007:22 s. 52.
[83] Naarttijärvi (2013) s. 231–234 & Westin (1968) s. 37–38 jfr Strömholm (1980) s. 23-39.

mellan staten och medborgarna med inneboende långtgående konsekvenser för rättsstatliga aspekter som frihet och demokrati.[84] Hornung och Schnabel uttrycker detta samspel som: "The protection of personal data is essential for a free and self-determined development of the individual. At the same time, the self-determined development of the individual is a precondition for a free and democratic communication order."[85] Teknikutvecklingen och de diskussioner som har följt i dess spår har därför bidragit med en ny förståelse av integritetsbegreppet.[86]

Ur en mer rättshistorisk synvinkel lyfter Naarttijärvi fram att privatlivet inte har värderats högt hos de som ser detta som en individualism som är ett "uttryck för en snobbig, elitistisk eller ultraliberal hållning som misstänkliggör politiska och sociala institutioner."[87] Det är allmänt känt att totalitära regimer inte värdesätter en personlig integritet, utan att bristen på detta fungerar som ytterligare ett maktmedel och där övervakningen är ett led i att bryta ner befolkningen.[88] En mer modern tendens med teknikutvecklingen belyses av Thomas Bull som efterfrågar en konstitutionell debatt om integritetsbegreppet. Han menar nämligen att det moderna samhället genomsyras av en paradoxal inställning till den personliga integriteten: samtidigt som tekniken har medfört en enkel kommunikationskanal för enskilda har den även inneburit risk för integritetsintrång. Sambandet har en politisk sprängkraft eftersom Bull ser en ökande känslighet för integritetsintrång och ”kränkningar” (Bulls citering), samtidigt som detta åtföljas av en "starkt ökande" exponeringsvilja för omvärlden. Slutsatsen Bull drar är att den "integritetsvåg" som sköljer över samhället inte lämnar beslutsfattare oberörda, men menar att samhället bör motstå frestelsen att följa med vågen och istället i varje enskild situation kritiskt fråga om påstådda hot mot personlig integritet *verkligen* föreligger".[89]

Ett annat modernt fenomen, som i den allmänna debatten utgör ett ständigt återkommande argument för att låta statens behov av insamling av tele-och internettrafik gå före den personliga integriteten, utgörs av det så kallade "jag har inget att dölja"-argumentet. Detta implicerar att man inte behöver oroa sig för övervakning om man inte har några direkta hemligheter. Personlig integritet utifrån detta synsätt handlar om att dölja eventuella fel man har begått. Solove menar att argumentet bygger på tanken att de myndigheter som hämtar in informationen är ofelbara. En annan synpunkt han för fram är att det finns otaliga historiska exempel på att det som anses harmlöst idag kan vara något som staten inte ser på med blida ögon imorgon.[90] Gällande just ”harmlösa uppgifter” framhåller Strömholm att den

[84] Solove (2011) s. 47 ff, Naarttijärvi (2013) s. 230 och Bull (2009) s. 7–21, 59–61.
[85] Hornung och Schnabel (2009) s. 85.
[86] Naarttijärvi (2013) s. 230.
[87] Naarttijärvi (2013) s. 231, citatet är hans fria översättning och tolkning av Gutwirth (2002) s. 51–52. Se vidare Gutwirth kapitel 3: *Ambiguous Privacy*.
[88] Modeér (2009) s. 49 och Westin (1968) s. 22–23 jfr Derlén m.fl. (2016) s. 315, Bogdan (2003) s. 173–181 om det socialistiska rättssystemet, Naarttijärvi (2013) s. 231.
[89] Bull (2013a) s. 305–306.
[90] Solove (2011) s. 21, 32 och 209 om "The -Nothing -to -Hide-Argument."

typen av uppgifter, tillsammans med annan i och för sig oskadlig information, kan ge en samlad kunskap om den person vars uppgifter har lagrats.[91] Även Naarttijärvi är kritisk och menar att privatlivet inte kan betraktas som en individuell rättighet, frånkopplat från de samhällseffekter som övervakningsåtgärder medför. Han menar att det finns en tendens bland de individer som inte tillhör en utsatt grupp i samhället att se på vissa rättigheter som "andra människors rättigheter".[92] Detta bygger på ren psykologi: finns det ingen större risk att du själv eller anhöriga kommer att behöva hävda en rättighet, kommer du med största sannolikhet värdera fysisk säkerhet högre. Ludvig Beckman menar att demokrati därför fordrar "ett visst mått av trygghet" och att osäkerhet kan hämma en individs engagemang. En annan aspekt av denna "rent-mjöl i påsen"-syn är att den innebär en felaktigt placerad bevisbörda enligt Naarttijärvi, detta eftersom det gör att individen ska påvisa sin oskuld när det egentligen är staten som borde visa på en legitim anledning att fråga.[93] Det står alltså klart att begreppet personlig integritet är mångfacetterat. För läsarens del är förhoppningen att en större förståelse för begreppets komplexitet som avvägningsaspekt har vunnits. Nedan följer en kortfattad historisk tillbakablick på grundläggande rättigheter för enskilda och därefter följer nuvarande reglering av den personliga integriteten.

3.2 Historisk bakgrund

3.2.1 Framväxt av rättighetskataloger i väst

Föreställningen om att den enskilde ska ha vissa grundläggande fri- och rättigheter gentemot statsmakterna är inte ny. Upplysningstankarna och de rättigheter som framgår av *Habeas Corpus Act* från 1679 och *Bill of Rights* från 1689 har haft stor inverkan på den senare rättsutvecklingen på området. Likaså den klassiska *Déclaration des droits de l'homme et du citoyen*, från 1789 och rättighetstilläggen till *United States Bill of Rights* från 1791 har i hög grad påverkat utvecklingen i andra länder, med följden att allt fler rättighetsförklaringar tillkom under 1800-och 1900-talen. De tidigaste rättighetskatalogerna var inriktade på främst civila och politiska rättigheter för att senare under 1900-talet, övergå till mer socialt orienterade sådana, även om dessa i allmänhet inte var rättsligt bindande utan istället utgjorde målsättningsstadganden. Den moderna utvecklingen präglas i stor utsträckning av internationellt samarbete som har gett upphov till folkrättsligt bindande konventioner.[94]

[91] Strömholm (1980) s. 35, Strömholm (1971) s. 709–710.
[92] Naarttijärvi (2013) s. 240.
[93] Naarttijärvi (2013) s. 238–241 och Beckman (2004) s. 494.
[94] SOU 2008:125 s. 385–386, Sterzel (2015) s. 86. Se även Strömholm (1971) s. 695 ff.

3.2.2 Utvecklingen av ett svenskt integritetsskydd

Sedan långt tillbaka har det funnits bestämmelser tänkta att tillskriva den enskilde vissa rättigheter och på så vis skydda denne från statsmakternas godtycke. Redan landslagens konungaed stadgade att kungen skulle "styrka rättvisa och sanning och nedtrycka vrångvisa, osanning och orätt…".[95] Detta skydd påverkade i sin tur utformningen av hemfridsskyddet i 16 § i 1809 års regeringsform, även om detta inte betraktas som ett regelrätt skydd för medborgerliga fri-och rättigheter. Till exempel saknades ett skydd för förtrolig kommunikation såsom post-och telefonhemlighet.[96]

I ljuset av den politiska utvecklingen i Europa under 1930-talet aktualiserades frågan om regeringsformen 1809 skulle få ett förstärkt skydd, men inget av de förslag på nya rättigheter i dess 16 § realiserades. Det var först med ikraftträdandet av 1974 års regeringsform och 2 kap. 6 § som ett uttryckligt skydd för den personliga integriteten infördes. Detta trots att ett sådant integritetsskydd tillkom genom undertecknandet av Europakonventionen år 1952. Av paragrafen framgår bland annat att var och en är skyddad mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Hur bestämmelsen och dess motiv har tolkats utifrån senare års utveckling av den elektroniska kommunikationen kommer att behandlas i avsnitt 4.5.2.[97]

Sedan 1976 gäller även det allmänna målsättningsstadgandet i 1 kap. 2 § RF om att den offentliga makten ska utövas med respekt för den enskildas frihet och värdighet. Genom tillägget i paragrafens fjärde stycke framgår att det allmänna ska värna den enskildes privatliv och familjeliv, även om detta alltså inte har någon bindande verkan för det allmänna och därmed inte ger upphov till individuella rättigheter. Däremot bekräftas att myndigheterna i möjligaste mån bör beakta den enskildes integritet så långt detta är möjligt i förhållande till andra lagstadgade skyldigheter.[98] Gällande integritetsskyddet på dataskyddsområdet övervägdes under 1980-talet att ge detta en tydligare förankring i RF. Föredragande statsråd ansåg dock att det var förenat med stora svårigheter eftersom det inte hade gått att ge en klar definition av begreppet personlig integritet och att det inte kunde betraktas som ett statiskt begrepp.[99]

[95] SOU 1941:20 s. 11 och Nergelius (1996) s. 545, historisk tillbakablick se s. 589 ff.
[96] Prop. 1973:90 s. 192, SOU 2007:22 s. 48 jfr Naarttijärvi (2013) s. 205.
[97] Jfr prop. 1975/76:209 s. 123, 147–148 och Lexino/JUNO kommentar till RF (1974:152) 2 kap. 6 § not 27, hämtad 2021-05-15.
[98] SOU 2008:125 s. 387, 470–471, prop. 2009/10:80 s. 173, prop. 1975/76:209 s. 128, 131. Jfr Bremdal (2014) s. 57–68. Vidare diskussion om RF 1:2 följer i nästa avsnitt.
[99] Prop. 1987/88:57 s. 9–11 jfr SOU 2008:3 s. 115–117.

3.3 Rättsutveckling under 2000-talet

3.3.1 RF:s skydd för den personliga integriteten

Genom 2010 års grundlagsrevisionen och tillkomsten av det andra stycket i 2 kap. 6 § RF tillförsäkras att var och en är skyddad mot betydande intrång i den personliga integriteten om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Avgörande för om så är fallet är vilken effekt åtgärden får. I förarbetena förutspåddes att nya metoder för övervakning och kartläggning av enskilda skulle komma till stånd genom den tekniska utvecklingen och det var därför av vikt att grundlagsbestämmelserna inte skulle utgöra ett hinder för framtida lagstiftning till skydd för samhällsintressen, utan istället anpassas så att de enbart skulle omfatta de mest ingripande åtgärderna.[100] Idag framgår av 2 kap. 6 § andra stycket RF att inskränkningar i den personliga integriteten får ske genom lag enligt de förutsättningar som 2 kap. 20–22 §§ RF anger. Detta innebär att en begränsning endast tillåts om den tillgodoser ett ändamål som är godtagbart i ett demokratiskt samhälle, och den får inte gå utöver vad som anses nödvändigt med hänsyn till det bakomliggande syftet som föranledde begränsningen. Därtill får begränsningen inte heller sträcka sig så långt att det inverkar menligt på den fria åsiktsbildningen.[101] Motiveringen till den här tågordningen var att lagstiftaren skulle tvingas att tydligt redovisa de avvägningar som hade gjorts vid en proportionalitetsbedömning. Vidare ansåg regeringen att detta kunde förväntas borga för att avvägningarna i fråga om integritetsintrång i ökande grad skulle bli mer ingående belysta vilket på så vis skulle höja lagstiftningens kvalité.[102] I ett internationellt perspektiv är konstruktionen, med stadgande av möjliga inskränkningar i den enskildes fri-och rättigheter, istället för att dessa har formulerats positivt av lagstiftaren, ovanlig.[103]

Främst premierar den svenska grundlagen den fria åsiktsbildningen, vilket får till följd att skydd från exempelvis brevkontroll och åsiktsregistrering inte primärt ska tillförsäkra medborgarna personlig integritet, utan detta motiveras snarare utifrån att denna fria åsiktsbildning ska skyddas. Det framgår heller inte vilka inskränkningar som får göras från det allmänna i grundlagen, utan detta utläses i vanlig lagstiftning. Många av de i brottsbalken angivna brott mot person, liksom skadeståndslagens bestämmelser om ideellt skadestånd åsyftar att värna den enskildes integritet. Likaså offentlighetsprincipens inskränkningar i form av sekretessbestämmelser lutar sig huvudsakligen mot integritetshänsyn. Därtill ska Europakonventionens rättighetsskydd likväl som det ovan nämnda målsättningsstadgandet i 1 kap. 2 § RF om att det allmänna ska värna den enskildes privatliv, uppfyllas via bestämmelser i vanlig lagstiftning.

[100] Prop. 2009/10:80 s. 182, 250 och JUNO internet RF (1974:152) 2 kap. 6 §, not 28, 2021-03-03. Se även Bull & Sterzel (2019) s. 72–74.
[101] Prop. 2018/19:86 jfr Derlén m.fl. (2016) s. 281–290.
[102] Prop. 2009/10:80 s. 177 jfr SOU 2008:3 s. 190.
[103] Sterzel (2015) s. 88.

Grundlagarna förväntas således genomsyra den vanliga lagstiftningen och fastställer på så vis gränserna för vilka inskränkningar i grundläggande rättigheter som lagstiftaren kan företa.[104]

Generellt gäller att uppgifter som rör den enskilde och behandlas utan dennes vetskap anses utgöra ett större ingrepp i den personliga integriteten än om den enskilde har lämnat ett samtycke till behandlingen. Detta främst eftersom avsaknad av vetskap om vidtagna åtgärder gör att den enskilde inte kan tillvarata sina integritetsintressen. Vid bedömningen av ett eventuellt integritetsintrång ska uppgifternas karaktär och omfattning liksom ändamålet med behandlingen vägas in. Även utlämnandet av uppgifter till andra ska tas med i bedömningen. Den hantering som sker i brottsbekämpande syfte är känsligare jämfört med andra former av hantering hos myndigheter.[105]

Den rådande systematiken i regeringsformen, med en avsaknad av ett generellt skydd för den personliga integriteten, förstås av dess kritiker som ett tecken på att skyddsvärdet av denna är förhållandevis lågt.[106] Integritetsskyddskommittén menade att "en svag förankring av skyddet för den personliga integriteten i grundlagen kan innebära att integritetsskyddsaspekterna inte ges tillräcklig vikt när ny lagstiftning arbetas fram." [107] Inom ramen för sitt kartläggningsarbete har kommittén följt upp effekterna av införandet av paragrafens andra stycke och konstaterar att det är en svårtillämpad bestämmelse och den används på ett skiftande vis i lagstiftningsarbetet. Förståelse saknas för bestämmelsens innebörd och tillämpning och åtgärder för att komma till rätta med situationen presenteras därför av utredningen.[108] Att "integritetsskyddet rent allmänt värderas lågt" framkom även i propositionen till den reformerade grundlagen.[109] Inger Österdahls anser, trots regeringsformens reform, att dess 2 kap. 6 § ger ett rudimentärt skydd.[110] Samtidigt framhåller Fredrik Sterzel att begreppet rättsstatlighet visserligen är godtyckligt, men trots detta menar han att reformen av RF har gett de faktorer som förknippas med detta begrepp en mer framträdande plats.[111] För att se den svenska regleringen från ett annat perspektiv görs en jämförelse med det tyska integritetsskyddet nedan.

[104] SOU 2008:3 s. 207, 247–248 och SOU 2008:125 s. 470 jfr Hiller (2014) s. 133.
[105] Prop. 2009/10:80 s. 178–179, 183 och SOU 2018:65 s. 64.
[106] Integrationsskyddskommitténs kritiska synpunkter se SOU 2008:125 s. 470–471 jfr Naarttijärvi (2013) s. 206. Se även Strömholm (1980) s. 36–37.
[107] SOU 2008:125 s. 470.
[108] Lexino tryckt kommentar till RF (1974:152) 2 kap. 6 § s. 109 & SOU 2017:52 s. 230 ff.
[109] Prop. 2009/10:80 s. 176.
[110] Österdahl (2015) s. 77–78. Nergelius (2014) s. 141 som menar att skyddet är enkelt att kringgå för lagstiftaren.
[111] Sterzel (2015) s. 84–85.

3.4 RF:s integritetsskydd i ljuset av tysk rätt

Mellan raderna kan man från tysk horisont utläsa en vis förvåning över den svenska integritetsregleringen. Hiller menar att det är den svenska synen på offentliga handlingar, som beskrivs som att den bär upp den svenska demokratin (“tragende Säule der Demokratie”) som har påverkat svenskars syn på privatsfären.[112] I tysk rätt däremot spelar individuell autonomi en central roll i identitetsbegreppet.[113] Givet landets historia och Weimarförfattningens brister är det i grundlagen, das Grundgesetz (GG), som antogs 1949, av högsta prioritet att slå vakt om de medborgerliga fri- och rättigheterna.[114] Denna inleds därför med en omfattande rättighetskatalog, die Grundrechte, i art. 1-19.[115] Portalstadgandet slår fast människovärdets okränkbarhet och av art 1 stycke 3 framgår att rättigheterna i grundlagens kapitel 1 binder alla statliga, lagstiftande, verkställande eller dömande myndigheter som omedelbart gällande rätt. Betoningen på detta precis i inledningen är en direkt reaktion på den nationalsocialistiska regimens missaktning av människovärdet.[116] Vidare stadgar artikel 2 en rätt till frihet, liv, kroppslig integritet och en frihet att utveckla sin person så länge detta inte inkräktar på andras rättigheter eller går emot den konstitutionella ordningen. Den generella frihet (allgemeine Handlungsfreiheit) som framgår av paragrafen är ett arv av de franska augustirättigheterna från 1789 och artikeln är ett uttryck för ett generellt skydd för personligheten, allgemeines Persönlichkeitsrecht.[117]

Gällande rätten till telekommunikation och brevhemlighet skyddas detta i artikel 10. Därtill har vissa medborgerliga rättigheter ett så kallat Wesensgehalt, “väsensinnehåll”, vilket innebär att dessa besitter ett okränkbart värde.[118] Begränsningar av de grundlagsskyddade rättigheterna genom lag får därför aldrig inkräkta på deras väsensinnehåll. Det framgår av artikel 19 stycke 2 och det tyska rättsstatsidealet tar sig även uttryck i artikel 19 stycke. 4 om att den vars rättighet har kränkts av någon offentlig myndighet alltid ska ha möjlighet att väcka talan vid tysk domstol. Detta ökar rättighetskatalogens praktiska betydelse. Även artikel 20 stycke 1 och 3, som kortfattat går ut på att landet är en demokrati och att vanlig lag är underordnad och ska överensstämma med grundlagen, utgör viktiga fundament. Grundlagsskyddet förstärks därtill genom artikel 79 stycke 3 som stadgar att de principer som uttrycks i artiklarna 1 och 20 GG är

[112] Hiller (2014) s. 188, jfr Österdahl (2015) s. 74 ff.
[113] Naarttijärvi (2013) s. 224.
[114] Battis m.fl. (1999) s. 2–4, Zekoll & Reimann (2005) s. 53–54. Lindahl (2007) s. 158; § 48 i författningen, ”dikataturparagrafen”, möjliggjorde utfärdande av förordningar i strid med lag och grundlag. Motsvarande brister fanns i Paulskirchenverfassung 1849.
[115] Robbers (2019) s. 39 och Nergelius (2018b) s. 20.
[116] Battis m.fl. (1999) s. 213 jfr Bull (2015) s. 118–119.
[117] Robbers (2019) s. 39, 44, Nergelius (2018b) s. 20, Kuner (2003) s. 184. Se även Strömholm (1971) s. 697, 705 ff.
[118] SOU 2008:3 s. 206–207 och Bull (2015) s. 124–125. En längre analys av teorin om s.k. ”väsensinnehåll”, se Schwan (1984) s. 76–85.

omöjliga att avskaffa ens genom en grundlagsändring. Joakim Nergelius framhåller att det senare får en särskild betydelse genom stadgandet i artikel 1 stycke 2 om att de mänskliga rättigheterna utgör fundamentet i den tyska samhällsordningen.[119]

En skillnad länderna emellan visar sig genom att folksuveränitetsprincipen, som uttrycks i artikel 20, anger att den offentliga makten härstammar från folket och utövas sedan av valda, verkställande eller rättstillämpande organ. Thomas Bull menar att i Sverige däremot uppfattas ofta domstolarnas makt som ett hot mot folksuveräniteten medan domstolarna alltså ses som en del av denna i Tyskland. En av dessa, Bundesverfassungsgericht, författningsdomstolen, har spelat en central roll i utvecklandet av det starka skyddet för den personliga integriteten. Då någon av de ovan beskrivna "grundrättigheterna" inklusive artikel 20 har kränkts, kan nämligen den enskilde anhängiggöra ett författningsbesvär till författningsdomstolen enligt artikel 93 stycke 1 punkt 4a.[120] Denna har mandat att pröva vanlig lag i förhållande till rättigheterna i grundlagen. Artikel 92 i GG utrycker att författningsdomstolen är en av landets övriga domstolar, dock framgår av 1 § i Bundesverfassungsgerichtsgesetz att författningsdomstolen, till skillnad från övriga, är ett författningsorgan vilket alltså är ett uttryck för maktdelningsprincipen.[121] År 1983 slog domstolen fast att det finns en konstitutionell rätt till "informationssjälvbestämmande", informationelle Selbstbestimmung. Domstolen menade att trots att det inte framgår explicit av grundlagens artikel 1 och 2 har individen en sådan bestämmanderätt eftersom personlighetsrätten ger individen en rätt att självständigt utforma sin personlighet och detta innefattar en rätt för den enskilde att på egen hand avgöra vilken information som ska kommuniceras till andra.[122] Hiller menar att det inte finns något motsvarande den tyska, mer eller mindre heltäckande "personlighetsrätten" i svensk rätt. Även i Tyskland görs avvägningar mellan personlighetsrätten och andra rättigheter men trots detta menar hon att integriteten skyddas effektivare när den som i tysk rätt är en fristående rättighet som ställs mot en annan rättighet jämfört med om den utgör en avvägningsaspekt som i Sverige. Hiller menar att utformningen av 1 kap. 2 § RF medför att bestämmelsen är utan rättslig verkan för den enskilde, till skillnad från den tyska regleringen som alltså medger ett direkt skydd.[123] Likaså säger Nergelius "att åberopa bestämmelsen inför domstol torde exempelvis normalt vara utsiktslöst" och även Hirschfeldt menar att stadgandet inte ger "upphov till några rättigheter för den enskilde på samma sätt som t.ex. reglerna om grundläggande fri-och rättigheter i 2 kap. RF och

[119] Nergelius (2018b) s. 20–21 och Nergelius (1996) s. 207–208.
[120] Bull (2015) s. 119, 124 jfr Nergelius (1996) s. 208.
[121] Wennerström (1999) s. 82–83 och Nergelius (1996) s. 225.
[122] BVerfG 1 BvR 209/83 1983-12-15, 1983-12-15. Se även Robbers (2019) s. 44, Gutwirth, (2011) s. 5, Naarttijärvi (2013) s. 186, 232, Foster m.fl. (2010) s. 241–243, Knott (1986) s. 45–63. Se även Deutscher Bundestag, Drucksache 17/8999, 17. Wahlperiode 15. 03. 2012 s. 24 ff.
[123] Hiller (2014) s. 101–103, 133 jfr Nergelius (2018a) s. 139 och där vidare angivna hänvisningar till Nyman och Holmberg/Stjernquist. Se även Warnling Conradson m. fl. (2018) s. 59: "den enskilde kan ha svårt att göra sin "rätt" enligt lagrummet gällande…".

har som sagts inte ansetts juridiskt bindande."[124] Hirschfeldt nyanserar dock bilden och framhåller att den har fått en viss materiell betydelse i rättstillämpningen. Enligt Hirschfeldt får därför rambestämmelsen en "egentlig rättslig betydelse" trots att den alltså vid tillkomsten inte ansågs vara rättsligt bindande.[125] Bremdal framhåller att det är en risk för att den enskilde tappar respekten för grundlagen om den enbart består av "tomma ord" och i motsats till Nergelius menar han därför att även om stadgandet inte är direkt åberopbart får det betydelse i tolkningen av andra rättsregler. Bremdal menar därför att domstolar och andra rättstillämpare bör följa den riktning som stagandet markerar.[126]

Därtill menar Thomas Bull att även om grundrättigheterna i GG inte kan åberopas i ett direkt rättsförhållande mellan enskilda påverkar de tolkningen av privaträttsliga regler. Samtidigt kan sägas att ett bindande normativt instrument, som reglerna i den tyska grundlagen utgör, är något som skiljer Tyskland från andra länder där dessa bestämmelser istället utgör en politisk deklaration.[127] Gällande frågan om författningsdomstolen påpekar Sterzel att den ligger nära den svenska lagprövningsrätten som regleras i 11 kap. 14 § respektive 12 kap. 10 § RF. Han menar dock att "det starkt kan ifrågasättas om det finns underlag i vårt lilla land för en sådan domstol".[128] Till sist ska sägas att Bogdan framhåller att rättsordningens utformning sker under stark påverkan av landets historia.[129] Som framgår är detta framträdande i den tyska grundlagen med sin starka humanistiska prägel. Synsättet länderna emellan skiljer sig åt och i stort stöds en teori om att fri-och rättigheter primärt ska skydda den enskilde mot staten i den tyska rätten.[130] Hiller å sin sida konstaterar kort och gott att det svenska skyddet är betydligt svagare än det tyska.[131]

Den fortsatta framställningen i detta kapitel tar sikte på att beskriva Sveriges europarättsliga åtaganden när det gäller den personliga integriteten, därefter följt av det grundläggande regelverk som EU-rätten ställer upp.

[124] Hirschfeldt (2014) s. 39–41 och Nergelius (2018a) s. 139.
[125] Hirschfeldt (2014) s. 39–41, redogör där för praxis från HD liksom JO- och JK:s rättsliga tillsynsverksamhet.
[126] Bremdal (2014) s. 67. Vidare om rättsligt bindande aspekter och politik se även Wenander (2011) s. 548–551.
[127] Bull (2015) s. 124 och 139.
[128] Sterzel (2009) s. 66 och Sterzel (2015) s. 85.
[129] Bogdan (2003) s. 69. Se även Löw (1994) s. 7–9.
[130] Nergelius (1996) s. 249.
[131] Hiller (2014) s. 133.

3.5 Personlig integritet enligt Europarådets konventioner

3.5.1 Europakonventionen

I enlighet med den dualistiska synen på folkrättens förhållande till den inomstatliga rätten, blir denna gällande först efter att den har införlivats i nationell rätt. Europakonventionen, EKMR, är ett av de viktigaste folkrättsliga dokument vad gäller skyddet av den personliga integriteten och tack vare Europadomstolens långvariga rättspraxis har den en särställning bland andra traktater.[132] Den är inkorporerad genom 2 kap. 19 § RF som stadgar att lag eller annan föreskrift inte får meddelas i strid med denna. Trots undertecknandet 1952, var det för den enskilda medborgaren omöjligt att åberopa konventionen inför svensk domstol, vilket ändrades genom införandet av lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och grundläggande friheterna. Sedan 1995 gäller därför konventionen som svensk lag.[133] Konstruktionen innebär att EKMR har en särställning mellan vanlig lag och grundlag och detta möjliggör en lagprövning av svensk lag i förhållande till konventionen. I doktrin framhålls därför att den delvis har fått konstitutionell status.[134] Thomas Bull menar att europarätten har stärkt det nationella konstitutionella regelverket vilket har gett regeringsformens rättighetsskydd nytt liv. Ett tecken på det är att regeringen, i samband med grundlagsreformen, anförde att landets trovärdighet som fördragsslutande part till EKMR skulle öka om den personliga integriteten fick en tydligare förankring i RF.[135]

Den i arbetet inledningsvis nämnda statliga skyldigheten att skydda enskildas privatliv mot intrång, liksom att eventuella brott utreds, kan härledas till EKMR artikel 8 där det framgår att var och en har rätt till skydd för sitt privat-och familjeliv, sitt hem och sin korrespondens. Vidare anges att en offentlig myndighet enbart får ingripa i denna rättighet om den har lagstöd för detta och om det dessutom bedöms vara nödvändigt i ett demokratiskt samhälle med hänsyn till nationell säkerhet, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.[136] Kort sagt ska en proportionalitetsbedömning göras. Det är institutet *margin of appreciation, bedömningsmarginalen,* som sätter gränserna för vilka inskränkningar som får göras i konventionsrättigheterna vilket alltså påverkar bedömningen.[137] Naarttijärvi konstaterar att det av

[132] Formell beteckning se avsnitt 1.4 ovan. Nergelius (1996) s. 609, Bull (2013a) s. 295. Se även Internationell konvention om medborgerliga och politiska rättigheter, New York den 16 december 1966, SÖ 1971:42 jfr prop. 2019/20:64 s. 35, Naarttijärvi (2013) s. 188.
[133] Prop.1993/94:117 s. 6, prop. 2009/10: 80 s. 127 och Nergelius (1996) s. 609–610.
[134] Naarttijärvi (2013) s. 189.
[135] Prop. 2009/10:89 s. 176 och Bull (2013b) s. 79 jfr Bernitz & Kjellgren (2018) s. 109.
[136] von Hannover v. Germany, no 59320/00, ECHR 2004-VI p. 57 & Söderman v. Sweden, no 5786/08, ECHR 2013-XI p. 78.
[137] Derlén m.fl. (2016) s. 290-291och Naarttijärvi (2013) s. 202–203.

Europadomstolens rättspraxis rörande lagring och inhämtning av elektroniska uppgifter om den enskilde, framgår att det "utgör ett intrång i privatlivet helt oberoende av om, eller hur, dessa uppgifter sedermera används mot den enskilde på något sätt."[138] En annan sak är att intrång alltså kan vara berättigat inom ramen för en proportionalitetsbedömning.

Den negativa sidan av skyldigheten enligt artikel 8 är att undfallenhet och avsaknad av ett tillräckligt skydd kan leda till brott mot artikeln, med följden att staten står som ansvarig trots att integritetsintrånget är utfört av en enskild. En grundförutsättning för efterlevnad av artikeln är således en effektiv brottsbekämpning vilket ställer krav på de brottsbekämpande myndigheternas utredningsverktyg, såväl i "den verkliga världen" som för de brott som begås i den elektroniska miljön. När detta inte har funnits på plats har det ansetts utgöra kränkning av konventionen.[139] Detta var fallet i K.U. mot Finland där Europadomstolen uttalade att konfidentialitet för kommunikation och yttrandefrihet i vissa fall måste få ge vika för brottsbekämpningen. Fallet rörde en person som hade gjort sig skyldig till förtal, eller möjligen sexuellt ofredande, av en 12-årig pojke i Finland vars namn och bild hade publicerats på en dating-sida utan pojkens vetskap. När dennes familj senare blev varse publikationen vände de sig till finsk domstol. Den misstänkte personen kunde dock inte identifieras då det enligt den finska lagstiftningen inte var möjligt att tillgå IP-adressen från teleoperatören eftersom operatören inte fick lämna ut uppgiften när det rörde utredning av ärekränkning. Detta bröt mot artikel 8.[140] Ett aber i sammanhanget förs fram av Iain Cameron som menar att det är svårt att få en helt klar bild av Europadomstolens praxis vad gäller integritetsskyddets gränser och detta beror på att rättstillämpningen av artikel 8 är situationsbunden: " The generality of the principles involved tends to reduce its value in specific concrete situations."[141]

Till sist ska sägas att artikeln är nära förbunden med artikel 5 av vilken det framgår den statliga skyldigheten att upprätthålla ett straffrättsligt skydd och se till att ingripanden mot allvarlig brottslighet sker utan dröjsmål. För de svenska brottsbekämpande myndigheterna är det därför av största vikt att brott i den elektroniska miljön kan utredas effektivt eftersom motsatsen innebär att konventionsförpliktelserna inte efterlevs.[142]

3.5.2 Dataskyddskonventionen

Det generella skydd för den personliga integriteten som följer av artikel 8 i EKMR utvecklas i Dataskyddskonventionen[143]som stadgar ett antal

[138] Naarttijärvi (2013) s. 196–197 jfr Gellert (2020) s. 12 ff, Kelleher m.fl. (2018) s. 30 ff.
[139] Prop. 2018/19:86 s. 27 jfr Naarttijärvi (2013) s. 194–195.
[140] K.U. v. Finland, no. 2872/02, ECHR 2008-XII punkt 48-50.
[141] Cameron (2010) s. 427.
[142] Prop. 2018/19:86 s. 27–28 jfr Danelius (2015) s. 109, 112.
[143] Formellt Europarådets konvention från 1981 om skydd för enskilda vid automatisk behandling av personuppgifter (CETS 108).

grundläggande principer om dataskydd och därför betraktas som en precisering av nämnda artikel.[144] Dessutom utgjorde dataskyddskonventionen en viktig inspirationskälla vid utarbetandet av det EU-rättsliga regelverket avseende dataskydd.[145] Samtliga EU-medlemsländer har undertecknat denna och för Sveriges del trädde konventionen i kraft 1985.[146] Syftet med konventionen är att säkerställa respekten för grundläggande fri-och rättigheter, och då främst den enskildes rätt till personlig integritet vid automatiserad behandling av personuppgifter. Vid sådan behandling ska personuppgifterna användas för ett särskilt angivet ändamål.[147]

3.6 Personlig integritet enligt EU-rätten

3.6.1 Följder av Sveriges EU-anslutning

Följande avsnitt, 3.6, syftar till att beskriva vilka bestämmelser som EU-rätten ställer upp till skydd av den personliga integriteten. Inledningsvis behandlas kortfattat vilka följder Sveriges anslutning till unionen har medfört.

Sedan Sverige anslöt sig till EU har vissa beslutsbefogenheter överlåtits till de styrande i Bryssel vilket framgår av 2 och 3 §§ i lag (1994:1500) med anledning av Sveriges anslutning till Europeiska unionen, "anslutningslagen". Genom detta införlivas alltså gemenskapsrätten i den svenska rättsordningen. Följderna av EU-medlemskapet framgår även av 1 kap. 10 § RF som säger att landet är med i unionen liksom 10 kap. 6 § RF som stadgar att riksdagen har överlåtit beslutanderätt till EU under förutsättning att överlåtelsen inte rör svenska principer för statsskicket och att unionens fri-och rättighetsskydd måste uppfylla en likartad standard som RF och EKMR.[148] Den senare utformningen har hämtat inspiration från den tyska författningsdomstolens "so lange-praxis", det vill säga att domstolen sedan 1970--talet har fattat beslut rörande den nationella rättens förhållande till EU-rätten med formuleringen att "så länge som" EU håller sig inom vad som är förenligt med den tyska grundlagen kommer den att följa EU-domstolens rättspraxis.[149] Vidare framgår principen om tilldelade befogenheter av artikel 5 i FEU, vilken alltså styr avgränsningen av EU:s beslutsområde med följden att varje befogenhet som inte har tilldelats

[144] Prop. 2009/10:80 s. 174, SOU 2017:75 s. 73, Schneider (2017) s. 16 och Lexino/JUNO kommentar till RF (1974:152) 2 kap. 6 § not 28, hämtad 2021-03-03.
[145] Förslag till RÅDETS BESLUT om bemyndigande för medlemsstaterna att i Europeiska unionens intresse underteckna protokollet om ändring av Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (CETS nr 108), KOM (2018) 449 slutlig jfr SOU 2018:65 s. 62.
[146] SÖ 1982:50 jfr SOU 2018:65 s. 62.
[147] SOU 2017:75 s. 73 och Schneider (2017) s. 16.
[148] JUNO, RF (1974:152) 10 kap. 6 §, not 266, 2021-02-01, Bernitz m.fl. (2018) s. 108–109.
[149] Bull (2015) s. 130–131 och Bull och Lind (2008) s. 41.

unionen i fördragen istället är medlemsstaternas egna, detta enligt artikel 4 i FEU. Av den senare artikeln framgår även att EU ska respektera medlemsstaternas väsentliga statliga funktioner, särskilt funktioner vars syfte är att hävda deras territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar. EU-domstolen har uttalat att detta ansvar ”motsvarar det grundläggande intresset av att skydda statens väsentliga funktioner och samhällets grundläggande intressen och inbegriper förebyggande och beivrande av verksamhet som allvarligt kan störa de grundläggande konstitutionella, politiska, ekonomiska eller sociala strukturerna i ett land och i synnerhet direkt hota samhället, befolkningen eller staten som sådan, såsom bland annat terrorverksamhet.”[150]

Även om den beskrivna arbetsfördelningen kan framstå som klar framhåller Thomas Bull att det i praktiken är svårt att dra några exakta gränser för vilken överföring av kompetens som har skett till unionens organ. Han menar att för att subsidiaritetsprincipen, det vill säga att varje beslut från EU måste vara nödvändigt för att uppnå mål som inte kan nås med agerande på lägre nivå, ska fungera krävs en tydligare maktfördelning mellan unionsländer och EU.[151] Trots att förtydliganden har gjorts i Lissabonfördraget[152] är detta inte tillräckligt uttrycker Bernitz och Kjellgren.[153] Likaså diskuterar Jane Reichel EU-rättens förhållande till den nationella rätten i antologin *Arvet från Oxenstierna* och hon slår likt de övriga fast att ”den nationella rättens handlingsutrymme inte sällan kan vara oklar”.[154] Däremot, strikt normhierarkiskt betraktat, gäller att om en bestämmelse i nationell lag strider mot unionsrätten följer det av EU-rättens överordnade ställning att nationella myndigheter har en skyldighet inte tillämpa bestämmelsen. Är det på det viset att innebörden av unionsrätten är diffus ligger det i EU-domstolens hand att bestämma vad som följer av EU-rätten och vilka gränser som bland annat EU-stadgan medför.[155] Som med all form av makttilldelning är frågan kontroversiell och som kommer att beskrivas i kapitel 6 har kompetensfrågan mellan EU och medlemsstaterna gällande datalagring och personlig integritet vid hot mot nationell säkerhet, blivit intensifierad på grund av två domar från EU-domstolen under 2020.

Trots de beskrivna oklarheterna kring respektive parts befogenhet ska sägas att när det gäller direktiv är utgångspunkten att dessa är bindande för medlemsstaterna med avseende på de resultat som ska uppnås, detta enligt artikel 288 funktionsfördraget, FEUF. Denna bestämmelse i kombination med artikel 4.3 FEU om lojalt samarbete medför en skyldighet för medlemsländerna att i den nationella rätten säkerställa direktivens

[150] C-623/17 Privacy International m. fl. p. 74 och C-511/18, C-512/18, C-520/18 La Quadrature du Net m. fl. p. 135.
[151] Bull (2013a) s. 354 jfr Österdahl (2015) s. 79.
[152] Lissabonfördraget om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av europeiska gemenskapen (2007/C 306/01).
[153] Bernitz och Kjellgren (2018) s. 100, 110.
[154] Reichel (2012) s. 69.
[155] Ds 2014:23 s. 105. EU-Stadgan behandlas nedan under 3.6.2

genomförande.[156] Direktiven förutsätts därför generera nationella bestämmelser som i sin tur ska kunna åberopas av enskilda mot staten (till skillnad från förordningarna som är direkt tillämpliga). Då ofullständig och felaktig implementering av direktiv är vanligt förekommande har EU-domstolen utvidgat doktrinen om direkt effekt till att även omfatta direktiv, dock enbart för enskilda gentemot staten och alltså inte enskilda emellan. Enligt artikel 258.2 FEUF kan kommissionen föra talan om fördragsbrott mot medlemsstaten inför EU-domstolen.[157]

Mot bakgrund av detta försök att beskriva kompetensfördelningen inom unionen följer i nästa stycke en kort genomgång av de grundläggande EU-reglerna om personlig integritet.

3.6.2 EU-rättsliga bestämmelser till skydd för den personliga integriteten

Såväl EU:s primär - som sekundärrätt ställer upp en rad krav på skyddet av den personliga integriteten. Det är tydligt att det EU-rättsliga integritetsskyddet, genom Europeiska unionens stadga om de grundläggande rättigheterna, hädanefter EU-stadgan, är starkt influerad av EKMR och dess ovan beskrivna artiklar.[158] Därtill framgår av artikel 6.1 i FEU att unionen ska erkänna de rättigheter, friheter och principer som fastställs i EKMR och att dessa skrivningar ska ha samma rättsliga värde som fördragen har. Efterföljande artikel 6.2 FEU anger att unionen har anslutit sig till Europakonventionen, även om anslutningen inte ska medföra någon ändring av unionens befogenheter såsom de definieras i fördragen. När det gäller EU-stadgan är den normhierarkisk i paritet med fördragen, det vill säga de ligger samtliga högst upp. Innehållsmässigt ter sig EU-stadgan och EKMR lika, däremot har den förstnämnda en processuell fördel i och med att det för den enskilda kan te sig mer attraktivt att nyttja EU-rättens institutionella möjligheter jämfört med att vända sig till Europadomstolen. Detta eftersom den senare har ett stort antal väntande mål, vilket således även innebär en lång väntetid för ett avgörande. Samtidigt kan nämnas att för svenskt vidkommande dominerar EKMR området för rättighetsskydd.[159]

I fråga om EU-stadgans artiklar ska här nämnas artikel 6 som säger att var och en har rätt till frihet och personlig säkerhet, liksom artikel 7 som föreskriver att var och en rätten till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Därtill framgår av artikel 8 att den enskilde har rätt till skydd av sina personuppgifter.[160] Denna typ av

[156] FEUF, fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt 2012/C 326/0. Bergström (2012) s. 41.
[157] Bernitz och Kjellgren s. 58–59, 118–119.
[158] Prop. 2009/10:80 s. 175, SOU 2017:75 s. 70 jfr prop. 2018/19:86 s. 27–28, Bull m.fl. (2008) s. 57.
[159] Bernitz m.fl. (2018) s. 145, Bull (2013b) s. 73, 77 jfr Lynskey (2015) s. 127–129.
[160] C-203/15, C-698/15 Tele2, EU:C:2016:970 p. 93, C-293/12, C-594/12, Digital Rights, EU:C:2014:238, p. 53, C-362/14, Schrems, EU:C:2015:650, p. 39 jfr SOU 2017:75 s. 77.

uppgifter ska behandlas för bestämda ändamål och på grundval av den enskildes samtycke eller annan legitim anledning. Artikel 8 skyddar inte den lagrade informationen som sådan, utan skyddar istället den enskilde för de eventuella följderna av uppgiftshanteringen. Artikel 7 har därför en innehållsmässig fördel eftersom den tillhandahåller ett materiellt skydd av privatlivet som konkretiserar artikelns räckvidd.[161]

Gällande inskränkningar i de beskrivna rättigheterna, är detta möjligt att få till stånd så länge som den så kallade proportionalitetsprincipen beaktas. Utgångspunkten är att inskränkningar enbart får göras i lag och ska då vara förenliga med det väsentliga innehållet i rättigheterna. Vidare krävs det att inskränkningarna anses vara nödvändiga och går i linje med de mål av allmänt intresse som EU har erkänt, eller att inskränkningarna krävs för att skydda andra människors rättigheter och friheter.[162] Att proportionalitetsprincipen måste efterlevas framgår dels av EU-stadgans 52.1, dels av EU-domstolens fasta praxis, enligt vilken skyddet av den grundläggande rätten till respekt för privatlivet kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt.[163] EU-domstolen har uttalat att för att proportionalitetskravet ska vara uppfyllt krävs det att lagstiftningen föreskriver ”klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden” och att det av denna även framgår ett minimikrav så att personer vars personuppgifter påverkas, har en garanti för att uppgifterna skyddas mot missbruk.[164] Tolkningen av EU-stadgan får inte inskränka EKMR:s skyddsnivå enligt stadgans artikel 53 och därtill framgår av artikel 52.3 att i den mån stadgan omfattar rättigheter som har sin motsvarighet i EKMR ska de ha samma innebörd och räckvidd som enligt konventionen. Detta är dock inget hinder för ett mer långtgående unionsrättsligt skydd. För den enskilde bör därför den mest fördelaktiga regeln användas. Trots att den unionsrättsliga företrädesrätten alltså numera är kodifierad i en förklaring (nr. 17) till Lissabonfördragets slutakt är frågan fortsatt kontroversiell.[165] Bernitz och Kjellgren jämför företrädesrätten utifrån talesättet att det inte är möjligt att ”både äta kakan och ha den kvar” och menar att när medlemsländerna väl har delegerat sin makt till unionen att lagstifta och agera på ett visst område, kan de inte samtidigt behålla rätten att hävda egna nationella regler.[166] Denna komplexitet kommer att aktualiseras senare i redogörelsen i samband med att datalagringens omfattning behandlas.

---

[161] Schneider (2017) s. 18. Se även Lynskey (2015) s. 89 ff.
[162] Framkommer bland annat i C-203/15 och C-698/15 Tele2-domen, EU:C:2016:970 p. 94 jfr prop. 2018/19:86 s. 23–24, Derlén m.fl. (2016) analys av principen s. 288–290.
[163] Framgår bl.a. av C-203/15, C-698/15 Tele2, EU:C:2016:970 p.96, C-293/12, C-594/12, Digital Rights, EU:C:2014:238, p.52, C-362/14, Schrems, EU:C:2015:650, p.92 jfr prop. 2018/19:86 s. 28-29.
[164] C-511/18, C-512/18, C-520/18 La Quadrature du Net m.fl., EU:C:2020:791 p. 132, C-293/12, C-594/12, Digital Rights, EU:C:2014:238, p.54-55, C-203/15 och C-698/15, Tele2, EU:C:2016:970, p. 117.
[165] Bernitz &Kjellgren (2018) s. 101–107, 157. Gällande art. 53 se mål C-399/11, S. Melloni mot Ministerio Fiscal, EU:C:2013:107, p. 55–64.
[166] Bernitz och Kjellgren (2021) s. 53.

Med detta sagt är det alltså en balansakt för den nationella lagstiftaren att iakttaga proportionalitetsprincipen och samtidigt se till att den nationella lagstiftningen tillgodoser de positiva förpliktelser som bland annat EKMR ställer upp rörande statens skyldighet att skydda enskilda från ingrepp i de grundläggande rättigheterna från andra enskilda.[167] Slutligen ska här även nämnas två andra grundläggande bestämmelser som ska beaktas av den nationella lagstiftaren, nämligen artikel 2 i FEU som anger att unionen bland annat ska bygga på frihet liksom respekt för de mänskliga rättigheterna och likaså artikel 16.1 FEUF som anger att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.[168]

Mot bakgrund av dessa grundläggande bestämmelser följer i nästa kapitel en genomgång av de specialbestämmelser som gäller för just behandlingen av personuppgifter vid elektronisk behandling.

[167] Prop. 2018/19:86 s. 29. Om positiva förpliktelser se Derlén m.fl. (2016) s. 321–322.
[168] Art. 16 FEUF och GDPR-reformen, se vidare Kelleher & Murray (2018) s. 5 ff.

4 Integritetsskydd inom sektorn för elektronisk kommunikation

4.1 Utvecklingen av EU-rättens särskilda personuppgiftsskydd vid elektronisk behandling

Då regelverket rörande personuppgiftsskydd är ”snårigt” och då det förekommer många hänvisningar till olika rättsakter ska kommande två avsnitt redogöra för det EU-rättsliga personskyddet. Vid sidan av de primärrättsliga bestämmelserna som beskrevs i föregående kapitel fyllde tidigare direktiv 95/46/EG, dataskyddsdirektivet, en central roll i det EU-rättsliga personuppgiftsskyddet.[169] Likväl har det betydelse idag, trots att det är upphävt vilket alltså beror på korshänvisning från detta till senare antagna rättsakter. Syftet med direktivet var att skydda enskildas grundläggande fri- och rättigheter, i synnerhet rätten till ett privatliv, i samband med behandling av personuppgifter och ett vidare mål var att precisera och förstärka den ovan beskrivna dataskyddskonventionen (se artikel 1.1 resp. skäl 11). Direktivet skulle därtill borga för att personuppgifter skulle kunna utbytas medlemsländerna emellan. Med personuppgift, avsågs mycket förenklat sagt upplysningar om en identifierbar person och direktivet var tillämpligt på dessa vid automatisk behandling liksom annan personuppgiftsbehandling som skulle ingå i ett register (artikel 2a respektive 3.1). Bland direktivets många principer fanns bestämmelser om att den enskilda skulle informeras och få tillgång till uppgifter som hade behandlats. Gällande statens säkerhet fanns det dock undantag, detta rörde således områden som EU-rätten inte täcker, såsom försvar, allmän säkerhet och de enskilda staternas verksamhet på straffrättens område.[170]

För svensk del genomfördes direktivet genom personuppgiftslagen (1998:204). Ur en konstitutionell synvinkel påpekar Jane Reichel, hur rättsakten kontrasterades av den svenska rättstraditionen med en stark offentlighetsprincip som ofta får företräde i lägen då denna viktas mot andra aspekter som personlig integritet och dataskydd. Hon framhåller att detta på intet sett var en ny fråga för lagstiftaren att brottas med:”… the question of transparency has been sensitive from the very start of Sweden’s membership in the EU, and the debate is still ongoing”.[171] Sedermera kom det EU-

[169] Formellt Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter. Se SOU 2017:75 s. 71, Derlén m.fl. (2016) s. 326–330.
[170] SOU 2017:75 s. 71 jfr Siemen (2006) s. 212–213.
[171] Reichel (2017) s. 201, 215, 221 jfr Österdahl (2015), s. 77–78, 95–96.

rättsliga regelverket att reformeras och hur dåvarande reglering fortsatt interagerar med gällande rätt beskrivs nedan.

4.2 Nuvarande regelverk för dataskydd

Få EU-medborgare idag har inte hört talas om dataskyddsförordning, ofta förkortad GDPR.[172] Detta är resultatet av det reformarbete som startades 2012 med målet att effektivisera och harmonisera personuppgiftsskyddet inom EU. När GDPR antogs i april 2016 ersatte det därför det ovan beskrivna dataskyddsdirektivet 95/46/EG, och började tillämpas i maj 2018.[173] I samband med detta upphörde den svenska personuppgiftslagen att gälla och ersattes av lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen.[174] Sedan införandet av GDPR i Sverige finns således den generella regleringen av behandling av personuppgifter där.[175]

Alltjämt är det dock principerna i direktiv 95/46/EG som gäller även i GDPR och de hänvisningar till det upphävda direktivet som fortfarande förekommer ska betraktas som hänvisningar till GDPR. Detta framgår av artikel 94.2. i förordningen (jfr skäl 9 GDPR). Att så är fallet blir tydligt vid en jämförelse av de två rättsakterna. Av artikel 1 i GDPR framgår att förordningen fastställer bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter. Vidare ämnar förordningen till att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Därtill stadgas att det fria flödet av personuppgifter inom unionen inte får begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter. Utgångspunkten i GDPR är att all information rörande fysiska personer som kan identifieras utifrån informationen i dessa uppgifter är personuppgifter, vilket framkommer av artikel 4. Det kan till exempel röra sig om en lokaliseringsuppgift som är en av alla de uppgifter som förordningen omfattar. Jämförelsevis är artikeln en utvidgad version av ovan nämnda artikel 2a i direktiv 95/46/EG. Likt sin föregångare gäller GDPR inom EU för den som behandlar personuppgifter och är etablerad i unionen, liksom vid behandling av personuppgifter för individer hemmahörande i EU, enligt artikel 3. Därtill definieras i artikel 6 vad som menas med en laglig behandling av personuppgifter och precis som för direktiv 95/46/EG utgår även GDPR från ett antal principer som gäller vid personuppgiftsbehandling vilket framgår av artikel 5. Av central betydelse här är värnandet om

[172] Formellt Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[173] Prop. 2017/18:105 s. 17, SOU 2018:65 s. 63–65 och Müthlein (2017) s. 13–14.
[174] Prop. 2017/18:105 s. 7,18 och prop. 2017/18:269 s. 95. Se skäl 8 i GDPR, jfr dock med artikel 288 2 st. i FEUF om att förordningar är direkt tillämpliga i medlemsstaterna.
[175] Prop. 2017/18:105 s. 21 och prop. 2017/18:269 s. 95.

integritet och konfidentialitet, nödvändigheten av lagringen, samtycke från den berörda till att dennes personuppgifter behandlas (se art. 7 och 8) och en ändamålsbegränsning av de behandlade uppgifterna. Likaså finns det bestämmelser om radering av uppgifter i kapitel 3.

För läsarens förståelse ska här ett förtydligande till en angränsande rättsakt göras. Från GDPR:s tillämpningsområde undantas nämligen den behandling av personuppgifter som görs av behöriga myndigheter i syfte att förebygga, förhindra, utreda och klara upp brott liksom att verkställa straffrättsliga påföljder vilket framgår av artikel 2 (motsvaras av art. 3.2 i direktiv 95/46/EG). I detta ingår att förebygga och förhindra hot mot den allmänna säkerheten. För den här typen av personuppgiftsbehandling av myndigheter ska istället dataskyddsdirektivet (EU) 2016/680 användas.[176] Som tydliggjorts under syftesavsnittet handlar förevarande arbete om teleoperatörers lagring av data som i ett senare led kan lämnas ut till de brottsbekämpande myndigheterna. Detta medför att (EU) 2016/680 således ligger utanför den lagring som telekommunikatörer omfattas av kommer därför inte att behandlas i framställningen.[177]

Sammanfattningsvis i denna del har således GDPR, efterträtt det äldre dataskyddsdirektivet 95/46/EG, men likt det senare syftar även den nya förordningen till att skydda fysiska personer med avseende på behandling av personuppgifter och samtidigt säkra ett fritt flöde av personuppgifter inom unionen. Då det äldre direktivet inte genomfördes och tillämpades enhetligt över unionen ledde detta till en varierande grad av skyddsnivåer länderna emellan med en rättsosäkerhet som följd. Detta utgjorde ett hinder för fri konkurrens och ekonomisk verksamhet samt hindrade myndigheter att fullgöra sina plikter enligt unionsrätten, och den EU-rättsliga lagstiftaren ansåg att en förordning krävdes för att få till stånd en enhetlig rättstillämpning (jfr skäl 9–13 i GDPR). De beskrivna artiklarna utgör huvuddragen i det EU-rättsliga personuppgiftsskyddet och är en viktig ”grundplåt” för att förstå hur det generella skyddet för individen ter sig i förhållande till de regler som leverantörer av elektronisk kommunikation omfattas av i E-Privacy-direktivet. Detta direktiv behandlas i nästa avsnitt.

[176] Se skäl 19 i GDPR, prop. 2017/18:105 s. 18, prop. 2017/18:269 s. 95, SOU 2017:75 s. 72. Dataskyddsdirektivet heter formellt Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
[177] (EU) 2016/680 medförde att brottsdatalagen (2018:1177) trädde i kraft 2018, se SOU 2018:65 s. 65: att GDPR inte är tillämplig på den behandling som omfattas av brottsdatalagen, dock gäller att myndigheter som tillämpar brottsdatalagen även ska tillämpa GDPR i de delar av verksamheten som inte omfattas av brottsdatalagens tillämpningsområde.

4.3 Direktiv om integritet och elektronisk kommunikation – ”ePrivacy-direktivet”

4.3.1 Bakgrund och förhållande till annan lag

Mot bakgrund av redogörelsen för det äldre dataskyddsdirektivet (95/46/EG) och dess förhållande till GDPR i det föregående avsnittet ska resterande del av kapitlet ägnas åt E-Privacy-direktivet (även benämnt ”ePrivacy-direktivet”). Detta kompletterade och preciserade nämligen dataskyddsdirektivet så länge som det var i kraft.[178]

Som förklarades i uppsatsens inledningskapitel är E-Privacy-direktivet det regelverket som bland annat styr omfattningen av teleoperatörernas uppgiftslagring. När EG-kommissionen lade fram förslaget om direktivet år 2000 skedde det mot bakgrund av den snabba marknadsmässiga och tekniska utvecklingen, främst gällande internet och telefoni. En alltmer konkurrensutsatt marknad fordrade en modernisering av lagstiftningen och tanken var att direktivet, som alltså är inriktat på integritetsskyddsfrågor vid elektronisk kommunikation, skulle möta dessa nya krav. Direktivet ingick i ett större lagförslag som totalt omfattade sex olika direktiv, varav samtliga har genomförts i svensk rätt genom LEK.[179] Med EU-reformen ersattes det äldre teledataskyddsdirektivet, direktiv 97/66/EG och sedan genomförandet har ett ändringsdirektiv följt, direktiv 2009/136/EG.[180]

Syftet med direktiv E-Privacy-direktivet, är att harmonisera medlemsländernas regelverk gällande personlig integritet och att säkerställa ett likvärdigt skydd av, de i kapitel 3 beskrivna, grundläggande fri-och rättigheterna då personuppgifter behandlas vid elektronisk kommunikation inom unionen. På detta vis konkretiserar direktivet de rättigheter som framkommer av EU-stadgans artikel 7 och 8, vilket innebär att användare av elektronisk kommunikation ska kunna förvänta sig att kommunikationen förblir anonym och inte kan registreras om de inte har samtyckt till detta.[181] Det som för vissa internetanvändare framstår som ett enerverande godkännande av så kallade cookies sker mot bakgrund av direktivet som därför även går under det inofficiella epitetet ”Cookie-direktivet.”[182] Vidare ska direktivet säkerställa fri rörlighet för personuppgifter vid elektronisk kommunikation liksom utrustning och tjänster inom området elektronisk kommunikation, vilket framgår av artikel 1.1 och 3. Gällande berörda verksamheter framgår av artikel 1.3 att det inte ska tillämpas på områden som faller utanför tillämpningsområdet för FEUF, t.ex. de som omfattas av

[178] Ds 2014:23 s. 21 jfr Carey (2009) s. 12-13, Kelleher m.fl. (2018) s. 476.
[179] Prop. 2002/03:110 s. 64–65, SOU 2017:75 s. 79 och SOU 2007:22 s. 294–295. Kelleher m.fl. (2018) s. 473–487.
[180] Teledataskyddsdirektivet: Europaparlamentets och rådets direktiv 97/66/EG av den 15 december 1997 om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet. Prop. 2002/03:110 s. 69–70.
[181] SOU 2017:75 s. 77 och t.ex. C-623/17, Privacy International, EU:C:2020:790 p. 57.
[182] Se vidare i Carey (2009) s. 223–224, Kelleher m.fl. (2018) s. 479.

avdelningarna V och VI i FEU, hit hör bland annat beskattning. Uteslutet är även användning på verksamheter som avser allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Vidare definieras begreppen trafikuppgifter och lokaliseringsuppgifter i artikel 2 och dessa motsvaras av den beskrivning som gavs i uppsatsens kapitel 2. Däremot preciseras inte abonnemangsuppgifter i direktivet.[183] Som kommer att visas i det följande har detta orsakat huvudbry hos nationella lagstiftare runt om i unionen.

Mot bakgrund av GDPR:s intåg på den dataskyddsrättsliga scenen förändrades även samspelet mellan det äldre dataskyddsdirektivet och E-Privacy-direktivet, detta eftersom artikel 1.2 i det senare anger att bestämmelserna i det ska precisera och komplettera det äldre direktivet 95/46/EG. Däremot framgår av artikel 95 i GDPR att införandet av förordningen inte ska medföra några ytterligare förpliktelser för de som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med E-Privacy-direktivet.[184]

För den oinvigde kan navigationen mellan GDPR och det upphävda dataskyddsdirektivet 95/46/EG utifrån läsning av E-Privacy-direktivet te sig besvärlig. Målet för den EU-rättsliga lagstiftaren är att situationen ska åtgärdas, vilket framgår av skäl 173 i GDPR: ”För att klargöra förhållandet mellan denna förordning och direktiv 2002/58/EG bör det direktivet ändras. När denna förordning har antagits, bör direktiv 2002/58/EG ses över, framför allt för att säkerställa konsekvens med denna förordning.” I skrivande stund har dock inte något klargörande om direktivets förhållande till det äldre dataskyddsdirektivet respektive den nya dataskyddsförordningen presenterats. Arbetet med en översyn pågår allt jämnt sedan 2017. EU-kommissionen har lagt fram ett förslag på en ny förordning[185] vilket, om denna skulle realiseras, innebär att E-Privacy-direktivet i sådant fall skulle upphävas. Medlemsländerna har dock inte kommit överens om utformningen. I december 2020 informerades den svenska regeringen om hur arbetet med förslaget om den nya förordningen har förflutit under det tyska ordförandeskapet. Vissa bedömare har visat skepsis till att EU-kommissionens förslag kommer att leda till ny lagstiftning framgent överhuvudtaget.[186] Under närmast överskådlig tid kommer därför E-Privacy-direktivet fortsatt att styra på området.

---

[183] Prop. 2018/19:86 s. 93, 96, jfr skäl 11 om att direktivet inte omfattar frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av EU-rätten.
[184] Prop. 2017/18:105 s. 241 och 296.
[185] Prop. 2019/20:64 s. 51. Förslag till Europaparlamentets och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation), KOM (2017)10 slutlig. Jfr Kuner (2020) m.fl. s. 71, 348.
[186] Se Infrastrukturdepartementet, dagordning 7 december 2020 och Advokatfirman Delphi, 2020-02-17, *e-Privacy-förordningen (EPR) alltmer avlägsen*, se länkar i källförteckning, jfr

Med denna bakgrund till E-Privacy-direktivet och dess förhållande till andra närliggande rättsakter följer i nästa avsnitt en genomgång av direktivets centrala bestämmelser.

4.3.2 Centrala regler i E-Privacy-direktivet

Följande stycke ämnar till att förklara E-Privacy-direktivets kärnpunkt, nämligen den huvudregel om integritet som tillkommer den enskilde vid elektronisk kommunikation. Det är denna tanke som direktivet bygger på. Redan här ska sägas att direktivet som sådant är svårtillgängligt och de bestämmelser som jag har valt att lyfta har så långt som möjligt förenklats för läsarens skull. Den resterande framställningen bygger på en förståelse för dessa bestämmelser.

Med detta sagt ska sägas att den nämnda huvudregeln tar sig uttryck i artikel 4.1 där det framgår att det åvilar leverantörer av en tjänst inom området för elektronisk kommunikation en skyldighet att vidtaga åtgärder för att skydda användarens personuppgifter. Därtill ska medlemsstaterna i sin nationella rätt tillförsäkra konfidentialitet vid kommunikation via allmänna nät och allmänt tillgängliga elektroniska kommunikationstjänster enligt artikel 5, kort sagt påbjuds alltså konfidentialitet för trafikuppgifter. I synnerhet ska avlyssning, lagring och liknande metoder som medför att kommunikationen kan övervakas av andra personer än användarna utan de berörda användarnas samtycke förbjudas.[187] Därtill anger artikel 6 p. 1–3 när trafikuppgifter får behandlas och vilka krav som då ställs på uppgiftsbehandlingen. Utgångspunkten är att trafikuppgifter rörande abonnenter och registrerade användare ska raderas och avidentifieras när de inte längre behövs för sitt syfte att överföra kommunikation. Dock får trafikuppgifter som krävs för att kunna fakturera kunder liksom för att ta betalt för samtrafik[188] behandlas. Sådan behandling är tillåten endast fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning. Vid samtycke från abonnenten får även uppgifter behandlas för marknadsföringsändamål. Även artikel 9 som rör lokaliseringsuppgifter ställer krav på avidentifiering eller samtycke från abonnenten själv.[189] För de tre uppräknade artiklarna 5,6 och 9 är den övergripande målsättningen att utformningen av systemen för tillhandahållande av elektroniska kommunikationsnät liksom kommunikationstjänster ska sträva mot att begränsa mängden personuppgifter till ”absolut minimum”, enligt skäl 30. Dock medger artikel

prop. 2018/19:86 s. 108 där regeringen påpekar att det inom EU förs diskussioner om huruvida ett nytt EU-regelverk för lagring på det brottsbekämpande området bör införas.

[187] Prop. 2002/03:110 s. 253, SOU 2017:75 s. 78. Dock är så kallad buffring, det vill säga lagring av överförd information som sker för att diverse funktioner i nätet skall hinna behandla informationen, godkänd. I artikel 5 betecknas buffring som ”teknisk lagring.”

[188] Samtrafik innebär att operatörer kopplar samman näten för att slutanvändare ska kunna nå varandra enligt PTS, se länk i källförteckning.

[189] Prop. 2002/2003:110 s. 253, SOU 2017:75 s. 78–79. Artikel 8 hör till uppräkningen men ligger utanför syftet (rör tjänsteleverantörens krav på nummerpresentation till kund).

15.1 vissa undantag från den just beskrivna grundskyldigheten att garantera konfidentialitet vid elektronisk kommunikation i den nationella rätten. Medlemsstaterna får nämligen genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som framgår av direktivets artiklar 5, 6, 8.1-8.3 och 9 när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i dataskyddsdirektivet. För detta ändamål får medlemsstaterna vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som framgår av artikeln. Vidare framgår att de beskrivna åtgärderna ska vara i enlighet med de allmänna principerna i unionslagstiftningen, inklusive principerna i artikel 6.1och 6.2 i FEU.

Den enskildes rättigheter kringskärs således av artikel 15.1 då det behövs för att upprätthålla säkerhet och stävja brottslighet. Som framgår ställs dock krav på begränsningarna i rättighetsskyddet.[190] EU-domstolen har uttryckt att bland de allmänna principer som det refereras till i artikelns sista stycke ingår EU-stadgans rättigheter.[191] Därtill har klargjorts att de möjligheter att göra undantag från de rättigheter och skyldigheter som anges i artiklarna 5, 6 och 9 i direktivet inte kan användas som ett argument av den nationella lagstiftaren för att generellt frångå skyldigheten att säkerställa konfidentialitet vid elektronisk kommunikation. Detta eftersom det är av grundläggande betydelse att uppgifter hålls hemliga av hänsyn till respekten för privatlivet. Den enskildes vetskap om att lagring sker för polisiära ändamål kan nämligen ha en avhållande inverkan på utövandet av den enskildes grundläggande rättigheter. Uppräkningen i artikel 15.1 är enligt EU-domstolen uttömmande, därmed finns inga andra mål som kan motivera en begränsning av den enskildes rättigheter.[192] Däremot ska förtydligas att operatörerna inte lagrar uppgifter avseende tjänster som en annan tjänsteleverantör tillhandahåller, och utesluts gör även telefonsamtal via appar, webbplatsbesök och onlinespel. Regeringen har påtalat att dessa tjänster blir alltmer frekvent nyttjade.[193]

Nedan beskrivs hur direktivets integritetsbestämmelser har genomförts i LEK. Avsnittet bygger således vidare på den bakgrundshistorik till lagen som presenterades i kapitel 2.

[190] Prop. 2002/03:110 s. 253. (Art. 13.1 är idag art. 23 i GDPR, se Ds 2017:26 s. 49).
[191] C-131/12, Google Spain, EU:C:2014:317 p. 68, C-362/14, Schrems, EU:C:2015:650 p. 38.
[192] C-698/15, Tele2, EU:C:2016:970, p. 89, 104,142, C-207/16, Ministerio Fiscal, EU:C:2018:788, p. 52.
[193] Bl.a. Apple I-Message, Facebook Messenger, Skype, G-mail och Hotmail. Om filöverföringsprotokoll, FTP, se vidare i prop. 2018/19:86 s. 29–30.

4.4 Integritetsbestämmelser i LEK

4.4.1 Inledande anmärkningar

Inledningsvis ska sägas att syftet med kommande avsnitt är att beskriva gränsdragningen mellan integritet och lagring av elektronisk kommunikation i LEK. Det är en utmaning att förklara lagens föreskrifter om datalagring på ett pedagogiskt vis för läsaren, vilket dels beror på att lagen innehåller ett stort antal hänvisningar liksom undantag från huvudregler, dels på att datalagringen successivt har utökats och då med nya anledningar till att lagring får lov att ske. Gällande den fortsatta dispositionen presenteras i nästa avsnitt för det första de bestämmelser som gäller integritet vid datalagring. Efterföljande avsnitt behandlar den senare tillkomna lagringsskyldigheten som sker enbart mot bakgrund av brottsbekämpning. Den senare lagringsformen hänger nämligen ihop med de uppgifter som får lagras av operatörerna av andra ändamål än för just brottsbekämpning. I ett rent paragrafhänseende görs alltså en uppdelning mellan de olika lagringsformerna, ur praktiskt hänseende är det dock en mer flytande gräns vilket kommer att visa sig i det följande.

4.4.2 Integritet vid databehandling i LEK

Vid genomförandet av E-Privacy-direktivet i svensk rätt diskuterade regeringen vikten av att skyldigheten för operatörer att utplåna eller avidentifiera trafikuppgifter enligt direktivets artikel 6 inte fick gå utöver reglerna om hemlig teleövervakning enligt dåvarande 50 § första stycket 1 telelagen. Trafikuppgifter som var nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller kommunikationstjänst skulle också medges i LEK och detta med hänvisning till direktivets artikel 15.1. Likaså användes artikeln som stöd för att införa en möjlighet för myndigheter och domstolar att få tillgång till trafikuppgifter för att kunna lösa tvister om samtrafik och fakturering. För detta ändamål skulle således inte skyldigheten att radera eller avidentifiera trafikuppgifter inträda.[194] Samtliga lagringsmöjligheter infördes i kapitel 6. På motsvarande sätt som artikel 4 i direktivet framgår av detta kapitel i 3–4 b §§, de säkerhetsbestämmelser som gäller vid tillhandahållande av allmänt tillgängliga tjänster vid elektronisk kommunikation.[195] Likaså ska den konfidentialitet som artikel 15.1 i direktivet föreskriver säkerställas genom bestämmelser om förbud mot avlyssning i lagens 6 kap. 17 §. Därtill framgår en bestämmelse om tystnadsplikt i 6 kap. 20 § för den som i samband med tillhandahållandet av kommunikationen får del av information och detta omfattar uppgift om abonnemang, innehållet i ett elektroniskt meddelande och ”annan uppgift som angår ett särskilt elektroniskt meddelande”. Det senare är en benämning som inkluderar trafikuppgifter.[196]

[194] Prop. 2002/03:110 s. 259.
[195] Prop. 2010/11:46 s. 53, Ds 2014:23 s. 21–22 och SOU 2017:75 s. 80.
[196] Naarttijärvi (2013) s. 265.

Ett obehörigt röjande av uppgifter i strid med 20 § är straffsanktionerat i 20 kap. 3 § BrB som brott mot tystnadsplikten.[197]

Användarnas grundläggande rättigheter skyddas enligt lagens huvudregel i 6 kap. 5 § som säger att trafikuppgifter om abonnenter ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande av den som bedriver anmälningspliktig verksamhet. Dock finns här ett viktigt undantag. Regeln gäller nämligen inte om uppgifterna sparas för sådan behandling som anges i 6, 13, 16 a eller 16 c §§. Dessa avsteg från huvudregeln har mycket stor betydelse för de brottsbekämpande myndigheterna eftersom detta är en ingång i lagen som möjliggör tillgång till data som har lagrats hos teleoperatörerna. Detta motsvarar undantaget i artikel 15.1 i E-Privacy-direktivet. Därtill säger 6 kap. 6 § att trafikuppgifter som krävs för abonnentfakturering och betalning av avgifter för samtrafik får behandlas till dess att fordran är betald eller preskription inträtt och det inte längre lagligen går att göra invändningar mot faktureringen. Den som tillhandahåller en kommunikationstjänst ska lämna information om vilka trafikuppgifter som behandlas liksom hur länge det fortgår.

För både 6 kap. 5 och 6 §§ får behandling av trafikuppgifter endast utföras av den aktör som har fått i uppdrag av en verksamhetsutövare som är anmälningspliktig att sköta fakturering, trafikstyrning, kundförfrågningar, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av andra tjänster där uppgifterna behövs. Behandlingen skall begränsas till vad som är nödvändigt för verksamheten enligt 6 kap. 7§. Det just beskrivna, alltså undantagen från raderingsskyldigheten av uppgifter för operatörerna, kan således sägas utgöra ”en ventil” i lagen och av 6 kap. 8 § framgår därför när undantag från de ovan presenterade 6 kap. 5–7 §§ kan göras. Detta gäller när en myndighet eller en domstol behöver tillgång till sådana uppgifter som avses med de paragrafhänvisningar som framgår av 5 §. Av dessa hänvisningar ska enbart 6 kap. 6, 16 a samt 16 c §§ behandlas i förevarande arbete. Som ovan beskrivet är det 6 kap. 5 § som utgör lagens huvudregel och i paragrafens ursprungliga form fanns enbart det beskrivna undantaget i 6 § liksom 13 §.[198] Gällande de hänvisningar från 5§ som görs till undantagen i 6 kap. 16 a och 16 c §§ är dessa nämligen ett resultat av en annan EU-rättsakt och för förståelsens skull kommer dessa att behandlas separat under en egen rubrik.

De undantag som medges från 6 kap. 5 § och som framgår av 6 kap. 8 § gäller då uppgifterna behövs för tvistelösning, för meddelanden som omfattas av beslut enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, eller för elektroniska meddelanden som omfattas av ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken, samt då uppgifter är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en

[197] Ds 2014: 23 s. 22 och SOU 2017:75 s. 80. Straffsanktioner se 7 kap. 15 § i LEK.
[198] Prop. 2010/11:46 s. 8. Gällande 13 § rör den särskilda fall vid nummerpresentation och att samtycke inte krävs för utlämnande av lokaliseringsuppgifter vid nödsamtal.

elektronisk kommunikationstjänst. Gällande efterlevnaden av lagringskraven på operatörerna kan förenklat sägas att PTS får meddela förelägganden som kan förenas med vite enligt 7 kap. 3–5 §§.

Med all tydlighet framgår av förarbetena till direktivets genomförande att det från lagstiftarens sida inte fanns några funderingar kring att införa en regelrätt skyldighet för teleoperatörerna att lagra uppgifter enbart i brottsbekämpande syfte utifrån möjligheten som ges i artikel 15.1. Istället utnyttjades den lagring som skedde hos operatörerna av praktiska ändamål, i just brottsbekämpande syfte. I senare förarbeten har det uppmärksammats att det varken i LEK eller i dess förordning framgick vilka uppgifter som fick lagras.[199] Likaså diskuterades lagringstiderna för de undantag som ändå genomfördes mycket sparsmakat vid lagens införande. Vad gäller tidsspannet uttalades att: ”Uppgifterna får inte sparas längre än vad som är nödvändigt för syftet. Längre än ett år bör inte godtas, om det inte föreligger särskild anledning, såsom att tvist uppkommit eller förundersökning inletts i ett särskilt fall.” [200] Lagstiftaren anförde att i ”lagens sjätte kapitel ges de bestämmelser som krävs för att skydda användarnas personliga integritet m.m.” och att direktivet ”till största delen” genomfördes genom de föreslagna bestämmelserna i LEK.[201]

Synen på datalagring i Europa kom dock att drastiskt förändras två år senare vilket avspeglas i senare tillkomna paragrafer i LEK. Bakgrunden till detta och hur det påverkade svensk rätt förklaras i det följande. Förenklat kan sägas att datalagringen inom EU då gick från att möjliggöra lagring genom undantagen i artikel 15.1 i E-Privacy-direktivet, till att istället ålägga teleoperatörerna en lagring av uppgifter, och då enbart av brottsbekämpande ändamål. Den senare lagringstypen skulle alltså löpa vid sidan av den lagring som redan gjordes av mer praktiska hänseenden hos operatörerna, och som just har beskrivits i detta avsnitt.

4.5 Datalagringsdirektivet

4.5.1 Bakgrund

Detta avsnitt, 4.5, syftar till att presentera datalagringsdirektivet och vilken inverkan det har haft på nationell rätt.

Efter terrorattacken i Madrid den 11 mars 2004 fick rådet för rättsliga och inrikes frågor (RIF) i uppdrag av Europeiska rådet att snarast anta gemensamma åtgärder i fråga om lagring av trafikuppgifter. Arbetet resulterade slutligen i det så kallade datalagringsdirektivet.[202] Syftet med

[199] Prop. 2010/11:46 s. 28.
[200] Prop. 2002/03:110 s. 259–260, 392.
[201] Prop. 2002/03:110 s. 119, 337.
[202] Formellt Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av trafikuppgifter som genererats eller behandlats i samband med tillhandahållande

direktivet framgick av dess artikel 1.1 och var att harmonisera reglerna om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät för att på så vis säkerställa att uppgifterna var tillgängliga för avslöjande, utredning och åtal av allvarliga brott.[203] Sverige var ett av de länder som tog initiativet till direktivet.[204] Det var en kontroversiell reglering, och bland annat Europeiska ekonomiska och sociala kommittén var starkt kritisk till det lagförslag som lades fram och sedermera antogs.[205]

”Bestämmelserna i direktivet är inte helt lättillgängliga”.[206] Klart är i alla fall att i och med datalagringsdirektivets genomförande ändrades förutsättningarna för tillämpningen av E-Privacy-direktivet och istället föreskrevs en mycket omfattande informationsinsamling som delvis avsåg ”ytterst integritetskänsliga uppgifter”.[207] Förenklat uttryckt skulle lagringen möjliggöra att behöriga myndigheter skulle kunna få information om vem som hade kontaktat vem, när kommunikationen fördes, var personerna då befann sig och vilken typ av kommunikationsmedel som användes. Därför skulle samtliga uppgifter om meddelanden (dock ej själva innehållet) som överfördes hos operatörer via fast och mobil telefoni lagras, liksom all internettrafik, e-post, internetåtkomst samt anslutningsform. Detta skulle fortgå i minst sex månader och högst två år och därefter var huvudregeln utplåning av uppgifterna. Kraven framgick av direktivets artiklar 3 liksom 5–7. Enligt artikel 8 framgick att uppgifterna skulle kunna lämnas över till behöriga myndigheter utan dröjsmål. Att brottsbekämpningen stod högre i kurs än integritetsaspekten i datalagringsdirektivet framgick allra tydligast i dess artikel 11 som uttryckte att artikel 15.1 i E-Privacy-direktivet inte fick tillämpas på de uppgifter som specifikt skulle lagras enligt datalagringsdirektivets bestämmelser.[208] Detta innebär således att kraven på proportionalitet och nödvändighet inte behövde tillämpas när inskränkningar i den personliga integriteten gjordes.

Sammanfattningsvis var alltså datalagringsdirektivets huvudregel ett åläggande mot operatörerna om en omfattande uppgiftsinsamling baserad på brottsbekämpande ändamål, vilket var raka motsatsen till hur frågan om lagring och integritet hade bedömts i E-Privacy-direktivet som istället alltså har konfidentialitet som utgångspunkt. För svensk del genomfördes datalagringsdirektivet genom en reform av LEK och de ändringar som gjordes i lagen präglar gällande rätt. Nedan följer en sammanfattning av

---

av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG. se prop. 2010/11:46 s. 11, SOU 2007:22 s. 300 jfr skäl 10 i direktivet.

[203] Skäl 7–11 preciserar syftet i artikel 1.1 jfr med skäl 21. Prop. 2010/11:46 s. 12.

[204] Cameron (2015) s. 136.

[205] JUNO internet, lag (2003:389) om elektronisk kommunikation 6 kap. 16 a §, not 288, 2021-02-20 och Förslag till Europaparlamentets och rådets direktiv om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG, KOM (2005) 438 slutlig.

[206] SOU 2007:22 s. 301.

[207] SOU 2008:3 s. 273–274 och prop. 2010/11:46 s. 47.

[208] Prop. 2010/11:46 s. 1, 12–13 och 39 och SOU 2017:75 s. 142.

lagstiftarens resonemang om hur avvägningen mellan personlig integritet och datalagring av brottsbekämpande ändamål skulle utformas.

4.5.2 Datalagringsdirektivets genomförande i Sverige – en utvidgning av LEK

Regeringens utgångspunkt vid genomförandet av det nya lagringskravet var att tillgodose brottsbekämpningens behov av trafikuppgifter samtidigt som den enskildas integritet skulle värnas.[209] Under remissförfarandet ifrågasattes inte att tillgång till trafikuppgifter var av stor vikt för brottsbekämpningen, men samtidigt konstaterades att en lagring per se skulle innebära ett intrång i den personliga integriteten. JO och Datainspektionen (sedan 2021-01-01 Integritetsskyddsmyndigheten) var två av de instanser som betonade vikten av att i möjligaste mån begränsa de ingrepp i den personliga integriteten som det nya kravet innebar. De anförde dock att ”det konstateras att avvägningen mellan brottsbekämpning och integritetsskydd i allt väsentligt är given i direktivet”.[210] Positiva var även Tullverket och Svenska Antipiratbyrån som menade att utredarna ”på ett tillfredsställande sätt har belyst avvägningen mellan behovet av tillgång till trafikuppgifter och skyddet för den personliga integriteten.”[211] Desto hårdare kritik kom bland annat från Sveriges advokatsamfund och Juridiska fakulteten vid Lunds universitet som menade att utredningen i allt för hög grad betonade brottsbekämpningsintresset, på bekostnad av skyddet för den personliga integriteten. Internetleverantören Bahnhof AB ansåg att direktivet inte skulle genomföras eftersom det i så hög grad inkräktade på den personliga integriteten.[212]

Som beskrivet ovan möjliggör visserligen artikel 15.1 i E-Privacy-direktivet att trafikuppgifter får lagras och lämnas ut till exempel för att enskilda ska kunna tillvarata sina rättigheter i en civilrättslig process. Den lagringsskyldighet som datalagringsdirektivet medförde omfattade alltså enbart brottsbekämpande ändamål. Vid sidan av den skyldigheten fortsatte de befintliga allmänna reglerna om behandling av trafikuppgifter i ovan beskrivna 6 kap. 5, 6 och 8 §§ i LEK, att gälla. Det vill säga leverantörerna av den elektroniska kommunikationen lagrade redan trafikuppgifter för bland annat fakturering. Avseende dessa uppgifter har lagen fortsättningsvis föreskrivit att reglerna om utplåning och avidentifiering i 6 kap. 5 § ska gälla. De här lagringsmöjligheterna som fanns i lagens ursprungliga form, sågs av regeringen som ett problem eftersom myndigheternas möjlighet att tillgå uppgifter var helt beroende av vad för uppgifter som operatörerna hade lagrat, och då alltså av andra skäl än för att finnas tillgängliga för brottsbekämpande ändamål. Lagring kom de facto att bero på fakturering av användarna eller för att förhindra obehörig användning av ett elektroniskt

[209] Prop. 2010/11:46 s. 16 jfr 2010/11: JuU14 s. 6–7 och 2011/12: JuU28 s. 5–7.
[210] Prop. 2010/11:46 s. 17, till grund för genomförandet låg SOU 2007:76.
[211] Prop. 2010/11:46 s. 17.
[212] Ibid.

kommunikationsnät. Både typen av uppgift som lagrades och tillhörande lagringstid var således styrda av praktiska faktorer snarare än de brottsbekämpande myndigheternas behov. Lagstiftaren befarade dessutom att tekniska framsteg eventuellt kunde medföra att operatörerna i framtiden inte skulle behöva lagra uppgifter för sin egen räkning i någon större utsträckning. För de brottsbekämpande myndigheterna skulle detta således innebära en minskad möjlighet att få ut information.[213]

Regeringen konstaterade att den absoluta merparten av de uppgifter som skulle börja att lagras inte skulle begäras ut för brottsutredningar, utan de skulle raderas då lagringstiden hade upphört utan att någon hade tagit del av dem: ”Detta skiljer sig inte från vad som i dag gäller i fråga om de trafikuppgifter som nät- och tjänsteleverantörerna lagrar för egna syften och som är tillgängliga för de brottsbekämpande myndigheterna.”[214] Gällande integritetsaspekten av den nya lagringen framhölls att ett intrång skedde vid lagring genom att den enskilda skulle uppleva att den privata sfären blev inskränkt: ”Lagringen skulle kunna leda till att enskilda i viss utsträckning avstår från att använda elektroniska kommunikationsmedel i syfte att undvika att uppgifter registreras.” Med hänvisning till 2 kap. 6 § RF (i dåvarande lydelse) och att det var förtroligheten i meddelande som skyddades menade regeringen att de föreslagna lagringskraven inte omfattades av denna grundlagsbestämmelse och detta eftersom lagringen alltså inte skulle omfatta själva innehållet i trafikuppgifterna.[215] Vid den här tiden hade riksdagen beslutat om att genomföra reformer av regeringsformen, men regeringen menade att det nyinförda andra stycket i 2 kap. 6 § RF tillät det integritetsintrång som de nya bestämmelserna i LEK skulle komma att innebära, detta eftersom inskränkningar i integritetsskyddet genom lag fortfarande skulle vara tillåtna enligt dåvarande lydelse av regeringsform 2 kap. 12 §, (nuvarande 2 kap. 20–22 §§ RF).[216]

Regeringen menade att direktivets uppräkning av de uppgifter som omfattades av datalagringen vägdes upp av ”… flera artiklar som ska garantera en rimlig proportion mellan intresset av att allvarliga brott avslöjas, utreds och lagförs respektive skyddet för enskildas integritet. Det gäller t.ex. den längsta acceptabla lagringstiden, att uppgifterna ska utplånas vid slutet av den tiden och att uppgifterna ska skyddas mot olika åtgärder som är skadliga från integritetsskyddssynpunkt.” [217] Målet var att åstadkomma ett transparent system som möjliggjorde att medborgarna kunde förutse vad för uppgifter om dem som skulle komma att lagras och hur de skulle användas i brottsbekämpningen. För att åstadkomma detta skulle lagringen enbart få ske om den kunde motiveras med stöd av artikel

[213] Prop. 2018/19:86 s. 84, prop. 2010/11:46 s. 18, 39.
[214] Prop. 2010/11:46 s. 18.
[215] Prop. 2010/11:46 s. 18–19 jfr prop. 1973:90 s. 243 och prop. 1975/76:209 s. 147 ff.
[216] Prop. 2010/11:46 s. 19 jfr prop. 2009/10:80. KU bedömde att den lagring som föreslogs i prop. 2010/11:46 omfattades av 2 kap. 6 § andra stycket RF, men var en grundlagsenlig inskränkning, JuU14 s. d 55–58.
[217] Prop. 2010/11:46 s. 20.

15. 1 i E-Privacy-direktivet. Detta innebar alltså ett förstärkt skydd eftersom artikeln uppställer krav på att en inskränkning av integritetsskyddet enbart får ske om åtgärden är nödvändig, lämplig och proportionell.[218]

I ett annat avseende valde regeringen dock att genomföra en lagringsskyldighet som gick utöver direktivet i och med att även en misslyckad uppringning skulle omfattas av lagen. Detta eftersom den utredning som föregick förslaget hade konstaterat att det fanns ett sådant behov hos de brottsbekämpande myndigheterna. Flera remissinstanser ställde sig dock kritiska till denna utvidgning. Sveriges advokatsamfund och TeliaSonera AB anförde bland annat att direktivet var en mycket kontroversiell lagstiftning och påpekade att det föregicks av en omfattande debatt över hela Europa. Detta menade de talade för att direktivet i så stor utsträckning som möjligt skulle genomföras inom de i direktivet givna ramarna. Även PTS framhöll att regeringen borde invänta hur tillämpningen av direktivet utvecklade sig på europeisk nivå innan operatörernas lagringsskyldighet utvidgades. Regeringen å sin sida menade att även om ”människors allmänna obehag inför att information om dem lagras” inte skulle underskattas, så vore det ”orealistiskt att utesluta detta växande informationsfält från de brottsbekämpande myndigheternas insyn.”[219] Regeringen ansåg att det var motiverat att lagringsskyldigheten skulle omfatta misslyckade uppringningar och lokaliseringsuppgifter vid samtalets slut för mobiltelefoni. Bland remissinstanserna var JO inne på samma linje som regeringen och hade inget att invända mot ett i vissa avseenden utvidgat lagringskrav. Detta mot bakgrund av att sedan skälen för lagring hade bedömts motivera ett intrång i integritetsskyddet, så borde brottsbekämpningsintresset ”väga relativt tungt.” Regeringen instämde i JO:s påpekanden. Däremot uteslöts lagring av pågående samtal eftersom det skulle föranleda en enormt stor lagring och skulle ”i princip innebära att t.ex. alla mobilanvändares rörelser under pågående samtal skulle lagras…”.[220] Likaså uteslöts myndigheternas önskan om att kunna få tillgång till data rörande besök på websidor eftersom det skulle ”innebära en betydande utvidgning i förhållande till de skyldigheter som följer av direktivet”.[221] Främst integritetsskäl men även kostnads-och konkurrensaspekter för operatörerna talade emot detta.[222]

Det framstår som att datalagringsdirektivet var mycket välkommet av lagstiftaren eftersom informationstillgången för de brottsbekämpande myndigheterna innan datalagringsreformen alltså stod och föll med operatörernas allmänna trafiklagring av det som benämns som ”andra skäl”. Brottsbekämpningens övertrumfande av andra aspekter visar sig även i att bland annat PTS och Stockholms handelskammare påtalade vilken konkurrensnackdel förslaget skulle innebära för svenska operatörer. En utökad lagring av integritetskänslig information skulle höja tröskeln för

[218] Prop. 2010/11:46 s. 20.
[219] Prop. 2010/11:46 s.31, 34–35.
[220] Prop. 2010/11:46 s. 35.
[221] Ibid.
[222] Prop. 2010/11:46 s. 32-35.

inträde på marknaden (små företag hade kanske inte de senaste servrarna och televäxlarna), leda till ökade kostnader för hanteringen av informationen och dessutom skapa en svåröverskådlig marknad för aktörerna. För företag verksamma i flera länder skulle dessutom anpassningskostnader av olika system uppstå. Regeringen menade dock att det fanns andra medlemsländer som skulle ha längre och mer omfattande lagring än i Sverige och att den svenska utformningen därför var berättigad. Regeringen anförde ” Även med beaktande av intresset av enskildas integritetsskydd samt kostnads- och konkurrensaspekter bedöms en sådan lagringsskyldighet vara proportionerlig i förhållande till ändamålet att ge de brottsbekämpande myndigheterna tillgång till behövliga uppgifter för att avslöja, utreda och lagföra brott. Lagringsskyldigheten utgör enligt regeringens uppfattning inte heller något hot mot den fria åsiktsbildningen.”[223]

Däremot var regeringen desto mer restriktiv och värnade den personliga integriteten framför brottsbekämpning när det kom till lagringstiderna. Som anförts ovan medgav artikel 6 i datalagringsdirektivet en lagring mellan 6 månader och 2 år. Bland annat Åklagarmyndigheten menade att äldre samtalslistor många gånger hade lett till att brott kunde klaras upp. Även Säpo vittnade om detta och framhöll att ett direktivets utlösande faktorer, terrordådet i Madrid 2004, hade lett till att historiska trafikuppgifter från Sverige hade efterfrågats av spanska myndigheter. Regeringen menade att strikt sett ur ett brottsbekämpningsperspektiv skulle därför en lagring på mer än två år kunna motiveras, dock innebar redan lagringen som sådan ett integritetsintrång, och att upplevelsen av detta intrång hade ett samband med lagringens omfattning. Därtill uttrycktes att risken för integritetsskador genom otillåten spridning ökade med längre lagringstider och därför beslutades om kortast möjliga tid, 6 månader. Gällande kostnaden för att identifiera och lagra trafikuppgifter bedömdes den till 200 miljoner kronor, vilket operatörerna skulle bekosta. Det allmänna skulle stå för kostnaden för ersättning till leverantörerna vid utlämnande av uppgifter som bedömdes uppgå till 20 miljoner kronor årligen. Bedömningen var att trafikuppgifter skulle begäras ut av rättsväsendet i ökad grad, vilket dock vägdes upp av de effektivitetsvinster i form av snabbare utredning som det skulle medföra. [224]

Datalagringsdirektivets genomförande innebar sju nya paragrafer till kapitel 6 i LEK: 6 kap. 3 a § och 16 a–16 f §§ som trädde i kraft den 1 maj 2012. I de senare finns grundläggande bestämmelser om lagringsskyldighet av trafik- och användaruppgifter för brottsbekämpande ändamål för de bolag som tillhandahåller elektroniska kommunikationsnät eller kommunikationstjänster. 6 kap. 3 a § stadgar att den som är skyldig att lagra uppgifter enligt 16 a § måste vidta särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling och att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana skyddsåtgärder. Av det paket med paragrafer som infördes kommer den fortsatta framställningen att vara koncentrerad kring 6 kap. 16 a och 16 d §§ då övriga paragrafer ligger

[223] Prop. 2010/11:46 s. 32 och 35–37.
[224] Prop. 2010/11:46 s. 38 – 39, 64, 68, 70.

utanför uppsatsen syfte. Den första av dessa, 16 a §, är helt central eftersom paragrafen reglerar lagringsskyldighetens omfattning. [225] Vid genomförandet beslutades att alla de uppgifter som ansågs viktiga för att kunna spåra och identifiera en kommunikationskälla skulle lagras enligt 16 a §. Den som bedrev sådan anmälningspliktig verksamhet som framgår av lagens 2 kap. 1 § var skyldig att lagra uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut. Denna lagringsskyldighet omfattade uppgifter som hade genererats eller behandlats vid telefonitjänst (även misslyckad uppringning), meddelandehantering, internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform). Den lagringsskyldige fick överlåta lagringsuppdraget åt annan. Av paragrafen framgick att regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om vilka uppgifter som ska lagras enligt denna paragraf.

Som framgår rörde det sig således om en generell lagringsskyldighet för operatörerna avseende samtliga uppgiftstyper och registrerade användare. Per G. Andersson menar att ” lagring av trafikdata i den omfattning som blir aktuell enligt datalagringsdirektivet i sig kan anses utgöra ett beaktansvärt intrång i den personliga integriteten” och att lagringen möjliggjorde en ingående kartläggning av ”enskildas rörelsemönster, sociala umgänge och livsföring i övrigt”.[226] En annan aspekt framförs av Naarttijärvi, som menar att lagringens utformning i paragrafen inte är särskilt detaljerad vilket i förlängningen leder det till att kraven för lagringen i praktiken kan avgöras på myndighetsnivå och av tekniska standardiseringsinstitut. Det sker alltså en maktförskjutning från lagstiftar- till myndighetsnivå: ”Detta har ibland beskrivits som ett uttryck för en teknokratisk utveckling där de folkvalda inte anses kompetenta eller lämpliga att göra tekniska bedömningar.”[227] Den rent tekniska beskrivningen av vad som ska lagras regleras av 39–40 och 44 §§ i lagens förordning, FEK. Uppdelningen är gjord med beaktande av det integritetsintrång som lagringen innebär. Regeringen bedömde att detta var förenligt med regeringsformens skydd av den personliga integriteten.[228] Även här är Naarttijärvi dock kritisk och menar att den faktiska effekten av regleringen är att lagstiftningen kan styras av regeringen, utan riksdagens deltagande.[229] Samtidigt, till lagstiftarens försvar, kan sägas att det hade kunnat bli tungrott om riksdagen skulle godkänna varje enskild förordningsändring rörande lagringens tekniska specifikation som regeringen skulle vilja genomdriva.

[225] SOU 2017:75 s. 137–138, prop. 2010/11:46 s. 1, 8–9, 11, 77–78. bet. 2011/12: JuU28, rskr. 2011/12:165–166 jfr prop. 2018/19:86 s. 16. Se även kommentar till lag (2003:389) om elektronisk kommunikation 6 kap. 16 a § JUNO, not 288, 2021-02-20.
[226] JUNO, lag (2003:389) om elektronisk kommunikation 6 kap. 16 a §, not 288, 2021-02-20.
[227] Naarttijärvi (2013) s. 276.
[228] Prop. 2010/11:46 s. 28, prop. 2018/19:86 s. 38–39.
[229] Kritik i Naarttijärvi (2013) s. 469. För fördjupande diskussion se även Wenander (2016).

Den andra av dessa centrala paragrafer, 16 d §, reglerar lagringstiden. Vid tidpunkten för införandet stadgades att de uppgifter som avsågs i 16 a § skulle lagras i sex månader räknat från den dag då kommunikationen avslutades och därefter genast raderas av den lagringsskyldige. Uppgifter som hade begärts ut före utgången av lagringstiden fick även lämnas ut senare om uppgifterna inte hade hunnits lämnas ut innan fristen löpte ut.

Sammanfattningsvis har datalagringsdirektivet satt spår i LEK genom att det idag finns ”två uppgiftsmängder” som löper parallellt.[230] Det tål att upprepas inför den fortsatta framställningen att utöver de uppgifter som operatörerna *har möjlighet* att lagra för sina egna ändamål, finns det uppgifter som operatörerna är *ålagda* att lagra för brottsbekämpande ändamål. Det är alltså den senare lagringsformen som tillkom på grund av datalagringsdirektivet. I nästa kapitel beskrivs två avgöranden från EU-domstolen som medförde att den svenska avvägningen mellan personlig integritet och brottsbekämpning kom på skam.

[230] Prop. 2018/19:86 s. 84.

5 Digital Rights och Tele2 – avgörande rättsfall för Sverige

5.1 Digital Rights-domen

5.1.1 Bakgrund

I ett av datalagringsdirektivets skäl (22) framgick att det respekterade EU-stadgans grundläggande rättigheterna och att det tillsammans med E-Privacy-direktivet syftade till att ”säkerställa full respekt för medborgarnas grundläggande rättigheter med avseende på privatlivet och kommunikationer samt skyddet av deras personuppgifter…”, men bilden delades inte av EU-domstolen då den dömde i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., i april 2014.

Det första målet, C-293/12, gällde en begäran om förhandsavgörande från High Court, Irland och avsåg en tvist mellan Digital Rights Ireland Ltd och den irländska staten. Frågan var om lagenligheten av nationella lagstiftningsåtgärder beträffande lagringen av uppgifter om elektronisk kommunikation. Digital Rights yrkade att High Court skulle ogiltigförklara dels datalagringsdirektivet, dels ett avsnitt av den inhemska implementeringslagen. Den nationella domstolen ville därför få svar på hur datalagringsdirektivet förhöll sig till rätten till respekt för privatlivet i artikel 7 i EU-stadgan respektive artikel 8 i EKMR.

Det andra målet, C-594/12, avsåg en begäran om förhandsavgörande från österrikiska Verfassungsgerichtshof, och gällde prövningen av den lag genom vilken datalagringsdirektivet genomfördes i österrikisk rätt, i förhållande till grundlagen. Målen anhängiggjordes av bland annat delstaten Kärntens regering och 11 128 andra sökande. Dessa yrkade på ogiltigförklaring av en paragraf i implementeringslagstiftningen då de menade att denna kränkte den enskildes rätt till sina uppgifter. Den österrikiska domstolen frågade därför om datalagringsdirektivet var förenligt med EU-stadgans artikel 7, 8 och 11 med tanke på datalagringens omfattning liksom att majoriteten som skulle bli föremål för lagringen nästintill uteslutande avsåg personer vars beteende inte på något sätt motiverade att uppgifter om dem lagrades. Var ingreppet proportionerligt i förhållande till den målsättning som eftersträvades i direktivet?

I sitt svar till de båda nationella domstolarna inledde EU-domstolen med att konstatera att de uppgifter som skulle lagras ” kan sammantagna göra det möjligt att dra mycket precisa slutsatser om de personers privatliv, vilkas uppgifter har lagrats – såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i

övrigt, de aktiviteter som de utövar, deras sociala relationer och de umgängeskretsar som de rör sig i ” (p.27). EU-domstolen fann att direktivet innebar ett ”synnerligen allvarligt” intrång i rätten till privatlivet och skyddet av personuppgifter enligt artiklarna 7 och 8 i EU-stadgan och att lagringen kunde bidra till att berörda personer upplevde ”en känsla av att deras privatliv står under ständig övervakning” (p. 37).

Därefter övergick domstolen till att bedöma om ingreppet i EU-stadgans artiklar 7 och 8 dock kunde anses vara motiverat, eftersom det som i kapitel 3 beskrivet, är det möjligt att göra inskränkningar i det grundläggande skyddet så länge proportionalitetsprincipen beaktas. Begränsningarna ska då alltså vara nödvändiga och svara mot mål erkända av unionen (jfr p.38). Operatörernas lagringsskyldighet och myndigheternas tillgång till information kränkte trots allt inte det väsentliga innehållet i de rättigheter som EU-stadgan skyddar. Det materiella syftet med direktivet, att tillgängliggöra data för bekämpning av grov brottslighet och bidra till allmän säkerhet, motsvarade nämligen av unionen erkänt samhällsintresse. Detta baserat på domstolens praxis om bland annat bekämpandet av internationell terrorism (p. 41–42). Den enskilda har inte bara rätt till sin frihet utan även till personlig säkerhet.[231] Kravet att inskränkningen av en rättighet måste svara mot ett allmänt samhällsintresse var därmed uppfyllt (p. 44). Med detta konstaterat övergick domstolen till en mycket grundlig proportionalitetsavvägning.

Huvuddragen gick ut på att datalagringen var ägnad att uppnå direktivets mål eftersom denna innebar ökade möjligheter för myndigheterna att klara upp grova brott. (p.49) Dock menade man att även om detta säkerhetsmål var av allmänt samhällsintresse, kunde det inte ensamt motivera direktivets långtgående lagringsåtgärder (p. 51). Enligt fast praxis var det fastställt att skyddet av den grundläggande rätten till respekt för privatlivet var av sådan vikt att begränsningar av personuppgiftsskyddet ska inskränkas till ”vad som är strängt nödvändig” (p. 52). Lagstiftningen måste därför föreskriva tydliga regler så att personer vars uppgifter har lagrats har garantier som möjliggör ett effektivt skydd mot missbruk och otillåten tillgång till dessa (p. 54). Visserligen är en lagringsskyldighet en ändamålsenlig åtgärd för att uppnå syftet att upprätthålla allmän säkerhet och motverka allvarlig brottslighet. Detta i sig skulle därför kunna motivera intrång i de grundläggande rättigheterna, men då hade det krävts att direktivet skulle ha preciserade regler gällande omfattningen av rättighetsintrånget. Istället omfattades alla personer, elektroniska kommunikationsmedel och trafikuppgifter utan att det gjordes några åtskillnader, begränsningar eller undantag utifrån syftet att bekämpa allvarliga brott (p.57). Därtill gjordes ingen åtskillnad i lagringstid mellan de olika datauppgiftsslagen utifrån den funktion de skulle fylla. Här brast därför lagstiftningens objektivitet (p. 63–64). Därtill fanns säkerhetsbrister då det inte fanns några specifika föreskrifter om skydd av lagrade uppgifter (p. 66–67). Direktivets ingrepp i EU-stadgans grundläggande rättigheter var således inte avgränsat och därför

[231] Jfr SOU 2017:75 s.139, SOU 2015:31 s. 115 och Ds 2014:23 s. 104.

gick det inte att säkerställa att detta var absolut nödvändigt för att uppnå syftet (p. 65). Till sist konstaterades att unionslagstiftaren hade överskridit sin befogenhet vid direktivets antagande eftersom kraven på proportionalitet i förhållande till rättigheterna i artiklarna 7, 8 och 52.1 i EU-stadgan inte hade efterlevts. EU-domstolen ogiltigförklarade därför datalagringsdirektivet (p. 69, 71).

5.1.2 Konsekvenser av domen i Sverige

I och med direktivets ogiltigförklarande meddelade ett flertal svenska teleoperatörer att de inte avsåg att lagra data i enlighet med kapitel 6 i LEK. Detta eftersom domen indikerade att de nationella bestämmelserna stod i strid med grundläggande EU-rätt och därmed fanns det inget rättsligt stöd för att lagra uppgifter. PTS gick ut med att rättsläget var oklart och att myndigheten därför inte skulle utfärda straffavgifter för de bolag som inte lagrade data. Följden blev att två olika utredningar tillsattes.[232]

Först ut, den 29 april 2014, tillsatte justitieministern en särskild utredare som skulle granska de svenska reglernas tillämplighet mot bakgrund av domen. Detta utmynnande i en departementsskrivelse där utredaren Sten Heckscher kom fram till att det svenska regelverket avseende lagring enligt 6 kap. 16 a–f §§ LEK inte stod i strid med varken EU-eller europarätten. Han betonade att EU-domstolen hade underkänt datalagringsdirektivet utifrån en ”*samlad bedömning* av de utpekade omständigheterna…” och inte att domstolen kritiserade en generell och odifferentierad datalagring som sådan.[233] Detta menade Heckscher talade för att domen inte kunde tolkas som att domstolen hade ”redovisat en lista på åtgärder som i alla delar måste vara vidtagna för att regleringen inte ska anses oproportionerligt”.[234] Istället skulle föreskrifterna i LEK ses i ljuset av hur tillgången till uppgifterna reglerades. En generell lagringsskyldighet kunde inte per se göra lagen oproportionerlig, dessutom skulle en begränsning verka alltför menligt på brottsbekämpningen. Därtill framhölls att Sverige hade en lagringstid på direktivets miniminivå, vilket skulle uppfylla kravet på en strikt nödvändig begränsning, såsom domen föreskrev.[235]

Denna analys följdes sedermera upp av *Datalagring och integritet* (SOU 2015:31), som undersökte om det fordrades fler rättssäkerhets- och integritetsstärkande åtgärder för reglerna om lagring av uppgifter om elektronisk kommunikation. Kortfattat sagt drog utredarna även här slutsatsen att LEK var förenligt med EU-rätten, även om vissa förslag på förändringar presenterades.[236] Att teleoperatörerna däremot inte höll med blev tydligt i det som har kommit att kallas för Tele2-domen. Som nämnt

[232] Ds 2014:23 s. 104–105, Cameron (2015) s. 143, prop. 2018/19:86 s. 17.
[233] Ds. 2014:23 s. 23, 101 jfr C-203/15 och C-698/15 Tele2-domen, EU:C:2016:970 p. 46.
[234] Ds. 2014:23 s. 98.
[235] Ds 2014:23 s. 99–101 och SOU 2017:75 s. 21.
[236] SOU 2015:31 s. 15–16. För övriga förslag (som går utanför syftet här) se s. 16–21.

redan inledningsvis har denna haft en mycket stor inverkan på den svenska datalagringen och beskrivs i det följande.

5.2 Tele2-domen

5.2.1 Bakgrund

Utgången i Digital Rights-domen, det vill säga att EU-domstolen underkände datalagringsdirektivet, medförde att Tele2 Sverige AB, (Tele2 nedan) kort därefter underrättade PTS om att bolaget avsåg att upphöra med den datalagring i brottsbekämpande syfte och därtill radera de uppgifter som hade lagrats fram till tidpunkten för underrättelsen till PTS. Följden blev att Rikspolisstyrelsen lämnade in en anmälan till PTS om att Tele2 hade upphört att leverera uppgifter till polisen varpå PTS förelade bolaget att inom en angiven tid börja lagra igen. (p.44–45, 47 jfr p.1). Tele2 ansåg å sin sida att PTS hade tolkat Digital Rights-domen felaktigt och att den lagringsskyldighet som myndigheten ansåg förelåg stred mot EU-stadgan. Därför överklagades föreläggandet till Förvaltningsrätten i Stockholm, som dock ogillade detta genom dom den 13 oktober 2014, varpå detta överklagades till Kammarrätten i Stockholm. Där beslutades om vilandeförklaring av målet i väntan på förhandsavgörande från EU-domstolen. Kammarrätten önskade få klarhet i om en generell och odifferentierad lagringsskyldighet mot operatörerna, i ljuset av Digital Rights-domen, var förenligt med artikel 15.1 i E-Privacy-direktivet jämfört med artiklarna 7, 8 och 52.1 i EU-stadgan. Utgångspunkten var således att parterna var oense om räckvidden av Digital Rights-domen och dess inverkan på nämnda direktiv. Hur vid var egentligen Tele2:s datalagringsskyldighet och vad för tillgång skulle de nationella myndigheterna beviljas för de lagrade uppgifterna? (p.48, 51, 62–63). Det förhandsavgörande som sedermera meddelades av EU-domstolen den 21 december 2016, i de förenade målen C-203/15 och C-698/15, kom kort och gott att benämnas för Tele2-domen.

Inledningsvis konstaterade EU-domstolen att artikel 1.1 i E-Privacy-direktivet ska säkerställa ett likvärdigt skydd av de grundläggande rättigheterna, i synnerhet rätten till integritet och konfidentialitet vid personuppgiftsbehandling inom sektorn för elektronisk kommunikation. Dock undantas vissa verksamheter från direktivets tillämpningsområde enligt 1.3, bland annat då statens verksamhet på straffrättens område liksom försvar berörs (p. 68–69). Artikel 15.1 tillåter därför att de grundläggande rättigheterna i direktivet begränsas i den nationella rätten, under vissa angivna förutsättningar (jfr p 71). Syftet med de lagstiftningsåtgärder som artikel 15.1 medger, det vill säga att skydda nationell och allmän säkerhet, försvaret samt att förebygga, undersöka, avslöja och väcka åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem, konstaterar EU-domstolen också väsentligen sammanfatta de syften som de i artikel 1.3 listade verksamheterna har (p. 72). Detta till trots ska inte

direktivet tolkas som att de lagstiftningsåtgärder som avses i artikel 15.1 helt ska anses vara uteslutna från direktivets tillämpningsområde menade domstolen. Här måste nämligen direktivets systematik beaktas: ”Det skulle helt frånta den bestämmelsen dess ändamålsenliga verkan. Nämnda bestämmelse förutsätter nämligen med nödvändighet att de där avsedda nationella åtgärderna, såsom de om lagring av uppgifter i brottsbekämpande syfte, omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder endast under förutsättning att de däri angivna villkoren är uppfyllda” (p.73). Lagstiftningsåtgärder vidtagna av den svenska lagstiftaren som stödjer sig på artikel 15.1 och ålägger leverantörer av elektroniska kommunikationstjänster att tillhandahålla lagrade datauppgifter till svenska brottsbekämpande myndigheter, rör givetvis behandling av personuppgifter och omfattas därför av E-Privacy-direktivet konstaterade domstolen lakoniskt (p.74 och p. 78). Därför var direktivet tillämpligt på de svenska reglerna om datalagring (p.81). Vidare skulle tolkningen av artikel 15.1 vara strikt och ske mot bakgrund av EU-stadgan (jfr p. 89, 93).[237] EU-domstolens resonemang här om förhållandet mellan artikel 1.3 och 15.1 i E-Privacy-direktivet är inte helt tydligt och som utomstående är det svårt att begripa gränsdragningen mellan de båda artiklarna.

Trots detta något otydliga resonemang gick i alla fall EU-domstolen därefter vidare och konstaterade att LEK föreskrev ”en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter” och detta gällde alla abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel. Lagen ålade leverantörerna av elektroniska kommunikationstjänster ”att systematiskt och kontinuerligt lagra dessa uppgifter, utan undantag”. Huvudsakligen motsvarade den här lagringsskyldigheten alltså den som föreskrevs i det upphävda datalagringsdirektivet (p. 97) Utifrån uppgifterna gick det att ”dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats…” och medförde dessutom att det var möjligt att kartlägga berörda användare ”på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna” (p. 98–99). Detta betraktades som synnerligen allvarliga ingrepp i EU-stadgans artikel 7 och 8 och att lagringen skedde utan användarens vetskap kunde bidra med en ”känsla av att deras privatliv står under ständig övervakning” (p. 100, jfr p. 37 ovan i Digital Rights-domen). Lagringsmomentet kunde ha en inverkan på användarnas nyttjande av elektroniska kommunikationsmedel, och alltså i förlängningen vara menlig för yttrandefriheten. Ett sådant allvarligt ingrepp i privatlivet kan endast berättigas av bekämpandet av grov brottslighet (p. 101–102). Även om brottsbekämpningen i stor utsträckning kan vara beroende av moderna utredningstekniker kunde ingreppet inte i sig motivera en så pass långtgående lagringsskyldighet som LEK föreskrev (p. 103). Den svenska regleringen medförde att lagring av trafik-och lokaliseringsuppgifter blev huvudregeln, trots att direktivet stadgar att det ska vara ett undantag. Därtill innebar detta att alla operatörens användare

[237] Direktivets tillämplighet i sin helhet se p. 65–81 jfr prop. 2018/19:86 s. 23–24.

liksom alla elektroniska kommunikationsmedel, utan urskillning, omfattades även när det inte fanns något indicium om att ett beteende ens indirekt kunde ha samband med grov brottslighet. Regleringen var därför även tillämplig på personer vars kommunikation omfattades av tystnadsplikt. Detta frångick därmed det eftersträvade syftet med direktivets systematik.

Dessutom krävde LEK inget samband mellan de lagrade uppgifterna och ett hot mot den allmänna säkerheten och begränsades varken till en viss tidsperiod eller ett visst geografiskt område (p. 104–106). Slutsatsen var därför att LEK överskred gränserna för vad som ansågs som strängt nödvändigt och ansågs inte heller vara motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktivet i jämförelse med artiklarna 7, 8, 11 och 52.1 i EU-stadgan (p. 107).

Det finns inget hinder mot en lagstiftning som i förebyggande syfte tillåter en riktad lagring av trafik-och lokaliseringsuppgifter, i syfte att bekämpa grov brottslighet, men premissen är då att lagringen ska vara strängt nödvändig och att det av lagstiftningen tydligt ska framgå vad som ska lagras, vilka kommunikationsmedel och personer som avses liksom hur länge lagringen ska pågå. Särskilt ska preciseras under vilka omständigheter en sådan lagringsåtgärd får vidtas i förebyggande syfte eftersom det säkerställer en begränsad lagring. Det objektiva kravet är därför att ett samband måste kunna fastslås mellan det eftersträvade syftet och de uppgifter som är föremål för lagring (p.108–110 jfr Digital Rights p. 54). För att det ska gå att ta sikte på en viss personkrets krävs det att lagrade uppgifter om dessa individer ska kunna användas till att avslöja, direkt eller indirekt, en koppling till grov brottslighet, alternativt att uppgifterna kan bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten. En avgränsning av en personkrets kan göras genom ett geografiskt kriterium i de fall som de behöriga nationella myndigheterna, på grundval av objektiva omständigheter, bedömer att det i ett område finns en förhöjd risk för förberedelse eller genomförande av sådana handlingar (p.111).[238] Kammarrättens fråga besvarades därför med att artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i EU-stadgan, är ett hinder för nationell lagstiftning som i brottsbekämpande syfte, föreskriver en generell lagring av alla trafik – och lokaliseringsuppgifter för alla operatörens användare och alla typer av elektroniska kommunikationsmedel (p. 112).

5.2.2 Konsekvenser av domen i Sverige

Kammarrätten konstaterade att det med hänsyn till domen stod klart att LEK:s bestämmelser om lagring av trafikuppgifter för brottsbekämpande ändamål inte var förenliga med EU-rätten. Detta medförde att PTS inte heller hade något lagstöd för sitt föreläggande mot Tele2.[239] För de

[238] Jfr C-511/18, C-512/18, C-520/18 La Quadrature du Net m.fl., EU:C:2020:791 p. 149.
[239] Kammarrätten i Stockholm mål 7380–14, dom 2017-03-07.

brottsbekämpande myndigheterna innebar Tele2-domen alltså att de var tillbaka till den lagring som fanns att tillgå hos operatörerna innan datalagringsdirektivet trädde i kraft, det vill säga den lagring som skedde av praktiska, snarare än av brottsbekämpande ändamål.

5.3 Slutsatser av Digital Rights- och Tele2-domen

En följd av Tele2-domen var att den nationella datalagringsregleringen i många medlemsländer framgent behövde reformeras och de lagstiftande kvarnarna satte därför igång att mala runt om i unionen.[240] Från svenskt perspektiv menar jag att Tele2-domen kan sägas vara ”spiken i kistan” avseende den analys som de båda utredningarna gjorde efter Digital Rights-domen. Resonemanget om att det rörde sig om en s.k. *samlad bedömning* (utredarnas kursivering) utifrån de omständigheter som förekom i Digital Rights var därmed helt passé. Av Tele2-domen framkommer nämligen med all tydlighet att den svenska lagringen de facto underkändes då den var alltför omfattande. Med denna dom preciserade EU-domstolen vad som krävs av den nationella rätten för att den ska vara godtagbar utifrån EU-stadgans integritetsföreskrifter. Trots det som uttalades i departementsskrivelsen från 2014 om att Digital Rights-domen inte skulle betraktas som en ”lista på åtgärder” till den nationella lagstiftaren, kom Tele2-domen, som i mångt och mycket upprepar EU-domstolens ståndpunkter från Digital Rights-domen, att just utgöra en grundplåt vid reformarbetet av LEK:s kapitel 6. Resultatet av detta utgör, sedan den 1 oktober 2019, gällande rätt.

Slutligen får sägas att datalagringsdirektivet är ett exempel på brottsbekämpande åtgärder där, för att låna Integritetsskyddskommitténs formulering, ”lagstiftaren tonar ned integritetshänsynen och hastar fram lagstiftning när de yttre hoten mot samhället ökar eller upplevs ha ökat.”[241] Samtidigt kan det folkliga stödet för en sådan lagstiftning vara stark. I en av kommitténs attitydundersökningar framgick att majoriteten av den svenska befolkningen ansåg att den statliga kontrollen över medborgarna ”bör öka ytterligare i syfte att motverka terrorism och grov brottslighet.”[242] Tankarna går här osökt till ”jag-har-inget-att-dölja-argumentet.” Kommittén å andra sidan menade att det från integritetshänseende är oacceptabelt att yttre hot på detta vis skulle tas till intäkt för en mindre grundlig proportionalitetsbedömning av lagstiftaren då lagstiftning tas fram.[243] Således var detta även vad EU-domstolen konstaterade i Digital Rights-domen, och sedermera upprepade i Tele2-domen. Domarna illustrerar på detta vis den avvägningsproblematik som råder mellan integritet och brottsbekämpning. I kölvattnet av Tele2-domen har följt nya

[240] Internationellt reformarbete se prop. 2018/19:86 s. 137 och SOU 2017:75 s. 185–193.
[241] SOU 2007:22 s. 470.
[242] SOU 2007:22 s. 470.
[243] Ibid jfr ovan avsnitt 2.5 om svenskars generella inställning till personuppgiftshantering.

frågeställningar om hur den fortsatta maktfördelningen mellan EU och medlemsstaterna ska se ut när det gäller den datalagring som sker mot bakgrund av nationell säkerhet. Detta berörs i nästa kapitel, liksom avvägningen som gjordes mellan integritets- respektive brottsbekämpningsaspekten vid reformen av LEK.

6 Nya regler om datalagring för brottsbekämpning

6.1 Nationell översyn efter Tele2-domen

6.1.1 Reform av LEK:s lagringskrav

Följande avsnitt syftar till att ge en bild av hur regeringen resonerade kring den enskildes integritet och databehovet hos de brottsbekämpande myndigheterna då de lagändringar i 6 kap. 16 a och 16 d §§ LEK som trädde i kraft 2019 togs fram. Det är alltså den lagring som operatörerna är skyldiga att lagra av brottsbekämpande ändamål som kommer att behandlas och inte den praktiska lagring som även förser de brottsbekämpande myndigheterna med information. Som framgick av Tele2-domen var det den förstnämnda lagringssorten som underkändes. Även om det redan har förklarats under dispositionsavsnittet ska här återigen sägas att detta kapitel 6 är en fortsättning på uppsatsens kapitel 4. Anledningen till denna ordningsföljd är som ovan beskrivet att domarna i kapitel 5 är en förutsättning för att läsaren ska kunna ta till sig innehållet i detta kapitel. Kommande kapitel reflekterar därför innehållet i kapitel 4 och 5. Här återknyts även till det som har förklarats i kapitel 2 om de brottsbekämpande myndigheternas behov av datalagring.

Inledningsvis ska sägas att regeringen i förarbetena konstaterade att intresset av att bekämpa grov brottslighet inte ensamt kunde motivera den generella lagring som Sverige hade vid tiden. Samtidigt försvarade lagstiftaren sig mot EU-domstolens kritik genom att konstatera att LEK inte omfattade alla trafik- och lokaliseringsuppgifter, till exempel uteslöts lagring av position vid meddelandehantering, liksom enhetens positionen under pågående mobilsamtal.[244] Knäckfrågan var alltså hur lagstiftaren skulle säkra möjligheten till en effektiv brottsbekämpande verksamhet och samtidigt anpassa den svenska datalagringen så att den levde upp till EU-rättens krav på den personliga integriteten. I motiven framhölls vikten av tillgång till lagrad datatrafik eftersom lagstiftaren strävade mot att åstadkomma en ändamålsenlig tillämpning av behovs- och proportionalitetsprincipen som alltid gäller vid användning av tvångsmedel i svensk rätt. Datauppgifter möjliggör att de brottsbekämpande myndigheterna vid brottsmisstanke ska kunna kontrollera denna effektivt och med minsta möjliga integritetsintrång. Utan tillgång till uppgifterna vid brottsutredningar skulle detta kunna leda till att myndigheterna behöver använda sig av andra mer ingripande metoder sett ur ett integritetsperspektiv, såsom exempelvis hemlig avlyssning istället för inhämtning av lokaliseringsuppgifter.[245]

[244] Prop. 2018/19:86 s.22 och 30–31.
[245] Prop. 2018/19:86 s. 28–29 och 108.

Samtidigt påtalade remissinstanserna Polismyndigheten, Åklagarmyndigheten, Säpo och Tullverket att varje begränsning av lagringsskyldigheten skulle innebära allvarliga konsekvenser för brottsbekämpningen. Likaså var företrädare för olika upphovsrättsliga intresseorganisationer oroliga för att en begränsning av datalagringen skulle medföra att immaterialrättsliga brott skulle bli svårare att lagföra. Vidare påpekade Rädda barnen hur stor betydelse datalagringen har för sexualbrott mot barn. En annan form av kritik kom från bland andra Svea hovrätt som menade att utredningens förslag på författningsändringar var ”marginella och att förslagen även fortsättningsvis innebär en generell lagring.”[246] Det var därför mycket som talade för att förslagen var otillräckliga för att göra den nationella rätten förenlig med EU-rätten.[247]

6.1.2 Vilken lagringsmodell skulle väljas?

6.1.2.1 Att begränsa trafik – och lokaliseringsuppgifter

För det första stod regeringen inför valet mellan en så kallad riktad lagring, alternativt en begränsad lagring. Den förstnämnda är en situationsanpassad förebyggande lagring av uppgifter hänförliga till vissa personer, nummer eller platser samt vilka kommunikationsmedel som avses. Lagringen är alltså inriktad på vilka slags uppgifter som ska lagras och hur länge det ska fortgå. Som framgår av Tele2-domen ska en sådan lagring begränsas till vad som är strängt nödvändigt (p. 108). Regeringen menade att en riktad lagring kunde framstå som en rimlig lösning med hänsyn till avvägningen mellan integritetsintrånget och brottsbekämpningens effektivitet.[248]

Lagringsformen kom dock att avfärdas som olämplig på flera vis. En orsak var svårigheten med att på förhand veta hur lagring ska riktas eftersom det inte går att säga vem som i framtiden kommer att begå ett brott. Att ringa in vissa personer eller områden på detta vis skulle förfela syftet med hela lagringen. Följden skulle bli olika förutsättningar för brottsutredningar beroende på var i landet man befann sig utifrån om en gärning eller brottsplanering skedde i ett ”lagringsområde”. I förlängningen skulle detta kunna leda till en brottslighet som anpassar sig genom att förlägga gärningar på platser utan datalagring. Dessutom är riktad lagring problematisk vid internetrelaterad brottslighet eftersom denna inte är geografiskt begränsad. Inte heller dåd som sker vid större evenemang som statsbesök ansågs gagnas av en geografisk lagring, eftersom planering och kontakter mellan gärningsmän troligtvis sker under en längre tid och inte bara på attentatsplatsen. Underrättelseverksamheten som krävs för att upptäcka denna typ av brott är långvarig och dessutom riktad åt ett stort geografiskt område. Vid en avvägning fann regeringen att en riktad lagring mot en personkrets som inte hade en konkret brottsmisstanke mot sig innebar en

[246] Prop. 2018/19:86 s. 23.
[247] Prop. 2018/19:86 s. 22 och 35.
[248] Prop. 2018/19:86 s. 30, 34 jfr Big Brother Watch and others v. the United Kingdom, nos. 58170/13, 62322/14, 24960/15, ECHR 2018-IX p. 316–317.

stor rättighetskränkning och riskerade att bli diskriminerande mot en del grupper eftersom en viss personkategori skulle pekas ut som mer brottsbenägen jämfört med andra. Detta skulle gå stick i stäv med ändamålsenligheten och proportionaliteten. Därtill skulle lagringen medföra sekretessproblematik eftersom operatörerna skulle informeras om att lagring skulle ske på vissa platser och tider. Även om inte alla de drygt 500 stycken operatörerna som finns i landet skulle beröras av beslut om riktad lagring, eftersom vissa av dem har mycket stor marknadsandel, sågs lagringsformen som starkt förknippad med risker i och med att information skulle spridas hos operatörsanställda.[249]

Alternativet blev istället en generellt minskad lagring och därmed även medföljande integritetsintrång. Därför beslutades att enbart samla in uppgifter från mobiltrafik, eftersom det nästan uteslutande var uppgifter hänförliga till mobiltelefontrafik som inhämtas av de brottsbekämpande myndigheterna. Dessutom framhölls att en mobiltelefon, till skillnad från en fast lina, oftast är personlig, vilket medför att den användande personkretsen minskar. Effekten blir därför ett mindre intrång vid varje lagringstillfälle. Ekobrottsmyndigheten, Polismyndigheten, Skatteverket och Tullverket, framhöll att slopandet av fast telefoni skulle minska statens möjligheter att utreda allvarliga brott. Regeringen menade dock att endast de uppgifter som bedömdes vara strängt nödvändiga att lagra skulle ingå i lagringsskyldigheten för att möta proportionalitetskravet.[250] Fast telefoni omfattas därför inte av lagringen idag.

Gällande lokaliseringsuppgifterna var det av stor vikt att dessa inte skulle ”strypas” i för stor skala eftersom det i förlängningen kan innebära en negativ inverkan på den personliga integriteten. Vid första anblick kan detta låta märkligt men resonemanget bygger på en samverkan mellan trafik-och lokaliseringsuppgifter. Försvinner den ena lagringstypen så ger den andra mindre information vilket måste kompenseras och då i form av ökad lagring av den andra sorten. Lokaliseringsuppgifterna utgör nämligen en sådan väsentlig del av analysen av en misstänkts kommunikation med andra och bidrar därför till att öka nyttan med alla de övriga trafikuppgifter som lagras. Som exempel nämndes att uppgifter om att A kontaktade B är mindre värd än en uppgift om att A kontaktade B när A befann sig på en specifik plats och B var på en annan plats. Därför menade regeringen att lagringen av lokaliseringsuppgifterna bidrar till att den sammantagna lagringen i LEK blev mer proportionerlig. Samtidigt framhölls att dessa lokaliseringsuppgifter i högsta grad är integritetskänsliga eftersom man kan dra slutsatser om en persons geografiska förflyttningar och därmed även av privatlivet för de personer som omfattas av lagringen. ”Det är emellertid det som gör lokaliseringsuppgifter till ett välanvänt och extremt värdefullt verktyg, både i den vanliga brottsbekämpande verksamheten och i

[249] Prop. 2018/19:86 s. 33–35.
[250] Prop. 2018/19:86 s. 35, 39–40. Tidigare utredningar: se t.ex. SOU 2015:31 s. 215, 253 och 262 och SOU 2012:44 s. 389, 447–448, 462 och 514.

underrättelseverksamheten.” Att minska lagringen av lokaliseringsuppgifterna sågs därför som uteslutet.[251]

Likaså ansågs det uteslutet att ta bort lagringen av obesvarade samtal, då dessa kan vara väl så intressanta som lyckade sådana. Misslyckade uppringningar används som koder mellan underrättelseofficerare och agenter, liksom för att signalera budskap mellan gärningsmän. LEK medger även lagring av uppgifter om första aktiveringen av anonyma oregistrerade kontantkort. Användningen av dessa har blivit allt vanligare innan grova brott begås. En analys av kontantkortens aktivering kan ge en indikation om inköpsställe som kan leda till en identifiering av innehavaren. Dessutom kan uppgifterna från kontantkorten kopplas till fjärraktiverade bomber. Då uppgifterna avser anonyma tjänster och inte avslöjar något om en persons privatliv bedömdes dessa som ”inte särskilt integritetskänsliga”.[252]

6.1.2.2 Begränsning av abonnemangsuppgifter

Följande stycke syftar till att analysera avvägningen som gjordes om abonnemangsuppgifterna.

Gällande utredningen av internetrelaterade brott är uppgifter om abonnemang för internet, det vill säga vem som har en viss IP-adress, den i särklass viktigaste uppgiften. Internetåtkomsten är även nyckeln till att identifiera personer som kommunicerar med medgärningsmän och underrättelseofficerare, liksom för värvning till terroristorganisationer. Då internetanvändningen ökar och därmed även internetbrottsligheten, menade regeringen att nyttan av uppgifterna är mycket stor. Abonnemangsuppgifter bedömdes inte vara särskilt integritetskänsliga, eftersom de endast anger att ett visst abonnemang har givits internetåtkomst. Dock är det möjligt att med uppgifterna, sammankoppla en fysisk person med avtryck som personen har lämnat efter sig på internet, och detta gör uppgifterna mer integritetskänsliga. Vid en bedömning av detta framhölls att det i majoriteten av alla fall gällande privatpersoner (på grund av vissa tekniska skäl) oftast rör sig om en begränsad tid som den här sammankopplingen mellan abonnent och spår på internet är möjlig att göra. Om man ska följa en abonnents internetanvändning krävs, utöver dessa digitala avtryck, en stor mängd abonnemangsuppgifter. Då besök på webbplatser inte omfattas av datalagringsskyldigheten menade regeringen att de uppgifter som ska lagras ”aldrig innebär att det kan kartläggas hur en person har trafikerat internet”.[253] För att myndigheterna ska kunna bekämpa brott som har begåtts eller planlagts över internet ansåg regeringen att det var nödvändigt att lagra uppgifter som möjliggör spårning av kommunikationskällan vid internetåtkomst såsom IP-adress, registrerad användare och abonnentuppgifter: ”Nyttan och behovet av att lagra uppgifterna är så stora att de uppväger det integritetsintrång som lagringen innebär”.[254]

[251] Prop. 2018/19:86 s. 41.
[252] Prop. 2018/19:46 s. 15 och 42, jfr SOU 2007:76 s. 159.
[253] Prop. 2018/19:86 s. 43.
[254] Prop. 2018/19:86 s. 43–44.

Precis som med telefoni-och meddelandehantering är också tidsangivelser och varaktighet av kommunikationen helt avgörande för att lagring av internetåtkomst ska bli verkningsfull. Uppgift om när en internetanvändare loggar in respektive ut i tjänsten som ger internettillgång gör att myndigheterna kan spåra en användare, och på så vis skilja ut denne från andra internetanvändare, eftersom en och samma IP-adress kan tilldelas flera användare vid olika tidpunkter. Här gavs som exempel situationer när någon har kontaktat barn på internet i sexuella syften. Polisen kan då, tack vare tidsangivelser i kombination med IP-adress från en leverantör av en så kallad chatt-app, ta reda på vilken abonnent det är som har använt ip-adressen vid den aktuella tidpunkten. Finns inte en tidsuppgift kopplad till den IP-adressen blir alltså uppgiften om internetåtkomst inte lika användbar. I synnerhet när det rör mobil uppkoppling blir detta viktigt. Detta eftersom utrustningen kopplar upp sig direkt mot en mast och då lagras en lokaliseringsuppgift vid internetåtkomsten. Utan en tidsangivelse fyller lokaliseringsuppgiften ingen funktion. Sambandet är en förutsättning för så kallad basstationstömning, vilket innebär att uppgifter om vilka uppkopplingar som har gjorts mot en viss mast under en specifik period begärs ut. Regeringen framhöll att då uppgifterna om internetåtkomsten inte ger någon information om användarens själva nyttjande av internet, utan alltså enbart ger en tidsangivelse till när användaren har haft internetåtkomst, kan det inte ses som särskilt integritetskänsligt. Däremot skvallrar internetåtkomsten om den enskildes kommunikationsmönster och tillsammans med annan information möjliggörs även att en abonnent kan sammankopplas med en IP-adress. Det senare menade regeringen medförde att uppgifterna ”i viss mån” är integritetskänsliga. Efter en sammantagen bedömning av nyttan av att lagra uppgifterna och det begränsade integritetsintrång som detta medför, ansågs att ”det är strängt nödvändigt att lagringsskyldigheten även fortsättningsvis omfattar uppgifterna i fråga”.[255]

Vid internetåtkomsten är det även viktigt att myndigheterna kan spåra kommunikationskällan för att på så vis kunna hitta den geografiska plats som internetanvändaren kommunicerar ifrån. Lagringsskyldigheten omfattar därför uppgifter som identifierar utrustningen där kommunikationen avskiljs till en abonnent, eller till den som slutligt avskiljer kommunikationen. För en lagringsskyldig operatör slutar alltså ansvaret vid denna utrustning. Härefter kan kommunikationen lämna ett nät som ägs av någon som omfattas av lagringsskyldighet. I synnerhet när utvecklingen går mot att allt fler människor använder alternativa appar med samtals-och meddelandefunktioner som tillhandahålls av leverantörer som inte omfattas av lagringsskyldighet, ”är uppgifterna hänförliga till internetåtkomst ännu viktigare än tidigare.”[256] Detta eftersom uppgifterna då kan följas så länge som möjligt innan de övergår till icke lagringsskyldig kommunikation. Kommunikationskedjans sista led är alltså av stor vikt för de brottsbekämpande myndigheterna. Det är inte ovanligt att denna omfattas av ett nät som inte omfattas av LEK:s lagringsskyldighet, exempelvis som för

[255] Prop. 2018/19:86 s. 44–45.
[256] Prop. 2018/19:86 s. 45.

en bostadsrättsförenings egna nät. Om det inte är möjligt att ta reda på var kommunikationen avskiljs från det lagringsskyldiga nätet kan myndigheterna inte heller gå till nätägaren för att därigenom hitta abonnenten. Mot bakgrund av detta menade regeringen att lagringsskyldigheten fortsättningsvis skulle omfatta en identifikation av utrustningen där kommunikationen slutligt avskiljs mellan den lagringsskyldige och den som slutligt avskiljer kommunikationen till den enskilde abonnenten. Kommunikationskällan är alltså viktig för att rätt slutanvändare ska kunna hittas. [257]

Gällande den mobila internetåtkomsten innebär lagring av denna ett ganska stort intrång då detta i realiteten utgör lokaliseringsuppgifter. Samtidigt framhöll regeringen att intrånget var mindre jämfört med vid telefonitjänst och meddelandehantering, eftersom det vid mobil internetåtkomst inte finns någon korresponderande uppgift om till exempel med vem eller när personen har kommunicerat. Därför sågs mobil internetåtkomst som strängt nödvändiga att lagra. Däremot framfördes från myndighetshåll att behovet av användarens anslutningsform vid internetåtkomst var en uppgift som värderades lägre än till exempel just beskrivna uppgift om kommunikationskällan. Här blir det tydligt hur man från lagstiftarhåll vägde funktionen mot integritetsaspekten och vad som krävdes för att en uppgift skulle kvalificera sig som strängt nödvändig. Anslutningsformen vid internetåtkomst togs därför bort från lagringsskyldigheten.[258]

”Att valet av teknisk lösning hos operatörerna är avgörande för om det går att spåra en brottsmisstänkt eller inte framstår som orimligt och även oavsiktligt” [259] Målet med den nya regleringen i 6 kap. 16 a § LEK var teknikneutralitet. Till exempel skulle inte identifikationen av en IP-adress stå och falla med operatörens tekniklösning. På grund av brist på IP-adresser enligt den vanligast förekommande standarden (benämnd IPv4) har det blivit vanligare att internetleverantörer använder en alternativ standard (s.k. NAT-teknik). Då detta samtidigt innebär att upp till 60 000 abonnenter delar på samma publika IP-adress har det givetvis orsakat problem för de brottsbekämpande myndigheterna. Därför var bland annat Åklagarmyndigheten positiv till utredningens förslag om att kunna identifiera slutanvändaren vid internetåtkomst genom denna alternativa teknik (NAT-tekniken). Detta skulle nämligen motverka problemet med den tilltagande anonymiseringen på internet, bakom vilken kriminella personer kan dölja sig. Av motiven framgår också att regeringen fortsättningsvis, genom lagens förordning, ska kunna föreskriva en lagringsskyldighet som möjliggör identifiering av en abonnent.[260] Under remissförfarandet kom dock kritik från Juridiska institutionen vid Umeå universitet som påpekade att utvidgningen av NAT-tekniken skulle möjliggöra ”en långtgående lagringsskyldighet och delegation av normgivningsmakt på ett område som

[257] Prop. 2018/19:86 s. 45–46.
[258] Prop. 2018/19:86 s. 46 jfr s. 36 och 113.
[259] Prop. 2018/19:86 s. 44.
[260] Prop. 2018/19:86 s. 37, 44 och 95.

påtagligt påverkar individens rättighetsskydd.”[261] Även PTS hade synpunkter och menade att detta ur integritetsperspektiv var känsligt eftersom det i praktiken innebär att uppgifter om varje internetsession hos dessa operatörer lagras. Därtill menade Datainspektionen att det var oklart hur lagring av internetåtkomsten skulle kunna vara teknikneutral med tanke på anonymiseringstjänster och VPN-tunnlar som tillhandahålls av vissa operatörer. Regeringen menade dock att den nya lagringen inte omfattade sådana tjänster, detta då dessa aktiveras först efter internetåtkomsten.[262]

Sammanfattningsvis och grovt förenklat, kan sägas att den övriga, komplexa tekniska kritiken mot regeringens lagförslag gick ut på att de insamlade uppgifterna som behandlas vid spårning av vem som har använt en vis IP-adress sammantaget ger en mycket exakt information om abonnentens internetkommunikation. Regeringen menade att möjligheten att identifiera slutanvändaren vid internetåtkomsten visserligen medför en utvidgning av datalagringen, men menade samtidigt att det var förenligt med EU-rätten. Den tillkommande informationen avser nämligen samma sakförhållande som den lagrade huvudinformationen, alltså den aktuella IP-adressen, och krävs för att det ska gå att utläsa något vettigt ur adressen. Regeringen menade därför att integritetsintrånget inte ökade ”särskilt mycket av att fler tekniska uppgifter lagras i syfte att få fram den grundinformation som på grund av den tekniska utvecklingen inte längre går att få fram enbart genom lagring av själva IP-adressen.”[263] Dessutom skulle möjligheten att spåra en abonnent, även vid så kallad NAT-teknik hos leverantören ” förväntas vara en tämligen verkningsfull förstärkning av de brottsbekämpande myndigheternas förmåga att klara upp brott som begåtts med hjälp av internet.”[264] Den återgivna avvägningen mellan personlig integritet och brottsbekämpande ändamål, avseende dels trafik-och lokaliseringsuppgifter, dels abonnemangsuppgifter, ligger till grund för den nuvarande lagringsskyldigheten. Vid en jämförelse med den äldre lydelsen av paragrafen, som beskrevs ovan under rubrik 4.5.2, är omfattningen av lagringen i andra stycket mindre och av nuvarande lydelse framgår att det enbart är uppgifter som har genererats via en mobil nätanslutning som ska lagras vid telefoni- och meddelandehantering. Avseende mobiltelefoni omfattas de som kopplar upp sig mot master eller trådlöst lokalt nätverk (wifi) som tillhandahålls av någon som omfattas av lagringsskyldigheten. Däremot utesluts de telefoner som ansluter till ett privat trådlöst nätverk.[265] Till skillnad från tidigare gäller inte lagringsskyldigheten uppgift om nummer som ett samtal styrts till.

[261] Prop. 2018/19:86 s. 38.
[262] Prop. 2018/19:86 s. 37–38 och 44.
[263] Prop. 2018/19:86 s. 44, 95.
[264] Prop. 2018/19:86 s. 109.
[265] Prop. 2018/19:86 s. 113. Förordning om ändring i förordningen (2003:396) om elektronisk kommunikation uppdaterades även under 2019 så att lagringsskyldigheten i 6 kap. 16 a § har en teknisk specifikation där, jfr SFS 2019:500.

6.1.3 Datalagringens tidsomfattning

Som framgår av Tele2-domen fick Sverige även nedslag på lagringstiden i 6 kap. 16 d §, och detta trots att dåvarande regering hade lagt sig på datalagringsdirektivets miniminivå med 6 månaders lagringstid för alla uppgifter, oavsett sort, från och med den dag som kommunikationen avslutades. Regeringens resonemang vid minskningen av lagringstiden presenteras i detta avsnitt.

Genom att differentiera lagringstiden för de olika uppgifterna, var det möjligt att för varje uppgiftskategori väga in integritetskänslighet i förhållande till de brottsbekämpande myndigheternas behov av just den uppgiftstypen menade regeringen. Detta skulle alltså göra lagstiftningen proportionerlig och leva upp till kravet om att lagring inte fick vara längre än vad som ansågs strängt nödvändigt och motiveras ”på objektivt godtagbara grunder” som Tele2-domen föreskrev. Föga förvånande möttes förslaget om generellt förkortade lagringstider av motstånd hos de brottsbekämpande myndigheterna. Åklagarmyndigheten och Tullverket påpekade att en förkortning av lagringstiden även innebar en motsvarande försämring av möjligheten till att utreda brott. Ekobrottsmyndigheten menade att det i deras verksamhet är viktigt att kunna följa uppgifter under en längre tid, eftersom det ofta rör sig om seriebrottslighet. Dessutom anmäls ekobrott ofta en lång tid efter att den brottsliga handlingen är begången och lagstiftarens förslag om en 2 månaders lagringstid för lokaliseringsuppgifter skulle medföra att vissa brott inte skulle kunna utredas. Även Säpo ansåg att blott 2 månader skulle innebära att det för deras del blev omöjligt att rekonstruera kommunikationens förgreningar.[266]

Motsatt ståndpunkt presenterades av Tele2 och Göteborgs tingsrätt som båda påpekade att uppgifter som identifierar var kommunikationen slutligt avskiljs från en lagringsskyldig till abonnenten är extra integritetskänsliga eftersom dessa är att likställa med lokaliseringsuppgifter. Göteborgs tingsrätt önskade därför en djupare analys av lagringstidens proportionalitet. Varför skulle uppgifter om internetanslutningen, lagras i sex månader när den i princip motsvarade lokaliseringsuppgifter, som alltså endast skulle få lagras i två månader då de är klassade som mer integritetskänsliga? Regeringen hänvisade här till hur statistiken för lagringsbehovet hos de brottsbekämpande myndigheterna ser ut och varför det fanns belägg för att införa diversifierade lagringstider för olika uppgiftskategorier. Majoriteten av de uppgifter som hämtas in inom underrättelseverksamhet och i polisens utredningsarbete är nämligen yngre än fem månader, vilket pekade i riktningen mot att man inte behövde ha en lagringstid som överskred fem månader. Detta skulle vägas mot att omfattningen av lagringsskyldigheten för operatörerna skulle minskas och den minskade lagringsomfattningen kunde framöver leda till att kartläggningen av elektroniska spår i brottsutredningar skulle ta längre tid. Dessutom visade underlag från myndigheterna att just vid bekämpning av grov brottslighet behövdes äldre

[266] Prop. 2018/19:86 s. 50.

uppgifter. Regeringen höll därför fast vid huvudregeln som säger att lagringen av uppgifter gäller under 6 månader. Från detta gjordes undantag i och med att lokaliseringsuppgifterna gör det möjligt att kartlägga en persons rörelsemönster kunde detta ”ge tämligen integritetskänslig information om en person.”[267] Regeringen ansåg efter ”en avvägning mellan den nytta uppgifterna innebär för de brottsbekämpande myndigheterna och det integritetsintrång uppgiften innebär ” att en lagringstid om två månader skulle föreskrivas för lokaliseringsuppgifter.[268]

Vidare framhöll regeringen att många av de uppgifter som är kopplade till internetåtkomst inte är särskilt integritetskänsliga då de i sig inte avslöjar något om själva kommunikationen, exempelvis vem en internetanvändare har haft kontakt med. Information om IP-adresser har ett tidsbegränsat användningsområde beroende på att uppgifterna kan växla med korta mellanrum, och detta menade man leder till att” uppgifternas integritetskänslighet är lägre än annars och att det finns ett större behov av att spara uppgifterna en längre tid.”[269] Därtill hänvisade regeringen till uppgifter från polisen som vittnade om att utredningar har fått läggas ned då lagringstiden på sex månader för just IP-adresser är för kort. Exempelvis hälften av alla barnpornografibrott med utlandskoppling har fått avslutas av den här anledningen, eftersom uppgifterna är avgörande för att finna gärningsmannen. Regeringen gjorde bedömningen att Tele2-domen inte specifikt rörde abonnemangsuppgifter, alltså exempelvis en IP-adress, och menade att dessa ”typiskt sett är mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter.”[270] Därför ansågs EU-rätten inte hindra en förlängning av lagringstiden för dessa till 10 månader. Detta menade regeringen utgjorde ”en rimlig avvägning mellan integritetsintresset och de brottsbekämpande myndigheternas behov.”[271] Denna bedömning hade ifrågasatts under remissförfarandet av bland annat Svea hovrätt, som menade att Tele2-domen inte gav stöd för en sådan tolkning och en utökning av lagringstiden till 10 månader. Däremot gällande de uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten, bedömde regeringen att dessa var mer integritetskänsliga än övriga uppgifter om internetåtkomst, och därför sattes lagringstiden för dessa till 6 månader.[272]

Regeringen svarade på remisskritiken genom att trycka på att uppgifter om abonnemang i sig enbart i en begränsad utsträckning kan användas för den typ av ingående kartläggning av enskilda som EU-domstolen ansåg utgöra en mycket ingripande begränsning av enskildas rättigheter enligt EU-stadgan. Därtill menade regeringen att EU-domstolen hade uttalat sig generellt om helheten i det svenska lagringssystemet och att Tele2-domen därför ”i första hand riktar in sig på de mer integritetskänsliga trafik-och

[267] Ibid.
[268] Ibid.
[269] Prop. 2018/19:86 s. 51.
[270] Prop. 2018/19:86 s. 51, 94 jfr C-207/16, Ministerio Fiscal, EU:C:2018:788, p. 63.
[271] Prop. 2018/19:86 s. 51.
[272] Prop. 2018/19:86 s. 51.

lokaliseringsuppgifterna" liksom att det inte gick att, med hänvisning till domen, dra slutsatsen att LEK:s bestämmelser om lagring och tillgång till abonnemangsuppgifterna stod i strid med EU-rätten.[273] För att förtydliga: detta var alltså lagstiftarens stöd för att ha längre lagringstider för just abonnemangsuppgifterna jämfört med trafik-och lokaliseringsuppgifterna.

Den här särbehandlingen fick omfattande kritik av flera remissinstanser. Bahnhof AB, Tele2 Sverige AB, Com Hem AB och Civil Rights Defenders ansåg att IP-adresser visst omfattades av domen och att Sverige inte kunde instifta en lag som föreskrev en lagring i 10 månader. De hänvisade till att E-Privacy-direktivet, inte gör någon uppdelning mellan abonnemangsuppgifter och trafik- och lokaliseringsuppgifter. Istället menade remissinstanserna att det viktiga är bedömningen av om en uppgift kan klassificeras som en konfidentiell personuppgift som därför skyddas av direktivet. Dessutom menade de att Tele2-domen "måste läsas i ljuset av Digital Rights-domen och bestämmelserna i det upphävda datalagringsdirektivet som omfattade IP-adresser." [274] En sådan tolkning skulle medföra att Tele2-domen innefattade IP-adresser. Vidare framhölls att IP-adresserna är "långt mer integritetskänsliga än uppgifter om t.ex. vem som står bakom ett mobiltelefonnummer."[275] Härtill kan nämnas att Kammarrätten i Stockholm 2018, kommenterade den dom från 2017 som föranledde Tele2-domen[276], och menade att den "innebär att lagring av uppgifter om t.ex. abonnemang för brottsbekämpande ändamål som sker på grund av den skyldighet som följer av 6 kap. 16 a § LEK inte är en tillåten behandling av uppgifterna (och det även om bestämmelsen i 6 kap. 16 a § inte upphävts)."[277] Även om det är ett kammarrättsavgörande tyder det på att även där uppfattades det alltså som att Tele2-domen likväl omfattade abonnemangsuppgifter.

Att meningarna går isär om abonnemangsuppgifterna särställning i lagstiftningen är uppenbart. Inställningen hänger givetvis ihop med de olika aktörernas egenintresse. Motsatt ståndpunkt än just beskrivna intog nämligen Åklagarmyndigheten, som menade att regeringens utredare hade gjort en riktig tolkning av Tele2-domen. Om inte skulle de brott som inte är grova, men där tillgången på abonnemangsuppgifter är avgörande för att kunna driva en framgångsrik utredning, bli mer eller mindre omöjliga att lagföra. Implicit innebär det straffrihet för vissa brott vilket står i strid med EKMR. Oklarheten med abonnemangsuppgifter föranledde Säkerhets- och integritetsskyddsnämnden att be om att klarhet skulle bringas av den exakta innebörden. Därtill efterfrågades en djupare analys av regeringen från bland andra Datainspektionen och PTS. Å andra sidan menade regeringen att med beaktande av Sveriges internationella åtagande, och då i synnerhet EKMR, är utrymmet för att ha ett regelverk som inte ger myndigheterna möjlighet

[273] Prop. 2018/19:86 s. 94, 97.
[274] Prop. 2018/19:86 s. 92.
[275] Ibid.
[276] Kammarrätten i Stockholm mål 7380–14, dom 2017-03-07, behandlades i kap 5.
[277] Kammarrätten i Stockholm mål 2471–18, dom 2018-12-14.

att komma åt uppgifter som de är i behov av begränsat.[278]

Den oklara klassificeringen som abonnemangsuppgifterna går under avspeglar sig i de varierande, och i viss mån obegripliga, lagringstiderna som föreskrivs. Med detta sagt och mot bakgrund av regeringens avvägning framgår lagringstiderna idag av 16 d § första stycket där det stadgas att uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. För lokaliseringsuppgifter är lagringstiden dock endast två månader. Dessa lagringstider framgår av första stycket första strecksatsen och det som omfattas är telefonnummer, abonnemangsidentitet, utrustningsidentitet, abonnent och tid för samtalet eller meddelandet. Hit hör även tid och plats för den första aktiveringen av ett kontantkort. [279] Gällande uppgifter som har genererats vid internetåtkomst ska dessa lagras i tio månader och om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska de enbart lagras i sex månader. Detta framgår av första stycket andra strecksatsen och syftar på uppgifter om IP-adress, abonnentuppgifter samt datum för in – och utloggning i den tjänst som ger internetåtkomst.[280] Precis som i den äldre lydelsen av paragrafen, som återgavs i kapitel 4, räknas lagringstiden från den dag kommunikationen avslutades och att den lagringsskyldige ska radera uppgifterna när lagringstiden har löpt ut såvida inte en begäran om utlämnande har kommit in innan lagringstiden har löpt ut. I sådana fall ska den lagringsskyldige fortsätta att lagra uppgifterna till dess att de lämnats ut och utplånas först efter utlämnandet. Detta framgår av andra och tredje stycket. Likaså framgår av sista stycket att regeringen med stöd av 8 kap. 7 § RF kan meddela närmare föreskrifter om lagringstiden enligt första stycket.

6.1.4 Konsekvenser av lagändringarna

Ovan har lagstiftarens avvägningar vid den nya datalagringen av brottsbekämpande ändamål beskrivits. I detta avsnitt behandlas de följdverkningar som denna nya reglering bedömdes medföra för den brottsbekämpande verksamheten, teleoperatörerna och enskilda.

En av de viktigaste konsekvenserna till följd av de nya lagringsreglerna i 6 kap. 16 a och 16 d §§ var att Sverige skulle leva upp till kraven om integritetsskydd i 15.1 i E-Privacy-direktivet. Färre lagrade uppgifter skulle leda till mindre information som i sin tur möjliggör att slutsatser kan dras om människors vanor. Så löd regeringens huvudresonemang. Därtill skulle skyddet förstärkas av att man i lagen införde ett förbud om att lagra information utanför EU. Sammantaget skulle integritetsvinster uppnås.

[278] Prop. 2018/19:86 s. 92, 98.
[279] Prop. 2018/19:86 s. 114. Sedan 1 maj 2021 gäller motsvarande för föreläggande att bevara en lagrad uppgift enl. 27 kap. 16 § RB, se lag (2021:240).
[280] Prop. 2018/19:86 s. 114. Sedan 1 maj 2021 gäller motsvarande för föreläggande att bevara en lagrad uppgift enl. 27 kap. 16 § RB, se lag (2021:240).

Eftersom detta skedde på bekostnad av brottsbekämpningen anfördes, likt i de äldre motiven, ”brasklappen” om att de brottsbekämpande myndigheterna fortfarande skulle ha tillgång till den datalagring som görs av operatörerna av praktiska skäl. Vad däremot gäller underrättelseverksamheten framfördes att den inte har något tvångsprocessuellt medel som skulle kunna kompensera för den minskade lagringen. I det stora hela skulle den förändrade lagringsskyldigheten kunna leda till en minskad brottsuppklaring, men det bedömdes ändå inte påverka ”brottsligheten i samhället i stort”.[281] Därtill kunde förändringen även medföra att myndigheterna i vissa fall skulle avstå från att hämta in uppgifter från operatörerna. Å andra sidan skulle dessa behöva ställa fler frågor för att få en fullständig bild eftersom ”svaret på varje fråga nu blir något mindre informationsrik”.[282]

För operatörerna skulle lagstiftningen bli en kostnadsdrivande faktor eftersom datasystemen skulle behöva anpassas, dock hade ingen summa kunnat uppskattas. Regeringen lutade sig mot samma bedömning som gjordes i förarbetena till den svenska implementeringen av datalagringsdirektivet, innebärande att operatörerna skulle stå för anpassningskostnader liksom drift och underhåll av systemen. För de brottsbekämpande myndigheterna utgår sedan en avgift till operatörerna vid uppgiftsutlämnande. Remisskritiken i denna del bestod i farhågor om att teleoperatörerna skulle åläggas nya skyldigheter som skulle blockera utvecklingsresurser och dessutom riskera att förloras om det framgent skulle visa sig att lagringsskyldigheten bryter mot EU-rätten, vilket dessa instanser menade sannolikt skulle bli fallet.[283]

En reflektion gällande operatörerna är att deras val av lagringsteknik har blivit en konkurrensfaktor bolag emellan på ett vis som kan tänkas medföra framtida problem för de brottsbekämpande myndigheterna. Teleoperatören Bahnhof skrädde inte orden inför att lagändringarna trädde i kraft: ”Inte nog med att upphovsrättsmaffian, stora molnjättar, sociala plattformar, webbläsare och hemsidor övervakar, registrerar och sparar data om dig på internet så har den svenska staten beslutat att med hjälp av lagen göra detsamma. Till sin hjälp har de beordrat Sveriges tele- och internetleverantörer att spara all person- och trafikdata så att polisen kan komma åt informationen – utan att det finns misstanke om allvarligt brott.”[284] Farhågorna om en handlingsdirigerande lagstiftning kan därför sägas ha besannats på ett vis som kanske inte var tänkt i propositionen. Vad som där diskuterades var att de individer som vill ”gå under radarn” skulle välja de elektroniska kommunikationsmedel som inte omfattas av lagen alternativt har kortast lagringstid. Vad däremot bolaget Bahnhof har valt att göra är helt enkelt att utnyttja att den lagring som sker av ”andra skäl” i 6 kap LEK och, såsom beskrivet ovan i kapitel 4, är avskild från den lagring som sker av brottsbekämpande skäl. Bahnhof har lagringen som ett

[281] Prop. 2018/19:86 s. 47 och 108–109.
[282] Prop. 2018/19:86 s. 111–112.
[283] Prop. 2018/19:86 s. 111, jfr 22–23 och prop. 2010/11:46 s. 63–70.
[284] Bahnhofs hemsida, publicerad 2019-09-30, länk se källförteckning.

säljargument:” Alla Bahnhofkunder kan vara säkra på att deras kunddata ligger i säkert förvar hos oss, att vi raderar efter 10 månader och att vi aldrig kommer att lämna ut uppgifter i annat fall än i enlighet med LEK. Det innebär att om någon annan frågar efter kunddata, t ex en domstol som hanterar civilrättsmål, så har vi inget att lämna ut eftersom våra kunders uppgifter är inlåsta i ”kassaskåpet som är avsedd för LEK.” [285]

För den enskilda kan tänkas att operatörernas ökade kostnader för genomförande av nu gällande regelverk har hamnat på abonnemangsräkningen. Utöver denna rena spekulation, skulle alltså lagändringen i alla fall gynna den enskilda genom integritetsvinster enligt regeringen. Mindre ingripande åtgärder än de som lagändringen medför bedömdes inte kunna göras.[286] En annan sak är givetvis att den enskilde kan påverkas negativt om brottsuppklarandegraden i samhället i stort sjunker.

6.1.5 Hur viktas brottsbekämpning mot integritet?

Vid en jämförelse av tongångarna hos lagstiftaren vid införandet av LEK, i förhållande till de författningsändringar som följde i kölvattnet av Tele2-domen, blir det tydligt att brottsbekämpande åtgärder generellt sett har hamnat högre upp på lagstiftarens agenda. Som framgår av genomgången utkristalliserar sig ett mönster i förarbetena eftersom regeringen inför varje lagringsslag som antingen har lagts till eller tagits har vägt integriteten för den enskilde mot de effekter det skulle kunna ha för de brottsbekämpande myndigheterna. Vid borttagandet av den fasta telefonin var motiveringen mycket tydlig, en lagringsform som inte är absolut nödvändig vägdes mot det faktum att det ofta är flera abonnenter som delar på en sådan förbindelse. Vidare måste de integritetskänsliga lokaliseringsuppgifterna, för att kunna omfattas av lagringen, kunna påvisa en mycket stor nytta för de brottsbekämpande myndigheterna. Visa vi bedömdes till exempel IP-adresser inte vara särskilt integritetskänsliga vilket avspeglar sig i en 10 månaders lagringstid till skillnad från standarden på 6 månader. Gällande lagringen av dessa IP-adresser är det som regeringen påpekar ofta det enda sättet att komma åt förövare av olika internetrelaterade brott. Samtidigt hade det varit önskvärt med ett mer utförligt resonemang från regeringens sida kring vad som faktiskt skiljer IP-adressen från lokaliseringsuppgifter avseende en mobiltelefon. Som flera remissinstanser har gett uttryck för är dessa uppgifter, sett från den enskildes perspektiv, i stort lika integritetskänsliga och ändå skiljer sig lagringstiden med 8 månader dessa uppgifter emellan. Motiveringen i denna del från regeringen är svepande och vad som utgör grunden för så pass olika lagringslängder ter sig oklart för en utomstående. I vissa fall kan lagstiftning vara i behov av viss ”elasticitet”, men när det som i det här fallet rör två tekniska lagringsformer

[285] Ibid.
[286] Prop. 2018/19:86 s. 47.

som verkar ge ungefär likartad integritetskänslig information blir resonemanget svårbegripligt.

En annan aspekt pekar Naarttijärvi på, nämligen att en proportionalitetsavvägning, som fordras då en rättighet i regeringsformen kan komma att inskränkas, måste utgå från aktuell teknik för att inte strida mot 2 kap. 21 § RF. "Ett lagrum som på grund av teknisk utveckling får en förändrad faktisk inverkan på den personliga integriteten torde alltså inte kunna luta sig på tidigare avvägningar, då lagstiftarens ändamål inte blivit föremål för samma förändring."[287] Han slår fast att strävan efter teknikneutralitet, på detta vis synliggör en konflikt mellan två rättsstatliga grundvärden: förutsebarhet, som fordrar klara och precisa regler, liksom stabilitet i regelverket, vilket på detta område alltså förutsätter ett visst mått av teknikneutralitet.[288] Samtidigt kan sägas att det är en brist i E-Privacy-direktivet att abonnemangsuppgifter inte definieras där.

Med den svenska lagringen i åtanke följer en kortare utblick på den tyska rättens motsvarighet till LEK i nästa avsnitt. Som nämnt i uppsatsens inledande kapitel syftar det avsnittet till att se den svenska rätten utifrån ett annat unionslands synsätt. Avsnittet ägnas alltså åt at beskriva den tyska telekommunikationslagstiftningen och landets genomförande av datalagringsdirektivet.

6.2 Utblick på tysk datalagring för brottsbekämpande ändamål

Den orwellska "der gläserne Mensch", den genomskinliga människan, är i Tyskland en känd metafor för avsaknaden av dataskydd och syftar på en övervakande statsapparat.[289] Precis som Sverige genomförde landet datalagringsdirektivet genom ny inhemsk lagstiftning, och för deras del skedde det i december 2007. En rad paragrafer avseende teleoperatörernas lagringsskyldigheter tillkom genom 113 a-113 g §§, TKG. Ursprungligen infördes, likt den svenska dåvarande lagstiftningen, en lagring på 6 månader.[290] Däremot var reaktionerna mot lagstiftningen starka i Tyskland och samma dag som de nämnda paragraferna skulle träda i kraft anmälde en grupp medborgare som arbetade med datalagringsfrågor, *Arbeitskreis Vorratsdatenspeicherung*, lagstiftningen till författningsdomstolen och stöddes då av 30 000 tyskar.[291] Tre år senare förklarade denna att datalagringen i paragraferna 113 a och 113 b §§ TKG, gick emot grundlagens artikel 10 om rätten till brevhemlighet och telekommunikation.

[287] Naarttijärvi (2013) s. 470.
[288] Naarttijärvi (2013) s. 480.
[289] Stollreither (1986) s. 15–27. Se även Deutscher Bundestag, Drucksache 17/12290 s. 9 ff.
[290] HP Bull (2009) s. 91, Gutwirth (2011) s. 4–5. Tillgången regleras i kap. VIII och IX i Straffprozeßordnung, StPo (straffprocesslagen) och i 113 c § TKG.
[291] Gutwirth, (2011) s. 5.

Integritetsskyddet var alltså inte tillräckligt beaktat.[292] Domen rönte stor uppmärksamhet och innebar således att författningsdomstolen underkände datalagringsdirektivets införlivande i den tyska rätten, och detta alltså innan EU-domstolen hade avgjort Digital Rights-domen. Följden blev att datalagringen upphörde och år 2012 väckte Kommissionen en fördragsbrottstalan mot Tyskland, som för övrigt kom att bli det sista unionslandet att inte omsätta datalagringsdirektivet.[293]

Här uppträder en skillnad mellan Sverige och Tyskland eftersom datalagringsdirektivet fortsatte att utgöra gällande rätt i Sverige fram till Digital Rights-domen. Søren Koch menar att trots att den tyska nationella rätten har förlorat inflytande gentemot EU-rätten har det inte i någon större utsträckning förändrat landets rättskultur. Tyskland är en av EU:s främsta förespråkare och många harmoniseringsförslag har tyskt ursprung, men detta har ändå inte ändrat tyska praktikers generella skepticism mot EU-rätten.[294] Den svenska grundlagstolkningen å andra sidan ”har omgivits av anmärkningsvärd *tystnad* i den svenska akademiska diskussionen*”* hävdar Mattias Derlén med flera. De menar att detta hänger ihop med grundlagens undanskymda roll i rättslivet liksom domstolarnas position i allmänhet. Under efterkrigstiden sattes arbetet med mänskliga rättigheterna och domstolar som dessas garanter i centrum runt om i Europa, dock ej Sverige. Författarna säger att detta i stor utsträckning betraktades ”som ett hinder för det socialdemokratiska välfärdsbygget” och citerar därefter dåvarande stadsminister Olof Palme: ”Det är inte så att säga ett Ämbetsmanna-och Domstols-Sverige vi vill ha. Det var mot detta som folkrörelserna -både arbetarrörelsen och bonderörelsen- en gång reste sig.”[295] Samtidigt kan tilläggas att vissa kritiker anser att den tyska författningsdomstolen har fått ett alltför stort inflytande och i förlängningen har Tyskland blivit en domarbunden, snarare än lagbunden stat. Thomas Bull slår dock tillbaka mot det argumentet och menar att det ”närmast är oseriöst” att hävda att landet inte styrs av regeringen och parlamentet.[296]

Oavsett hur det förhåller sig är författningsdomstolen allt som oftast en komponent som berörs i tysk doktrin när det gäller dataskydd.[297] Gällande fördragsbrottstalan mot Tyskland var denna i alla fall ”ur världen” i och med Digital Rights-domen. Däremot gjorde bristen på uppgifter det tungrott för de tyska brottsbekämpande myndigheterna och regeringen framhöll kort och gott att ”datalagring var nödvändig” och beslutade därför att en ny, dock betydligt mindre omfattande datalagringsreglering, skulle träda i kraft. Den 18 december 2015 infördes denna nya datalagringsreglering och återigen blossade en intensiv debatt upp. I och med Tele2-domen i december 2016 ställdes regleringen i ny dager.[298] Nedan följer en mycket kortfattad

[292] Dom: BVerfG, 1 BvR 256/08 2010-03-02 jfr NJW 2010, 833. Art. 10 beskrevs ovan i kap. 3. Om proportionalitetsbedömning i författningsdomstolen, se Petersen (2017) s. 2–3.
[293] Roßnagel (2017) NJW 2017, 696 s. 696.
[294] Koch m. fl. (2017) s. 173, 198–199.
[295] Derlén m.fl. (2016) s. 499.
[296] Bull (2015) s. 141 jfr Koch m. fl. (2017) s. 182.
[297] Stollreither (1986) s. 15–27, Knott (1986) s. 45–63.
[298] Roßnagel (2017) NJW 2017, 696 s. 697 ff.

beskrivning av den rätt som började gälla 2017. Bilden av vad som utgör gällande rätt kompliceras av att en av landets regionala domstolar, Oberverwaltungsgericht für das Land Nordrhein-Westfalen (OVG NRW), fattade ett interimistiskt beslut den 22 juni 2017 om att lagringsreglerna för uppgifter om internetåtkomst inte behöver följas då dessa ej är förenliga med EU-rätten.[299] Utifrån lagtexten framgår i alla fall operatörernas lagringsskyldighet av 113 a § TKG och lagringstiderna regleras i 113 b § TKG. Dessa kan alltså sägas motsvara svenska LEK 6 kap. 16 a och 16 d §§. Enligt 113 b § stycke 1 punkt 1 TKG ska trafik-och abonnemangsuppgifter lagras i tio veckor och lokaliseringsuppgifter ska enligt punkten 2 lagras under en månads tid. Som framgår är lagringstiderna i den tyska lagen kortare jämfört med de svenska, gällande lokaliseringsuppgifter stiftar svensk lag alltså 2 månader och tysk 1 månad. I TKG gäller 2,5 månader för trafik-och abonnemangsuppgifter vilket i LEK motsvaras av lagringstider på 6 månader som huvudregel respektive 10 månader för just internetåtkomst.

Vidare framgår av 113 b § andra stycke punkt 1–3 TKG, att gällande allmänna kommunikationstjänster ska uppgifter lagras om uppringande nummer, det nummer som blir uppringt och nummer som samtalet har styrts till. Därutöver datum och tid när kommunikationen påbörjades och avslutades samt information om tjänsten som har används, om det är så att olika tjänster kan användas som en del av telefonitjänsten. Som framgår av den svenska lagen lagras inte längre fast telefoni. Gällande mobiltelefoni framgår av 113 b § andra stycke punkt 4 a-c TKG, att uppgifter om internationellt prefix för numren ska lagras och om det rör sig om kontantkortstjänster ska datum och tid för den första aktiveringen sparas. Motsvarande bestämmelse om kontantkort framgår av 16 a § LEK. För tysk internettelefoni stadgas under av 113 b § andra stycke punkt 5 TKG att IP-adresser och användar-id för den uppringande och den som mottager samtalet ska lagras. Detta gäller även för obesvarade samtal. Motsvarande uppgifter ska lagras när det rör SMS-och MMS-trafik och andra dylika meddelandetjänster. Lagras ska även tidsangivelser för när ett meddelande har skickats och tagits emot. I Sverige är alltså lagringen av mobiltelefonin beroende av om uppkoppling sker mot trådlöst lokalt nätverk eller mobil mast alternativt privat trådlöst nätverk, eftersom den senare typen inte ska lagras. I övrigt ter sig ländernas reglering lika. I den svenska lagen framgår att utrustningsidentitet ska lagras vilket inte framgår av den tyska lagen. Vad det innebär i myndigheternas praktiska arbete har jag inte kunnat ta reda på.

Till sist gällande den tyska lagringen framgår under avsnitt (3) i 113 b § TKG att för internettjänster ska uppgifter om användarens IP-adress och användar-id, identifikation för anslutningsterminal och även datum och tid för påbörjandet och avslutandet av internetanvändningen med den aktuella IP-adressen. Vidare framgår av 113 b § TKG att de lokaliseringsuppgifter som ska lagras endast avser mobiltelefoni samt internetanvändning.

[299] Beck-Online 2017-06-22, se källförteckning, jfr SOU 2017:75 s. 192.

Leverantörerna är skyldiga att lagra information om den mast som används av det nummer som ringer upp samt det uppringda numret i början av kommunikationen. För internetanvändning ska den mast som användes när internetåtkomsten påbörjades lagras. Utöver att lagringstiderna för de uppgifter som ger internetåtkomst, liksom att uppgifterna som identifierar utrustningen där kommunikationen slutligt avskiljs till abonnenten, lagras längre i Sverige än i Tyskland, verkar lagringen som sådan inte skilja sig åt.

Sammantaget kan inte sägas att den svenska och tyska lagringen skiljer sig nämnvärt åt mer än att Sverige generellt har längre lagringstider. Eventuellt är detta ett uttryck för en mer restriktiv tysk hållning när det gäller just frågan om hur länge myndigheterna ska kunna tillgå lagrade uppgifter, men det går inte att säkert säga. Däremot är det tydligt att motståndet mot den här formen av lagstiftning är starkare i Tyskland än i Sverige, liksom att den tyska författningsdomstolens agerande genom underkännandet av TKG i sin tidigare form faktiskt gjorde att gemene tysk respektive svensk under ett par års tid var föremål för olika omfångsrik datalagring.

Slutligen gällande tillgången till de just beskrivna uppgifterna framgår kraven av 113 c § TKG. De uppgifter som lagras av operatörerna av praktiska skäl, såsom exempelvis fakturauppgifter, kräver att brottsutredningen avser ”schwere Straftat”, alltså allvarliga brott såsom mord, narkotikabrott, rån, utpressning, bedrägeri liksom skattebrott. När det gäller de uppgifter som leverantörerna är skyldiga att lagra av brottsbekämpande ändamål, krävs det att utredningen avser särskilt allvarliga brott (Straftat von erheblicher Bedeutung) hit räknas bland annat mord, människohandel, allvarligare former av narkotika -och sexualbrott liksom barnpornografibrott och brott mot den tyska staten (”den Bestand des Bundes oder eines Landes”).[300] I Sverige görs också den här uppdelningen mellan de uppgifter som har lagrats av operatörerna av praktiska skäl och de som lagras till följd av brottsbekämpande ändamål. För att återknyta till avsnitt 2.3 ovan och de brottsbekämpande myndigheternas tillgång till uppgifter i Sverige är det tydligt att den låga tröskel för att få tillgång till abonnemangsuppgifter inte har någon motsvarighet i tysk rätt. Detta medför alltså en skillnad jämfört med tysk rätt eftersom tillgång till abonnemangsuppgifter för brottsbekämpande myndigheter i Sverige inte kräver brott av viss svårighetsgrad. Däremot gäller precis som enligt tysk rätt att tillgång till trafik-och lokaliseringsuppgifter vid brottsutredande verksamhet kräver allvarlig brottslighet och domstolsbeslut. Det återstår att se hur länge svensk och tysk lag kommer ha den utformning som har återgivits i redogörelsen. I oktober 2020 meddelades nämligen två domar från EU-domstolen som på nytt har aktualiserat frågan om medlemsländernas nationella lagstiftning i förhållande till EU-rätten vid datalagring för brottsbekämpande ändamål. Till sist i detta kapitel följer därför en sammanfattning av domarna liksom några tankar om vilka konsekvenser dessa kan tänkas få för de bägge länderna framöver.

[300] Lagkommentar till 113 a § Beck-Online, se länk i källförteckning jfr SOU 2017:75 s. 190–191.

6.3 Gällande rätt utifrån nytillkomna försvarspolitiska ställningstaganden av EU-domstolen

Detta avslutande avsnitt i kapitlet ska ägnas åt att analysera två avgöranden från EU-domstolen som kan ses som en uppföljning på Tele2-domen. Den svenska regeringen konstaterade efter Tele2-domen att EU-rätten satte upp ramarna för den nationella lagstiftningen om datalagring för brottsbekämpande ändamål.[301] Samtidigt står det klart att det inte är helt tydligt hur man ska tolka EU-domstolens syn på förhållandet mellan artikel 1.3, som alltså anger att verksamhet som avser allmän säkerhet, försvar och statens säkerhet inte omfattas av direktivets tillämpningsområde, och 15.1 i E-Privacy-direktivet. Som beskrivet i kapitel 4, och som framgår av redogörelsen av Tele2-domen i kapitel 5, ska inte E-Privacy-direktivet tillämpas på de frågor som inte omfattas av gemenskapsrätten. Regeringens syn speglas av den utredning som tillsattes i kölvattnet av Tele2-domen där det uttrycktes att EU-domstolen genom domen ansåg sig ha kompetens att besluta om lagring, inte bara för brottsbekämpande ändamål, utan även för nationell säkerhet och försvar och slutsatsen som drogs var att ”…oavsett för vilket ändamål uppgifterna används så är operatörernas lagring och myndigheternas tillgång till dessa uppgifter underkastade den reglering som följer av EU-rätten.” Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt ifrågasattes bedömningen. [302]

Gränsdragningen mellan dessa delar av den brottsbekämpande verksamheten har vuxit i betydelse i takt med att brottsligheten överskrider nationsgränser. Då artikel 4.2 FEU säger att nationell säkerhet är en nationell angelägenhet har datalagring på detta område också ansetts vara utesluten från de EU-rättsliga kraven på lagringen. Anna Jonsson Cornell uttryckte redan 2015 att den EU-rättsliga lagstiftaren därför står inför flera utmaningar:”One is the difficulty with which issues of national security can be separated from criminal law aspects in times of asymmetric security threats, including terrorism, and the difficulty to obtain a clear line between internal and external security.”[303] För att återknyta till avsnittet om nationell säkerhet i kapitel 2, kan sägas att begreppets ”luddighet” inte bara ger upphov till frågor om datalagringens materiella sida, utan även aktualiserar frågan om vem som har rätt att besluta om gränserna för datalagringen för nationella säkerhetsändamål?

Frågan var i centrum i domarna Privacy International m.fl. (C-623/17) och La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, som båda meddelades den 6 oktober 2020. Med domarna har EU-domstolen förtydligat hur datalagring för underrättelseorganens arbete med nationell säkerhet ska betraktas utifrån E-Privacy-direktivet och dess artikel 15.1. Att

[301] Prop. 2018/19:86 s. 19.
[302] Citat SOU 2017:75 s. 22–23. Kritik se prop. 2018/19:86 s. 19 jfr ovan art. 4 & 5 FEU.
[303] Jonsson Cornell (2015b) s. 180.

dessa domar låg i EU-domstolens ”pipeline” medförde att den svenska regeringen avvaktade med att införa en särskild reglering för datalagring för brottsbekämpning kopplad till nationell säkerhet. Regeringen uttryckte att området för nationell säkerhet och huruvida EU-rätten var tillämplig även på dessa frågor inte hade klargjorts av EU-domstolen. I gällande nationell rätt görs därför ingen åtskillnad mellan datalagring för brottsbekämpande ändamål och datalagring på området för nationell säkerhet.[304]

I det första målet, Privacy International,[305] prövades om ett krav på teleoperatörerna om att lämna ut uppgifter till en medlemsstats säkerhets- och underrättelsemyndighet omfattas av EU-rätten. Då denna utlämning föregås av lagring gör EU-domstolen flera uttalanden om synen på lagringsmomentet i artikel 15.1 i förhållande till nationell säkerhet. Det andra målet, La Quadrature du Net m.fl.[306] omfattade flera frågor, däribland EU-rättens integritetskrav på nationell lagstiftning som anger att teleoperatörer är skyldiga att lagra och tillhandahålla myndigheter uppgifter om elektronisk kommunikation, när syftet med lagstiftningen bland annat är att skydda nationell säkerhet. Båda målen berör således förhållandet mellan EU-rätten och medlemsstaterna när det gäller datalagring vid hot mot nationell säkerhet, om än ur olika infallsvinklar. Den svenska regeringen, tillsammans med andra länder, yttrade, sig i båda dessa mål och menade att ”åtgärder till skydd för nationell säkerhet faller utanför EU-rättens tillämpningsområde i enlighet med artikel 4.2 i FEU” och att E-Privacy-direktivet därför inte kan tolkas så att nationella åtgärder åsyftande att skydda den nationella säkerheten omfattas av direktivets tillämpningsområde (Privacy International p. 32–33, La Quadrature du Net m.fl. p. 89–92). EU-domstolen å sin sida svarade med att en sådan tolkning skulle innebära att artikel 15.1 fråntogs ”sin ändamålsenliga verkan” liksom att detta skulle gå emot direktivets systematik. Förenklat sagt menade EU-domstolen att medlemsländerna inte kan använda nationell säkerhet som ett argument för att kringgå unionsrättens krav i E-Privacy-direktivet. (La Quadrature du Net m.fl. p. 95–97, 99). Istället omfattar direktivet nationell lagstiftning som ålägger teleoperatörer att lagra och därefter överföra trafik- och lokaliseringsuppgifter till landets säkerhets- och underrättelsetjänst för att skydda nationell säkerhet (Privacy International p. 49, La Quadrature du Net m.fl. p. 104). EU-domstolen konstaterade i de båda domarna att målet att skydda nationell säkerhet, med beaktande av artikel 4.2 FEU, ”till sin art och på grund av sitt särskilda allvar” skiljer sig från de övriga mål som artikel 15.1 i E-Privacy-direktivet stadgar såsom att bekämpa brottslighet i allmänhet. Då hot mot nationell säkerhet är graverande skulle målet att skydda denna kunna motivera ett mer långtgående ingrepp i de grundläggande rättigheterna i jämförelse med de övriga mål som artikel 15. 1 innehåller. Detta dock under förutsättning att proportionalitetsprincipen iakttas (Privacy International p. 75 och La Quadrature du Net m.fl. p 136).

[304] Prop. 2018/19:86 s. 19, 21.
[305] C-623/17, Privacy International, EU:C:2020:790.
[306] C-511/18, C-512/18, C-520/18 La Quadrature du Net m.fl., EU:C:2020:791.

Vid sidan om detta förtydligade EU-domstolen i La Quadrature du Net m.fl. vilka lagstiftningsåtgärder, som i förebyggande syfte stadgar lagring av trafik- och lokaliseringsuppgifter till skydd av nationell säkerhet, som kan accepteras utifrån artikel 15.1 i direktivet. Lagring av trafik- och lokaliseringsuppgifter för polisiära ändamål utgör i sig ett ingrepp i de grundläggande rättigheter om respekt för privatlivet och skydd av personuppgifter, i artikel 7 respektive artikel 8 i EU-stadgan, och detta ”oberoende av om de uppgifter som avser privatlivet är av känslig art eller ej eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet.” (p. 115, 118). Även om de lagrade uppgifterna inte används är det en kränkning per se (p. 116). Med hänsyn till att trafik-och lokaliseringsuppgifter kan användas för att kartlägga en individs liv är uppgifterna lika känsliga som själva innehållet i kommunikationerna (p. 117). Artikel 15.1 tolkad mot bakgrund av artiklarna 7, 8, 11 och 52.1 i EU-stadgan, hindrar inte en lagstiftning som ger behöriga myndigheter rätt att ålägga teleoperatörer att lagra trafik-och lokaliseringsuppgifter för alla användare under en begränsad och förutsebar tidsperiod. Precis som i Tele2-domen ska denna tidsmässiga begränsning vara anpassad efter vad som kan anses som strängt nödvändigt. Dock krävs det att det ska föreligga ”tillräckligt konkreta omständigheter för att anse att den berörda medlemsstaten står inför ett sådant allvarligt hot mot nationell säkerhet” (p. 137–138). Lagringen måste vara begränsad, skydda personuppgifterna mot eventuellt missbruk och inte ske på en systematisk basis med tanke på de allvarliga ingrepp i användarnas grundläggande rättigheter utifrån EU-stadgans artikel 7 och 8 en sådan lagring medför (p. 139). Inte ens målet att tillförsäkra en effektiv brottsbekämpning kan således berättiga en ”lagstiftning om lagring av praktiskt taget hela befolkningens trafik- och lokaliseringsuppgifter” utan att det finns ett direkt eller indirekt samband mellan personer som berörs av lagringen och det eftersträvade brottsbekämpande målet (p. 145).

Till skillnad från i Tele2-domen, uttalade sig domstolen om integritetsintrånget vid lagring av IP-adresser och menade, med tanke på det allvarliga ingrepp som detta medför, att sådan lagring endast kan motiveras av bekämpande av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet (p. 153–154, 156). Domstolen gjorde även en bedömning av lagring av uppgifter om användarnas fysiska identitet vid den elektroniska kommunikationen. Detta ger inte någon information om kommunikationsdeltagarnas privatliv och det ingrepp som lagring av fysisk identitet medför är inte att betrakta som allvarligt (p. 157).[307] Med tanke på den avvägningsaspekt som artikel 15.1 bygger på ansågs därför en lagring av samtliga användares fysiska identitet som påkallad och godtagbar i brottsbekämpande syfte (p. 159).

Slutligen avseende lagringen av trafik- och lokaliseringsuppgifter framgår av domslutet att artikel 15.1, tillåter lagring av dess uppgifter, på ”ett generellt och odifferentierat vis” då staten ”står inför ett allvarligt hot mot

[307] jfr C-207/16, Ministerio Fiscal, EU:C:2018:788, p 59–60.

nationell säkerhet beträffande vilket det är visat att hotet är verkligt och aktuellt eller förutsebart”. Detta innebär alltså att EU-stadgans artiklar 7, 8, 11 och 52.1 tillåter att teleoperatörer åläggs av myndigheterna att lagra trafik- och lokaliseringsuppgifter om de övriga krav som EU-domstolen ställer upp följs. Ett sådant krav är att oberoende myndighet eller domstol ska kontrollera åläggandet och tidsperioden ska vara begränsad till ”vad som är strängt nödvändigt” med möjlighet till förlängning vid fortsatt hotbild. Därtill medger artikel 15.1 att den nationella lagstiftningen, till skydd av allmän och nationell säkerhet liksom för bekämpning av grov brottslighet, föreskriver en riktad lagring av trafik- och lokaliseringsuppgifter under förutsättning att objektiva, icke-diskriminerande kriterier avgränsar en viss personkrets alternativt ett geografiskt kriterium. Motsvarande krav ställde domstolen upp för en generell och odifferentierad lagring av IP-adresser. Bägge dessa typer av ålägganden fordrar en tidsbegränsning ”till vad som är strängt nödvändigt” men för trafik-och lokaliseringsuppgifterna skulle det vara möjligt att förlänga tidsfristen. Tidsangivelser förekommer alltså inte i domslutet. Till sist är ett krav att berörda personer ska garanteras ”effektiva garantier mot riskerna för missbruk.” (p. 168).[308]

6.3.1 Avgörandenas påverkan på nationell rätt

”Die Geschichte der Vorratsdatenspeicherung ist geradezu chaotisch “, alltså fritt översatt, menar författaren Stephan Beukelmann, att alla turer med datalagringen inte är annat än kaotiskt. Tyskland likt övriga EU kommer att behöva rätta sig efter de nya kraven som framgår av de refererade domarna. Datalagring för svårare brott, liksom en lagringstid för dessa brott på upp till sex månader måste därför återinföras i Tyskland. Beukelmann menar därför att lagringsskyldigheten i TKG inte gäller för närvarande.[309]

Nationell säkerhet må vara en diffus beteckning, men de båda senaste domarna visar tydligt att länderna själva vill styra över det som kan läsas in i begreppet. Den franska regeringen har meddelat att den motsätter sig EU-domstolens beslut eftersom denna har gett sig in i den nationella franska rätten. En tysk skribent menar att om den franska författningsdomstolen följer regeringens vilja är det som att öppna Pandoras ask, då andra medlemsstater kan komma att på liknande vis avfärda EU-domstolens slutsatser, även i andra frågor med motiveringen att det är en nationell angelägenhet.[310] Domarna lämnar alltså mycket att önska ur ett normhierarkiskt perspektiv. Detta då det inte framgår hur EU-domstolen har ansett sig ha mandat att sätta upp regler som avser hur lagringen ska respektera den personliga integriteten för den enskilde vid hot mot nationell säkerhet, när direktivets artikel 1.3 uttryckligen anger att det området inte omfattas av dess tillämpningsområde. Att argumentera för att direktivet i annat fall förlorar sin ändamålsenliga verkan, förklarar dessvärre inte direktivets förhållande till artikel 4.2 i FEU. Det återstår att se hur LEK

[308] C-746/18, Prokuratuur, EU:C:2021:152 p.30–35.
[309] Beukelmann, (2020) NJW-Spezial 2020, 696 jfr Ogorek (2021), NJW 2021, 531 s. 547.
[310] Holland, Martin publicerad på Heise Online, 2021-03-04, se länk i källförteckning.

kommer att påverkas av EU-domstolens ställningstagande. Utifrån domslutet i La Quadrature du Net m.fl. verkar det som att lagstiftarens ”svängrum” vid utformande av den lagring som sker på grund av hot mot nationell säkerhet är något vidare än vad som gäller för övrig brottsbekämpande verksamhet. Bortsett från att stödet för EU-domstolens beslutanderätt i frågan är oklar har La Quadrature du Net m. fl. i alla fall förtydligat lagringens materiella krav.

Detta medför, för svensk del, att regeringens bedömning av abonnemangsuppgifter sätts i nytt ljus. Detta eftersom EU-domstolen ställer lika höga integritetskrav på dessa som för övriga trafikuppgifter. Regeringens hänvisning till att Tele2-domen inte uttalade sig specifikt om abonnemangsuppgifter och att det därmed gick att ha en förlängd lagringstid för dessa uppgifter i LEK är inte längre ett hållbart argument. Om det är så att Sverige ska ha längre lagringstider för dessa uppgifter ska en sådan motivering grunda sig i att dessa är strängt nödvändiga för brottsbekämpningen, vilket i sådant fall kan övertrumfa den personliga integriteten utifrån en objektiv behovsprövning. Att hänvisa till att EU-domstolen inte har klargjort vad som gäller med abonnemangsuppgifter duger nämligen inte efter La Quadrature du Net m.fl. Vid nästa översyn av lagen vore det utifrån, såväl legalitetsskäl som med tanke på förutsebarheten, önskvärt med en mer ingående motivering till abonnemangsuppgifternas särreglering i LEK.

6.3.2 En särskild svensk syn på datalagring?

Avslutningsvis i detta kapitel ska en konstitutionell aspekt av den svenska synen på datalagringen dryftas. Ester Herlin-Karnell skriver nämligen i sin artikel *Corona and the Absence of a Real Constitutional Debate in Sweden*, att det långvariga svenska EU-medlemskapet till trots lyser den svenska debatten om dataskydd och integritet i förhållande till rättsstatsaspekter med sin frånvaro. Landets domstolar har under åren av medlemskap varit skyldiga att övervaka och se till att Sverige lever upp till sina åtaganden och garantera individer sina rättigheter enligt EU-och europarätten men detta har inte avspeglat sig i synen på den här frågan. Hon menar att landet är i behov av en rejäl konstitutionell och demokratisk debatt. “For a country that prides itself of respecting EU values and encourages EU solidarity, this is remarkable as not all EU values and EU legal duties such as data protection are upheld.” Detta utgör en konstitutionell utmaning med hänsyn till EU:s dataskyddsreglering, artikel 16 FEUF liksom artikel 8 i EKMR menar Herlin-Karnell.[311]

Något som eventuellt styrker hennes tes är att det trots ett aktivt sökande har varit svårt att få tag i en svensk analys av de nya EU-domarna. Pernilla Norman och Wictor Wallenius har skrivit en kort analys för Juno och anför att ” EU-domstolen ger i sin dom vägledning i den svåra och delikata

[311] Herlin-Karnell 2020-04-10, publicerad på Verfassungsblog, se länk i källförteckning.

balansgången med upprätthållande av dataskydd och integritet för den enskilda å ena sidan, och medlemsländernas behov av information för att bekämpa terrorism och andra hot mot nationell säkerhet å andra sidan”.[312] Som författarna påpekar möjliggör den tekniska utvecklingen att terrorister får verka fritt i det fördolda. Samtidigt utgörs en hotbild mot det liberala samhället av en allmänt ökande övervakning, liksom de inneboende risker som föreligger när stora mängder data om privatpersoner kan komma i fel händer. Jag håller med om att det är en svår utmaning som den nationella lagstiftaren står inför när dessa parametrar ska viktas mot varandra. Klart är i alla fall att den svenska responsen på de två EU-domarna, i jämförelse med den kontinentaleuropeiska reaktionen, får ses som blygsam, långt ifrån franska protester, eller tyska benämningar av den EU-rättsliga datalagringsregleringen som ”kaotisk”.

[312] Norman & Wallenius, JUNO 2020-10-13, länk se källförteckning.

7 Avslutande synpunkter

7.1 En avvägning förenad med svårigheter

Från det ena hållet i den allmänna debatten efterfrågas ”hårdare tag” mot den eskalerande gängkriminalitet, från annat håll hörs orwellska metaforer om samhällsutvecklingen. Ur en praktisk tillämpningsaspekt är det av stor vikt att de brottsbekämpande myndigheterna är medvetna om hur de lagrade personuppgifterna får användas, likväl är det viktigt att även allmänheten är varse detta för att lagstiftningen inte ska skapa misstro mot den statliga övervakningen. Lagstiftarens avvägningar har därför betydelse för lagstiftningens förankring hos befolkningen. Detta i synnerhet i en tid när det förhåller sig på det vis som Thomas Bull påpekar där vi ser en tilltagande användning av modern teknik, och i dess kölvatten följer en ökad exponeringsvilja på internet, vilken parallellt åtföljs av en så kallad ”kränkthetskultur”, det vill säga situationer där påstådda integritetsövertramp har skett.

Efter att ha fördjupat mig i den datalagring som sker för brottsbekämpande ändamål har jag fått en större förståelse för vilken delikat avvägning som den nationella lagstiftaren har stått inför vid genomförandet av E-Privacy-direktivet, och därefter datalagringsdirektivet. Systematiken i såväl den EU-rättsliga, som den nationella rätten har bitvis varit mycket svårtillgänglig och tekniskt komplex. Ur både en legalitetsaspekt såväl som med tanke på förutsebarheten får sägas att det är mycket svårt att dels, få en överblick av de olika rättsakter som sinsemellan samverkar vid datalagring av brottsbekämpande ändamål, dels begripa hur avvägningen mellan den personliga integriteten och behovet av data för de brottsbekämpande myndigheterna görs på lagstiftningsnivå. Visserligen finns det många områden inom juridiken där det brister i förutsebarhet. Dock har, som framkommer av redogörelsen, den EU-rättsliga lagstiftaren själv uttryckt att nuvarande reglering är olycklig eftersom E-Privacy-direktivet hänvisar in i det upphävda dataskyddsdirektivet.

Syftet har utgått från de två kärnpunkterna personlig integritet och datalagring för brottsbekämpande ändamål. I detta avslutande kapitel diskuteras undersökningens resultat. Här anläggs därför en mer sammantagen och bred syn på ämnet jämfört med i uppsatsens utredande del. De inledande mer lagtekniskt orienterande frågeställningarna som rör innebörden av datalagring hos teleoperatörer liksom vilka integritetskrav som LEK ställer upp för operatörerna har behandlats ingående i kapitel 2 och 4. För dessa tekniska aspekter hänvisas därför till dessa kapitel. Nedan följer istället en diskussion utifrån den här specifika datalagringens påverkan på individ och samhälle liksom hur EU-rättens utveckling under de senaste åren har påverkat den nationella lagstiftningen.

Inledningsvis i denna del ska sägas att det europarättsliga integritetsskyddet, genom Europakonventionen, har stärkt regeringsformens rättighetsskydd genom att denna numera har en förankring i grundlagen. Avsaknad av ett tillräckligt skydd för den enskildes privatliv enligt artikel 8 kan leda till brott mot artikeln där staten står som ansvarig trots att integritetsintrånget är utfört av en enskild. Av utredningen framgår att en effektiv brottsbekämpning är en förutsättning för att artikel 8 ska kunna uppfyllas. En del brott skulle bli omöjliga att klara upp utan tillgång till lagrad elektronisk kommunikation. Som framgår preciseras artikeln av dataskyddskonventionen, vilken även har stått modell vid utarbetandet av det beskrivna EU-rättsliga regelverket avseende dataskydd. Att Europakonventionen har präglat EU-stadgan är tydligt. Som framgår av de återgivna domarna är artiklarna 6 och 7, som skyddar frihet och privatliv, möjliga att inskränka så länge proportionalitetsprincipen beaktas. Det låter tydligt och klart men rättsfallen illustrerar att det är desto svårare att åstadkomma en välavvägd datalagringslagstiftning, som inskränker nämnda friheter, i praktiken. Detta inte minst då synen på datalagring drastiskt har förändrats i EU under de senaste åren, vilket givetvis påverkar den nationella bedömningen av vad som kan anses utgöra acceptabla inskränkningar i integritetsskyddet. Även fördragen anger en rätt till personuppgiftsskydd och det sammantagna skyddet är därför grundmurat. En sista reflektion på detta som kan göras är att det idag, till skillnad från under perioden då datalagringsdirektivet utgjorde gällande rätt, inte är möjligt för de nationella lagstiftarna att kringgå personuppgiftsskyddet med hänvisning till att det krävs för brottsbekämpande ändamål.

I anslutning till dessa synpunkter ska här utvecklingen av EU-rättens datalagringslagstiftning kommenteras. Av den gjorda jämförelsen mellan dataskyddsdirektivet och GDPR framgår att rättsakternas grundläggande principer är lika och det handlar i grund och botten om att personuppgifter ska kunna utbytas säkert inom unionen. Som redan diskuterats är deras förhållande till E-Privacy-direktivet oklart utformat. Klart är i alla fall att EU-stadgans artikel 7 och 8 konkretiseras av E-Privacy-direktivet när det gäller personuppgiftsbehandling vid elektronisk kommunikation. Som användare ska man därför kunna förvänta sig att förbli anonym vid sådan kommunikation såvida inte samtycke har givits till annat. Den artikel som uppsatsen har tagit avstamp i, artikel 15.1 i E-Privacy-direktivet, har inte i sak påverkats av GDPR. En annan sak är att det idag är svårare att navigera mellan de olika regelverken. Som har förklarats möjliggör nämnda artikel en nationell lagstiftning som tillåter datalagring hos operatörerna dels av praktiska skäl, dels för brottsbekämpande ändamål. I och med datalagringsdirektivets intåg kan sägas att dessa undantag som stadgas i artikeln blev en huvudregel då alla uppgifter som förekom hos operatörerna skulle lagras för brottsbekämpande ändamål. Med tanke på det starka skydd som den personliga integriteten åtnjuter både i EU- stadgan och EKMR får det snarast ses som förvånande att datalagringsdirektivet kunde ”klubbas igenom”. I viss mån tycker jag därför att bedömningarna som har legat bakom den EU-rättsliga datalagringen bitvis har omgärdats av godtyckliga

bedömningar. Detta med tanke på den diametrala svängning som skedde mellan införandet av datalagringsdirektivet och Tele2-domen.

7.2 Individ och samhälle i den elektroniska miljön

Innebörden av uttrycket personlig integritet är svårt att greppa, vilket får följden att skyddet av denna givetvis inte är skriven i sten. Ambitionen i undersökningen har som framgår av syftet inte varit att uttömmande redogöra för begreppets innebörd, utan snarare ge en bild av dess komplexitet liksom hur gällande rätt ser ut. Utifrån dels Integritetsskyddskommitténs utredningar, dels litteraturen framträder en bild av att integritetsskyddet i svensk rätt är förhållandevis svagt. Med tanke på att grundlagarna förväntas genomsyra den vanliga lagstiftningen och sätta gränser för vilka inskränkningar lagstiftaren får göra i rättighetsskyddet, blir så att säga trycket på den senare hårdare än i till exempel det tyska systemet där grundlagsskyddet redan från start är starkare. Det är således LEK som ska upprätthålla den praktiska gränsen för statens insyn i individens privatliv på det här specifika området. Såtillvida fyller LEK en viktigare roll än den tyska TKG eftersom konstitutionen där redan borgar för ett mycket starkt individskydd. Inte minst uppträder den här skillnaden länderna emellan utifrån den tyska författningsdomstolens underkännande av datalagringsdirektivet utifrån att detta gick emot den tyska grundlagens artikel 10 om rätten till privat telekommunikation. Utifrån jämförelsen mellan de bägge länderna i kapitel 3 kan sammanfattningsvis sägas att Tyskland har ett osedvanligt starkt integritetsskydd, medan det svenska integritetsskyddet i regeringsformen främst är en avvägningsaspekt som i enlighet med kraven i grundlagen får inskränkas i vanlig lag. Ytterligare en förstärkning för den enskildes integritetsskydd i Tyskland tillkommer genom möjligheten att vända sig till författningsdomstolen, liksom doktrinen om det som kallas för informationssjälvbestämmande. Även med beaktande av uppsatsens diskussion om regeringsformens målsättningsstadgande i 1 kap. 2 §, där olika synsätt framträder, sällar jag mig till Hillers analys av svensk och tysk rätt i detta avseende och anser därför att skyddet för den personliga integriteten såväl i materiellt som i processuellt hänseende är starkare i Tyskland. Dock menar jag att detta inte avspeglar sig märkbart i ländernas nationella datalagringslagstiftning. I det jämförande avsnittet (6.2) om de båda ländernas datalagring av brottsbekämpande ändamål stod det nämligen klart att lagringen i den tyska 113 a § TKG och 6 kap. 16 a § LEK huvudsakligen är likartad, även om ländernas lagringstider i 113 b § TKG och 6 kap. 16 d § LEK skiljer sig åt. Varför det förhåller sig så har inte undersökningen kunnat ge ett svar på.

Däremot är det tydligt att synen på den personliga integriteten skiljer sig åt mellan Sverige och Tyskland. Jag tror att detta har ett samband med det Søren Koch har påpekat om att tysk rättskultur i vissa avseenden uppvisar en generell skepsis mot EU-rätten. Författningsdomstolen spelar en viktig

roll som väktare för den personliga integriteten, och som framkommer är den allt som oftast en komponent som berörs i tysk doktrin om dataskydd. Motsvarande referenspunkter likt den tyska författningsdomstolen har jag inte funnit i den svenska rättsdebatten på området. Jag tror att ländernas olika historia under främst 1900-talet spelar en viktig roll här. Utformningen av det tyska polisväsendet är ett direkt svar på de övergrepp som begicks av Gestapo och Stasi. Likaså är utformningen av ländernas respektive integritetsskydd präglad av deras olika politiska bakgrunder. Weimarförfattningens brister har starkt präglat den nuvarande tyska grundlagen. Sverige å andra sidan har dominerats av ett mycket starkt statsbärande parti som, likt Derlén påpekat ovan, snarast har sett domstolarnas makt som ett hot mot den verkställande och lagstiftande makten.

Utifrån undersökningen kan sägas att E-Privacy-direktivet har stärkt det svenska integritetsskyddet, detta på grund av direktivets starka koppling till EU-stadgans skydd vilket visade sig ha effekt på det svenska integritetsskyddet i LEK. Om detta vittnar Tele2-domen. Hade Tele2 haft sitt säte i Tyskland under 2016 hade bolaget aldrig behövt driva en process likt den i Sverige eftersom Tyskland vid tiden inte tillät tillämpning av datalagringsdirektivet. Indirekt påverkade detta abonnenterna. I Sverige har intresset för dessa domar varit svagare än i Tyskland utifrån vad som framkommit i de båda ländernas rättspolitiska debatt och likaså gäller för de domar som meddelades av EU-domstolen i slutet av 2020. Visserligen är det, som Sterzel påpekar, storleksmässigt två vitt skilda länder, men inte ens med det förbehållet går det att komma undan att svenskar generellt verkar ha mindre synpunkter på detta med dataskydd. Däremot skulle det även gå att vända på perspektiven och säga att med tanke på gradskillnaden i ländernas konstitutionella skydd för den personliga integriteten är ländernas olika lagringstider för uppgifterna i TKG och LEK försvinnande små.

I ett bredare samhällsperspektiv står det klart att ett starkt integritetsskydd gagnar demokratin, detta eftersom en grundtrygghet gynnar individers engagemang i samhället. I en tid när tekniken blir alltmer utvecklad gäller det att slå vakt om det Burke och Tocqueville benämnde som ”majoritetens tyranni.” En förutsättning för det upplysta och demokratiska samhället är att inga röster tystas av rädsla för repressalier. Utifrån detta måste de skäl som väger över vid brottsbekämpande arbete, och därmed behov av datalagring, vägas över inte bara av individens eget behov av personlig integritet, utan även det öppna samhällets behov av en fri kommunikation, även en elektronisk sådan. Som Solove och Naarttijärvi båda påpekar spiller därför ett starkt individskydd över på samhället. Att lämna ut personlig information upplevde mer än hälften av de tillfrågade svenskarna i den av Integritetsskyddskommittén redovisade undersökningen, som en inte oproblematisk fråga. Den enskilde bör alltså kunna förvänta sig att lagstiftaren kan presentera legitima skäl till varje inskränkning i den personliga integriteten vid utarbetandet av datalagringslagstiftning. Om inte kan den misstro som Integritetsskyddskommittén ovan flaggade för bli ett faktum vilket i sig skadar såväl individ som samhälle. Paradoxalt nog har

uppsatsen visat att i tider av ökat politiskt våld och tryck på samhällsapparaten kan den folkliga opinionen samtidigt vara stark för den typ av långgående lagstiftning som datalagringsdirektivet utgjorde. Att skyddet för den personliga integriteten i sådan lagstiftning är undermåligt övertrumfas då av argument om ”hårdare lagstiftning” och ökad statlig kontroll. I linje med ”jag-har-inget-att-dölja”-synen var även majoriteten av svenskarna välvilligt inställda till att lagstiftarens tumskruvar drogs åt för att möjliggöra ett effektivt arbete mot den grova brottsligheten enligt Integritetsskyddskommitténs attitydundersökning. Likt nämnda kommitté menar jag att en ogrundad proportionalitetsbedömning vid utarbetandet av en för den enskilde ingripande lagstiftning är oacceptabelt i en rättsstat. Utifrån avsnittet 6.1.5 ovan som behandlade den svenska lagstiftarens viktning mellan brottsbekämpningens datalagringsbehov och den personliga integriteten har jag dragit ett par slutsatser som ska presenteras i det följande.

Sett i ett historiskt perspektiv är internet och platsen som det tar i människors vardagsliv något nytt. I den allmänna samhällsdebatten hörs ibland röster som vittnar om en tid innan det utvecklade IT-samhället, dessa synpunkter kommer ofta hand i hand med ett obehag inför teknikutvecklingen och dess inneboende övervakningsmekanismer. Ser man det så vill man givetvis inte ha någon datalagring överhuvudtaget. Samtidigt har jag under arbetets gång insett att den frihet som de flesta individer törstar efter vid internetuppkoppling eller då de ringer i sin telefon, betalas med någon annans frihet. Med detta menar jag att skulle ingen datalagring överhuvudtaget ske skulle färre brott kunna klaras upp. Fallet K.U. mot Finland är ett bra exempel på att brottsbekämpningen i vissa fall får ge vika för rätten till en fredad kommunikation på internet utifrån EKMR artikel 8. Arbetet med uppsatsen har gjort mig varse hur mycket information operatörerna har tillgång till om enskilda liksom vilket otroligt viktigt verktyg både trafik- och lokaliseringsuppgifter är för svenska brottsbekämpande myndigheter. Övervakningen av den elektroniska kommunikationen utgör på så vis ett sofistikerat hot mot den personliga integriteten. För den enskilde förstår jag att det kan uppfattas som mindre ingripande att staten inte lyssnar av eller kan se innehållet i meddelanden som sänds, samtidigt ska inte vidden av den kartläggning som är laglig att företa idag underskattas. Ett geografiskt rörelsemönster, vanor och umgänge kan skvallra mycket om en person. Å andra sidan visar undersökningen att internet är en förutsättning för att en del brott kan begås. För att bland annat kunna leva upp till Europarådets konvention om skydd för barn mot sexuell exploatering och sexuella övergrepp krävs det effektiva utredningsverktyg i den elektroniska miljön. Jag valde ut regeringens lakoniska yttrande om att internet är ”en etablerad plattform för våldsbejakande extremism och terrorismpropaganda” vilket vid första anblick kan låta väldigt svartsynt, men jag menar att en individ inte kan förvänta sig att man ska kunna röra sig i den elektroniska miljön utan övervakning. Frihet och säkerhet är nämligen väldigt nära förbundna. Premissen för att skörda de bra sidorna med internet får därför betalas med att man ger upp en del av sin frihet. Detta förtar dock inte att lagringen av kommunikationen per se är en mycket ingripande

åtgärd i en människas privatliv. Av denna anledning tycker jag att högre krav kan ställas på den bakomliggande motiveringen till vissa delar av lagringen. För närvarande är behandlingen av abonnemangsuppgifter i nationell rätt oklar, och på EU-nivå omgärdas lagringen som sker mot bakgrund av nationell säkerhet av frågetecken.

I fråga om den nationella avvägningen framgår det av kapitel 6 att det är ett växelspel mellan lagringens utformning och integritetsskyddet eftersom ett underskott av lokaliseringsuppgifter hos operatörerna kan leda till att detta måste kompenseras genom att myndigheterna istället behöver mer trafikuppgifter. Lokaliseringsuppgifterna utgör en väsentlig del av en misstänkt persons kommunikation med andra vilket gör att de ökar nyttan med övriga trafikuppgifter som lagras. Det är därför tydligt att de uppgifter med den största verksamhetsnyttan för de brottsbekämpande myndigheterna också är de som gör mest ingrepp i den personliga integriteten. Samtidigt är lagringen av dessa en mycket kostnadseffektiv insats som har visat sig ha hög ”verkningsgrad” inom det polisiära arbetet. Jag har redan uttryckt åsikten att datalagring är ett nödvändigt ont, men med detta sagt är det ändå bra att lagringstiden för just lokaliseringsuppgifterna har dragits ner i svensk rätt till två månader. Detta just med tanke på hur otroligt informationsrika dessa uppgifter är. Tidsramarna i LEK är inte en naturlag men med nuvarande regelverk blir det tydligare att de känsligaste uppgifterna har en kortare lagringstid än övriga uppgifter. Som beskrivet ovan gjordes ingen åtskillnad uppgifterna emellan under datalagringsdirektivets tid. Inte bara utifrån att denna systematik underkändes av EU-domstolen i Tele2-domen, utan även utifrån den enskildes förståelse för lagstiftarens avvägning, är det bra att LEK idag föreskriver en differentierad lagringstid.

När E-Privacy-direktivet genomfördes i Sverige var tongångarna i förarbetena annorlunda jämfört med hur det lät i propositionen när datalagringsdirektivet skulle genomföras. Synen på den rättsliga avvägning mellan personlig integritet och brottsbekämpningens informationsbehov har som sagt svängt under de senaste åren, såväl i nationell rätt som i EU-rätten. Vad som var nytt med datalagringsdirektivet var alltså att det infördes en lagring enkom för brottsbekämpande ändamål, vid sidan av gällande regelverk som alltså hade använts i de fall då de brottsbekämpande myndigheterna var i behov av dessa uppgifter. Som framgår av undersökningen är detta en direkt spegling av en förändrad syn på förhållandet mellan brottsbekämpning och integritet i EU. Att Sverige underkändes i EU-domstolen i Tele2-domen beror främst på utformningen av datalagringsdirektivet liksom de två (felaktiga) analyser som följde i kölvattnet av Digital-Rights-domen, och alltså inte på implementeringen som sådan. Lagstiftaren höll sig inom direktivets satta ramar. Under de dryga tio år som löpte mellan de två propositionerna förändrades inställningen till vad som skulle ses som acceptabla intrång i den personliga integriteten. Den lagstiftning som sågs som tillräcklig i förhållande till de brottsbekämpande myndigheternas arbete sågs alltså som otillräckliga då datalagringsdirektviet skulle genomföras. Som beskrivet är det den lagringsformen som de brottsbekämpande myndigheterna har haft att tillgå

innan det att datalagringsdirektivet trädde i kraft, liksom under perioden efter Tele2-domen innan dess att det nya regelverket från 2019 trädde i kraft. Genom datalagringsdirektivets genomförande i den svenska rätten har det utvecklats två parallella lagringsformer som nyttjas av de brottsbekämpande myndigheterna. Det som innan datalagringsdirektivet var den primära källan till information för de brottsbekämpande myndigheterna har nu blivit ett substitut. Som framgick av förarbetena till datalagringsdirektivets genomförande är dock gränserna mellan dessa två uppgiftsmängder inte särskilt tydliga. Detta hade varit helt i sin ordning om det inte, som i operatören Bahnhofs fall, visade sig att detta har blivit ett konkurrensmedel bolag emellan. Att locka kunder med att någon praktisk lagring inte sker går emot hela tanken med E-Privacy-direktivet och därmed även LEK då ett mål är att främja fri konkurrens på marknaden för elektronisk kommunikation. Framtiden får utvisa om detta kan tänkas bli en trend bland operatörer och om det medför någon negativ effekt för de brottsbekämpande myndigheterna. Frågan om snedvriden konkurrens får i sådant fall effekter inte bara nationellt utan kan även bli en konkurrensfaktor mellan olika bolag inom det EU-rättsliga området. En annan fråga som har väckts är hur man lagstiftningsvägen ska komma åt brottslighet om alltfler brott sker i den så kallade VPN-tunneln. Som framkommer ovan tangerade dåvarande Datainspektionen denna aspekt i sin fråga till regeringen, men detta vidareutvecklades aldrig. Även om det än så länge är hypotetiskt kan detta bli ett framtida problem ifall användandet av denna teknik ökar. Det återstår alltså att se hur väl 6 kap. 16 a och 16 d §§ kommer att fungera i praktiken.

Utöver det som redan har påpekats om hur operatörer kan utnyttja den praktiska lagringens möjlighet att kringgå de föreskrifter som gäller för den lagring som sker för brottsbekämpande ändamål, kan sägas att det i övrigt finns nackdelar med lagstiftarens strävan mot så kallad teknikneutralitet eftersom mindre operatörer inte har lika stora resurser vad gäller utformningen av diverse olika tekniklösningar som de större operatörerna har. Som framkommer av undersökningen är abonnemangsuppgifter inte en tydligt definierad kategori och lagringen av dessa kan därför inte heller sägas vara teknikneutral i och med att olika operatörer tillämpar olika lagringsmetoder när det gäller IP-adresser. Vad gäller de synpunkter som teleoperatörerna har inkommit med under remissförfarandet kan givetvis sägas att dessa är partsinlagor, trots detta har deras synpunkter bäring eftersom dessa bolag är de som faktiskt ska utföra lagringen och se till att säkerheten för uppgifterna upprätthålls. Jag ser dock inget bra alternativ till målet om en teknikneutral lagstiftning, åtminstone har inget annat förslag presenterats i undersökningens underlag.

Till sist några slutsatser kring uppsatsen vidare syfte som alltså har varit att reda ut vilken effekt EU-rättens normhierarkiska förhållande till nationell rätt får på den nationella lagstiftningen som föreskriver datalagring i brottsbekämpande syfte. Som har visat sig i redogörelsen rör sig den här lagstiftningen i ett område som är i gränslandet mellan EU-rätt och nationell rätt. Bernitz och Kjellgren påpekar ovan i avsnitt 3.6.2 att den EU-rättsliga

företrädesrätten är ett kontroversiellt område trots att denna alltså har kodifierats genom Lissabonfördraget. Likaså menar Bull och Reichel att gränsdragningen är komplex fråga. Effekten av detta visar sig i de två domar Privacy International m.fl. och La Quadrature du Net m.fl. som analyserades i kapitel 6. Den nationella säkerheten ska fortsättningsvis vara varje medlemsstats eget ansvar och E-Privacy-direktivet ska därför inte omfatta spörsmål som rör detta. Ytterligare en aspekt är att begreppet nationell säkerhet som det har visat sig i kapitel 2 är ett diffust begrepp som sådant. De båda domarna har redan analyserats ingående i kapitel 6 och här ska jag därför bara sammanfatta att jag tycker att styrkan i La Quadrature du Net m. fl. ligger i att lagringens materiella krav har förtydligats. Detta är positivt med tanke på att behandlingen av abonnemangsuppgifterna inte tidigare har ansetts fordra lika höga integritetskrav som övriga trafikuppgifter. En stor brist är dock det jag redan har påtalat i avsnitt 6.3.1. att det av de båda domarna inte framgår hur EU-domstolen har ansett sig ha befogenhet att besluta om lagringens utformnings just när det gäller nationell säkerhet. Av E-Privacy-direktivet framgår som sagt att detta område ska undantas och därmed vara något som den nationella lagstiftaren har på sitt eget bord. Sammanfattningsvis blir det då svårt att förstå hur artiklarna 1.3 och 15.1 ska förstås. Huvudargumentet från EU-domstolen för att få besluta om den lagring som sker av hänsyn till nationell säkerhet var som sagt att E-Privacy-direktivet i annat fall skulle förtas sitt syfte. Hur detta kan vara förenligt med FEU art 4.2 är svårt att begripa. Gällande den svenska lagstiftarens bedömning av abonnemangsuppgifter i ljuset av dessa domar hänvisar jag till analysen i kapitel 6. Här nöjer jag mig med att konstatera att om det inte finns en tydlig kategorisering av de olika lagringsslagen medför detta givetvis en rättsosäkerhet och i förlängningen en risk för att datalagringslagstiftningen blir föremål för vaga tolkningar. För att den datalagring som görs för brottsbekämpande ändamål fortsatt ska ha förtroende hos den enskilde är det av stor vikt att lagringens krav preciseras. Ett sådant exempel som jag redan har pekat på (i avsnitt 6.1.3) och som togs upp från remissinstanserna, är den inkonsekvens som gäller lagringstiderna för abonnemangs- respektive lokaliseringsuppgifter. Uppgifter om internetanslutning medges en lagring om sex månader, trots att dessa mer eller mindre motsvarar lokaliseringsuppgifter. De senare får dock enbart lagras i två månader då de anses vara så pass integritetskänsliga. Ska lagstiftningen bli begriplig och om det ska gå att följa lagstiftarens tankegång vid avvägningen mellan personlig integritet och datalagring för brottsbekämpande ändamål är den senare typen av frågetecken något som med fördel bör redas ut vid nästa översyn av lagen.

Avslutningsvis är det viktigt att komma ihåg att frihet vid elektronisk kommunikation, och därmed avsaknad av datalagring, till syvende och sist går ut över någon annans frihet att deltaga i samhället. Brottsuppklarning är en av grundbultarna i samhällskontraktet och ska man tro Hobbes är alternativet till detta än sämre för den enskildes frihet. Med detta sagt är det dock viktigt att förtroendet för att den lagring som sker görs utifrån en välgrundad avvägning. För säkerheten och för friheten.

Käll- och litteraturförteckning

Tryckta källor

Offentligt tryck

Utredningsbetänkanden

SOU 1941:20 Betänkande med förslag till ändrad lydelse av § 16 regeringsformen

SOU 2005:38 Tillgång till elektronisk kommunikation i brottsutredningar m.m.

SOU 2007:22 Skyddet för den personliga integriteten - kartläggning och analys

SOU 2007:76 Lagring av trafikuppgifter för brottsbekämpning

SOU 2008:3 Skyddet för den personliga integriteten - Bedömningar och förslag

SOU 2008:125 En reformerad grundlag

SOU 2010:103 Särskilda spaningsmetoder

SOU 2012:44 Hemliga tvångsmedel mot allvarliga brott

Ds 2014:23 Datalagring, EU-rätten och svensk rätt

SOU 2015:31 Datalagring och integritet

SOU 2016:41 Hur står det till med den personliga integriteten? – En kartläggning av Integritetskommittén

Ds 2017:26 En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar

SOU 2017:52 Så stärker vi den personliga integriteten

SOU 2017:75 Datalagring – brottsbekämpning och integritet

SOU 2018:65 Informationsutbyte vid samverkan mot terrorism

Propositioner och regeringsskrivelser

Prop. 1973:90 med förslag till ny regeringsform och ny riksdagsordning m. m.

Prop. 1975/76:209 om ändring i regeringsformen

Prop. 1987/88:57 om grundlagsfäst integritetsskydd

Prop.1992/93:200 om en telelag och en förändrad verksamhetsform för Televerket, m.m.

Prop.1993/94:117 Inkorporering av Europakonventionen och andra fri- och rättighetsfrågor

Prop. 2002/03:110 Lag om elektronisk kommunikation, m.m.

Prop. 2005/06:64 Genetisk integritet m.m.

Prop 2009/10:80 En reformerad grundlag

Prop. 2010/11:46 Lagring av trafikuppgifter för brottsbekämpande ändamål - genomförande av direktiv 2006/24/EG

Prop. 2011/12:55 De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation

Skr. 2017/18:69 Redovisning av användningen av hemliga tvångsmedel under 2016

Prop. 2017/18:105 Ny dataskyddslag

Prop. 2017/18:269 Brottsdatalag – kompletterande lagstiftning

Prop. 2018/19:86 Datalagring vid brottsbekämpning – anpassningar till EU-rätten

Prop. 2019/20:15 Skydd av Sveriges säkerhet vid radioanvändning

Prop. 2019/20:64 Hemlig dataavläsning

Utskottsbetänkanden

Bet. JU 2010/11: JuU14 Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG

Bet. JU 2011/12: JuU28 Lagring av trafikuppgifter för brottsbekämpande ändamål

Riksdagsskrivelser

Rskr. 2011/12:165
Rskr. 2011/12:166

Litteratur

Battis, Ulrich och Gusy, Christoph, (1999), *Einführung in das Staatsrecht.* 4 uppl. C.F. Müller Verlag, Hüthig GmbH.

Beckman, Ludvig (2004) *Demokrati och genetisk integritet.* SvJT 2004 s. 487–503.

Bengtsson, Bertil (2011), *SOU som rättskälla.* SvJT s. 777–785.

Bergström, Maria, (2012), *Vilka krav ställs när EU-rätten ska genomföras i Sverige?,* i Bull, Thomas och Halje, Lovisa och Bergström, Maria och Reichel, Jane och Nergelius, Joakim, *Arvet från Oxenstierna – reflektioner kring den svenska förvaltningsmodellen och EU.* Sieps Svenska institutet för europeiska studier s. 39–57.

Bernitz, Ulf, (2010), '*Europarätten* ', i Bernitz, Ulf och Heuman, Lars och Leijonhufvud, Madeleine och Seipel, Peter och Warnling-Nerep, Wiweka och Vogel, Hans-Heinrich (2010) *Finna rätt.* 11 uppl. Norstedts Juridik AB s. 59–89.

Bernitz, Ulf och Kjellgren, Anders, (2018), *Europarättens grunder.* 6 uppl. Norstedts Juridik AB.

Bernitz, Ulf och Kjellgren, Anders, (2021), *Introduktion till EU.* 7 uppl. Norstedts Juridik AB.

Beukelmann, Stephan *Neues von der Vorratsdatenspeicherung,* Neue Juristische Wochenschrift, NJW-Spezial 2020, 696.

Bogdan, Michael, (2003), *Komparativ rättskunskap.*2 uppl. Norstedts Juridik AB.

Bremdal, Patrik (2014), *'Är RF 1 kap. 2 § bara tomma ord? - Några tankar om målsättningsstadgandet i RF',* i Åhman, Karin, *Regeringsformen 40 år 1974–2014.* Uppl. 1. Iustus Förlag AB s. 57–68.

Bull, Hans Peter, (2009), *Informationelle Selbstbestimmung- Vision oder Illusion?* Mohr Siebeck.

Bull, Thomas och Lind, Anna-Sara, (2008), *'Europeiska unionens stadga om grundläggande rättigheter',* i SOU 2008:43 Tre rapporter till grundlagsutredningen s. 7–57.

Bull, Thomas, (2013a), *Fundamentala fragment – ett konstitutionellt lapptäcke*. Iustus Förlag AB.

Bull, Thomas, (2013 b), *'Regeringsformens renässans'* i Bull, Thomas och Lundin, Olle och Rynning, Elisabeth, *Allmänt och enskilt – offentlig rätt i omvandling: festskrift till Lena Marcusson.* Iustus Förlag AB s. 67–81.

Bull, Thomas (2015), *'Tyskland'*, i Jonsson Cornell, Anna (red.), *Komparativ konstitutionell rätt.* 2 uppl. Iustus Förlag AB s. 117–142.

Bull, Thomas och Sterzel, Fredrik (2019), *Regeringsformen – en kommentar*. Studentlitteratur AB.

Cameron, Iain, (2000), *National Security and the European Convention on Human Rights.* Iustus Förlag AB.

Cameron, Iain, (2010), *'Expert report to the Inquiry on Certain Police Methods'*, i SOU 2010:103 Särskilda spaningsmetoder, s.427-492.

Cameron, Iain (2015), '*Law Enforcement Access to Metadata in Sweden*', i Lind, Anna-Sara, och Reichel, Jane och Österdahl, Inger, (redaktörer), (2015), *Information and Law in Transition – Freedom of Speech, the Internet, Privacy and Democracy in the 21st Century*. 1 uppl. Liber AB s. 136–146.

Carey, Peter, (2009), *Data Protection A Practical Guide to UK and EU Law*. 3 uppl. Oxford University Press.

Danelius, Hans, (2015), *Mänskliga rättigheter i europeisk praxis En kommentar till Europakonventionen om de mänskliga rättigheterna.* 5 uppl. Norstedts Juridik AB.

Derlén, Mattias och Lindholm, Johan och Naarttijärvi, Markus, (2016), *Konstitutionell rätt.* 1 uppl. Wolters Kluwer Sverige AB.

Foster, Nigel och Sule, Satish, (2010), *German Legal System and Laws.* 4 uppl. Oxford University Press.

Gellert, Raphaël, (2020), *The Risk-Based Approach to Data Protection.* 1 uppl. Oxford University Press.

Gutwirth, Serge, (2002), *Privacy and the Information Age.* Rowman & Littlefield Publishers, Inc.

Gutwirth, Serge och Poullet, Yves och De Hert, Paul och Leenes, Ronald (red.) (2011), *Computers, Prvacy and Data Protection: an Element of Choice*, Springer Science+Business Media B.V, https://link-springer-com.ludwig.lub.lu.se/content/pdf/10.1007%2F978-94-007-0641-5.pdf e-bok besök 2021-03-11.

Hiller, Vera, (2014), *Der Konflikt zwischen Persönlichkeitsschutz und Pressefreihet im deutschen und schwedischen Recht – Unter besonderer Berücksichtigung des Rechts am eigenen Bild.* 1 uppl. Nomos Verlagsgesellschaft.

Hirschfeldt, Johan (2014), '*Författningens kärnvärden – symbolik, politik och juridik*', i Åhman, Karin, *Regeringsformen 40 år 1974–2014.* Uppl. 1. Iustus Förlag AB s. 33–56.

Hobbes, Thomas (1651), *Leviathan* / *Thomas Hobbes; edited with an introduction and notes by J.C.A. Gaskin*, Oxford University Press, (1998), https://eds-b-ebscohost-com.ludwig.lub.lu.se/eds/ebookviewer/ebook/bmxlYmtfXzEyMzA5X19BTg2?sid=609b629a-b594-4e4b-bfb7-a467a955aecc@pdc-v-sessmgr01&vid=0&format=EB&rid=1
e-bok besökt 2021-02-26.

Husa, Jaakko, (2015), *A New Introduction to Comparative Law.* Hart Publishing Ltd.

Husa, Jaakko (2017a), '*Methodology of Comparative Law Today: From Paradoxes to Flexibility?*', i Adams, Maurice och Husa, Jaakko och Oderkerk, Marieke, *Comparative Law Methodology.* Volym I. Edward Elgar Publishing Limited. s. 51-95.

Husa, Jaakko (2017b), *'Interdisciplinary Comparative Law – Between Scylla and Charybdis?'*, i Adams, Maurice och Husa, Jaakko och Oderkerk, Marieke, *Comparative Law Methodology.* Volym II. Edward Elgar Publishing Limited. s. 25-39.

Häthén, Christian, (2014), *Stat och straff.* 2 uppl. Studentlitteratur AB.

Ipsen, Jörn, (2019), *Allgemeines Verwaltungsrecht.* 11 uppl. Verlag Franz Vahlen.

Jensen, Ulf och Rylander, Staffan och Lindblom, Per Henrik (2018), *Att skriva juridik.* 6 uppl. Iustus Förlag AB.

Jermsten, Henrik (2018), *Kommentar till regeringsformen (1974:152) 2 kap. 6 §* i Eka, Anders och Hirschfeldt, Johan och Jermsten, Henrik och Svahn Starrsjö, Kristina (2018), *Regeringsformen* – med kommentar –. 2 uppl. Karnov Group AB s. 102–109.

Jonsson Cornell, Anna (2015a), '*Den komparativa konstitutionella rättens teori och metod – en introduktion*', i Jonsson Cornell, Anna (red.), *Komparativ konstitutionell rätt.* 2 uppl. Iustus Förlag AB s. 17-38.

Jonsson Cornell, Anna (2015b), '*Privacy Rights and Data Protection in Law Enforcement Cooperation: Comparing the US and EU*', i Lind, Anna-Sara, och Reichel, Jane och Österdahl, Inger, (redaktörer), *Information and Law in Transition – Freedom of Speech, the Internet, Privacy and Democracy in the 21st Century.* 1 uppl. Liber AB s. 170-193.

Kelleher, Denis och Murray, Karen, (2018), *EU Data Protection Law.* 1 uppl. Bloomsbury Professional Ltd.

Kischel, Uwe (2019), *Comparative Law.*1 uppl. Oxford University Press.

Kleineman, Jan (2013), '*Rättsdogmatisk metod* ', i Korling, Fredric och Zamboni, Mauro (red.), *Juridisk metodlära.* Studentlitteratur AB s. 21–45.

Koch, Søren och Skodvin Knut Einar och Øyrehagen Sunde, Jørn (red.), (2017), *Comparing Legal Cultures.* Fagbokforlaget.

Knott, Maria (1986), '*Inhalt und Schranken des Rechts auf „informationelle Selbstbestimmung" nach dem Urteil des Bundesverfassungsgerichts zum Volkzählungsgesetz*', i Vollkommer, Max (red.), *Datenverarbeitung und Persönlichkeitsschutz – Beiträge zu aktuellen Problemen des Datenschutzes in Recht und Praxis.* Universitätsbund Erlangen-Nürnberg e.V. s. 45–63.

Kuner, Christopher, (2003), *European Data Privacy law and Online Business.* 1 uppl. Oxford University Press.

Kuner, Christopher och Bygrave, Lee A. och Docksey, Christopher, (2020), *The EU General Data Protection Regulation (GDPR) A Commentary.* I uppl. Oxford University Press.

Kutscha, Martin (2006), *Wörterbuch zur Inneren Sicherheit*, https://link.springer.com/chapter/10.1007/978-3-531-90596-9_82 E-bok, besökt 2021-02-06.

Leenes, Ronald och Gutwirth, Serge och van Brakel, Rosamunde och De Hert, Paul och (red.) (2017), *Data Protection and Privacy: (In)visibilities and Infrastructures.* E bok: *https://link-springer-com.ludwig.lub.lu.se/content/pdf/10.1007%2F978-3-319-50796-5_1.pdf* Besökt 2021-05-29.

Lindahl, Rutger, (red.), (2007), *Utländska politiska system.* 12 uppl. SNS Förlag.

Lynskey, Orla, (2015) *The Foundations of EU Data Protection Law.* 1 uppl. Oxford University Press.

Löw, Konrad, (red.) (1994), *Terror und Extremismus in Deutschland.* Duncker & Humblot GmbH.

Mill, John Stuart, (1960), *Utilitarianism, liberty, representative government.* J. M. Dent & Sons Ltd.

Modéer, Kjell Å, (2009), *Juristernas nära förflutna Rättskulturer i förändring.* Santérus Förlag.

Müthlein, Thomas, (red.), (2017), *Datenschutz-Grundverordnung - General Data Protection Regulation.* 2 uppl. Datakontext GmbH.

Naarttijärvi, Markus, (2013) *För din och andras säkerhet – konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*. Iustus Förlag AB.

Nergelius, Joakim, (1996), *Konstitutionellt rättighetsskydd.* 1 uppl. Fritzes Förlag AB.

Nergelius, Joakim, (2014), *Svensk statsrätt.* 3 uppl. Studentlitteratur AB.

Nergelius, Joakim, (2018a), *Svensk statsrätt.* 4 uppl. Studentlitteratur AB.

Nergelius, Joakim, (2018b), *Komparativ statsrätt.* 9 uppl. Juristförlaget i Lund.

Ogorek, Markus *Anlasslose Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage,* Neue Juristische Wochenschrift, NJW 2021, 531.

Petersen, Niels, (2017), *Proportionality and Judicial Activism.* Cambridge University Press.

Prölss-Peter, Jutta, (1986), '*Moderne Verwaltung und Datenschutz – Sicherheitsinteresse contra Bürgerfreiheit-*, i Vollkommer, Max (red.), *Datenverarbeitung und Persönlichkeitsschutz – Beiträge zu aktuellen Problemen des Datenschutzes in Recht und Praxis*'. Universitätsbund Erlangen-Nürnberg e.V. s. 65–82.

Reichel, Jane (2012), '*Hur kontrolleras EU-rätten i Sverige- vad gör riksdagen?* ', i *Arvet från Oxenstierna – reflektioner kring den svenska förvaltningsmodellen och EU.* Sieps Svenska institutet för europeiska studier s. 58–74.

Reichel, Jane, (2013), '*EU-rättslig metod*', i Korling, Fredric och Zamboni, Mauro (red.), *Juridisk metodlära.* Studentlitteratur AB s. 109-140.

Reichel, Jane, (2017), '*The Swedish right to freedom of speech, EU data protection law and the question of territoriality*', i Lind, Anna-Sara, och Reichel, Jane och Österdahl, Inger, (redaktörer), *Transparency in the future – Swedish openness 250 years.* Ragulka press s. 201-224.

Robbers, Gerhard, (2019), *An Introduction to German Law.* 7 uppl. Nomos Verlagsgesellschaft.

Robinson, Olivia F och Fergus, T David och Gordon, William M, (2000), *European Legal History.* 3 uppl. Oxford University Press.

Roßnagel, Alexander (2017) *Vorratsdatenspeicherung rechtlich vor dem Aus?*, Neue Juristische Wochenschrift, NJW 2017, 696.

Sandgren, Claes (2009), *Vad är rättsvetenskap?* Jure Förlag AB.

Sandgren, Claes (2015), *Rättsvetenskap för uppsatsförfattare.* 3 uppl. Norstedts Juridik AB.

Schneider, Jochen, (2017), *Datenschutz nach der EU-Datenschutz-Grundverordnung.* Verlag C.H. Beck oHG.

Schwan, Eggert, (1984), *Amtsgeheimnis oder Aktenöffentlichkeit? Der Auskunftsanspruch des Betroffenen, das Grundrecht auf Datenschutz und das Prinzip der Aktenöffentlichkeit.* J. Schweitzer Verlag.

Siemen, Birte, (2006), *Datenschutz als europäisches Grundrecht.* Duncker & Humblot GmbH.

Solove, Daniel J., (2011), *Nothing to Hide: the False Tradeoff between Privacy and Security.* 1 uppl. Yale University Press.

Sterzel, Fredrik, (2009), *Författning i utveckling* - tjugo studier kring Sveriges författning. Iustus Förlag AB.

Sterzel, Fredrik, (2015), '*Sverige*', i Jonsson Cornell, Anna (red.), *Komparativ konstitutionell rätt.* 2 uppl. Iustus Förlag AB s. 71–92.

Stollreither, Konrad, (1986), '*Der gläserne Mensch – noch Zukunft oder schon Gegenwart?*', i Vollkommer, Max (red.), *Datenverarbeitung und Persönlichkeitsschutz – Beiträge zu aktuellen Problemen des Datenschutzes in Recht und Praxis.* Universitätsbund Erlangen-Nürnberg e.V. s. 15–27.

Strömholm, Stig (1971), *Integritetsskyddet Ett försök till internationell lägesbestämning.* SvJT 1971 s. 695–736.

Strömholm, Stig (1980), '*Individens skyddade personlighetssfär*' i *Om våra rättigheter* (1980) antologi utgiven av Rättsfonden. Almqvist & Wiksell s. 23–39.

Trolle Önnerfors, Elsa och Wenander, Henrik, (2016), *Att skriva rätt Goda råd för att skriva uppsats i juridik.* 1 uppl. Wolters Kluwer Sverige AB.

Trolle Önnerfors, Elsa och Wenander, Henrik, (2019), *Att skriva rätt Goda råd för att skriva uppsats i juridik.* 2 uppl. Wolters Kluwer Sverige AB.

Warnling Conradson, Wiweka och Bernitz, Hedvig och Sandström, Lena och Åhman, Karin (2018), *Statsrättens grunder.* 6 uppl. Norstedts Juridik AB.

Wenander, Henrik (2011), *'En princip om internationell öppenhet – 1 kap. 10 § regeringsformen och socialförsäkringsrätten'*. Förvaltningsrättslig tidskrift 3/2011.

Wenander, Henrik (2016), *Myndighetsföreskrifter – Demokratisk anknytning, politisk styrning och rättssäkerhet*. Tidsskrift for Rettsvitenskap 05/2016 (Volum 129).

Wennerström, Erik, (1999), *Några främmande staters politiska system.* 5 uppl. Iustus Förlag AB.

Westin, Alan F., (1968), *Privacy and Freedom.* Atheneum for the Assoc. of the Bar of the City of New York.

Zekoll, Joachim och Reimann, Mathias, (2005), *Introduction to German Law.* 2 uppl. Kluwer Law International.

Zweigert, Konrad och Kötz, Hein (1998), *Introduction to Comparative Law.* 3 uppl. Oxford University Press.

Österdahl, Inger, (2015), '*Transparency versus Secrecy in an International Context: a Swedish Dilemma*', i Lind, Anna-Sara, och Reichel, Jane och Österdahl, Inger, (redaktörer), *Information and Law in Transition – Freedom of Speech, the Internet, Privacy and Democracy in the 21st Century.* 1 uppl. Liber AB s. 74-99.

Litteratur, övrig

Rättsfallsreferat, osignerat på Beck-Online, *Verfassungswidrige Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten,* Neue Juristische Wochenschrift, NJW 2010, 833.

Elektroniska källor

Advokatfirman Delphis Techblog, *e-Privacy-förordningen (EPR) alltmer avlägsen,* publicerad 2020-02-17 17 https://www.delphi.se/sv/tech-blog/e-privacy-forordningen-epr-alltmer-avlagsen/ besökt 2021-01-08.

Beck-Online osignerad artikel publicerad 2017-06-22, Becklink 2007033, *OVG Münster: in TKG vorgesehene Vorratsdatenspeicherung verstößt gegen Unionsrecht*, https://beck-online-beck-de.ludwig.lub.lu.se/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2

007033.htm&anchor=Y-300-Z-BECKLINK-N-2007033&jumpType=Jump&jumpWords=Becklink%2B2007033
besökt 2021-03-23.

Deutscher Bundestag, Drucksache 17/8999, 17. Wahlperiode 15. 03. 2012, https://dserver.bundestag.de/btd/17/089/1708999.pdf
besökt 2021-03-03.

Deutscher Bundestag Drucksache 17/12290 17. Wahlperiode 06. 02. 2013, https://dserver.bundestag.de/btd/17/122/1712290.pdf
besökt 2021-03-03.

Holland, Martin, *Paris: EuGH-Urteil gegen Vorratsdatenspeicherung verletzt* ”*Verfassungsidentität*”, publicerad på Heise Online 2021-03-04, https://www.heise.de/amp/news/Paris-EuGH-Urteil-gegen-Vorratsdatenspeicherung-verletzt-Verfassungsidentitaet-5072311.html
Besökt 2021-03-05.

Hornung, Gerrit och Schnabel, Christoph, *Data protection in Germany I: The population census decision and the right to informational self-determination*, publicerad i Computer Law & Security Report, Volume 25, Issue 1, 2009, p. 84-88, tillgänglig via Universität Kassel: https://www.uni-kassel.de/fb07/index.php?eID=dumpFile&t=f&f=566&token=982b30547e56fb9f2eb130a7b27c177d774c20e2

Herlin-Karnell, Ester, *Corona and the Absence of a Real Constitutional Debate in Sweden*, Verfassungsblog, publicerad 2020-04-10 https://verfassungsblog.de/corona-and-the-absence-of-a-real-constitutional-debate-in-sweden/
Besökt 2020-09-14.

Infrastrukturdepartementet, Sekretariatet för EU och internationella frågor, kommenterad dagordning till videomöte den 7 december 2020 med telekommunikationsministrar: https://www.regeringen.se/4ad8fc/contentassets/ea32daec918d41a7af001bbd31a01a27/kommenterad-dagordning-infor-telekommunikationsministrarnas-informella-videomote-7-december-2020
besökt 2021-01-08.

Karlung, Jon, *Bahnhof inför datalagring, men endast i ”kassaskåpet” som inte är avsedd för upphovsrättsmaffian*, publicerad 2019-09-30 Bahnhof, https://bahnhof.se/press/press-releases/2019/09/30/bahnhof-infor-datalagring-men-endast-i-kassaskapet-som-inte-ar-avsedd-for-upphovsrattsmaffian besökt 2021-01-29.

Norman, Pernilla och Wallenius, Wictor, *Dataskydd vid brottsbekämpning – EU-domstolen förtydligar intresseavvägning*, Juno internet publicerad 2020-10-13, https://juno-nj-se.ludwig.lub.lu.se/b/documents/3382793?dq=direktiv%202002%2F58%2F

eg%20dataskydd%20integritet&persist=document&t=eu_court_of_justice_rulings#SUMCLX_6_2017_CJ_0623 Besökt 2021-03-08.

Post-och telestyrelsen, *Samtrafik*, uppdaterad 2021-02-24, https://www.pts.se/sv/bransch/telefoni/konkurrensreglering-smp/fast-samtrafik/ Besökt 2021-03-14.

Elektroniska lagkommentarer

Andersson, Per G. kommentar till lag (2003:389) om elektronisk kommunikation 6 kap. 16 a § JUNO internet, not 288, besökt 2021-02-20.

Andersson, Per G. kommentar till lag (2003:389) om elektronisk kommunikation 6 kap. 16 a § JUNO internet, not 290, besökt 2021-02-20.

Jermsten, Henrik kommentar till regeringsformen (1974:152) 2 kap. 6 §, not 28, JUNO internet, besökt 2021-03-03.

Jermsten, Henrik kommentar till regeringsformen (1974:152) 2 kap. 6 §, JUNO internet/ Lexino version 2019-01-01 senast genomgången 2021-01-01, besökt 2021-03-03.

Svahn Starrsjö, Kristina kommentar till regeringsformen (1974:152) 10 kap. 6 §, not 266, JUNO internet, besökt 2021-02-01.

Lagkommentar till 113 a§ Telekommunikationsgesetz, TKG, Beck-Online. BeckOK StPO/Bär, 38. Ed. 1.10.2020, TKG § 113a Rn. 1–19 https://beck-online-beck-de.ludwig.lub.lu.se/Dokument?vpath=bibdata%2Fkomm%2Fbeckokstpo_38%2Ftkg%2Fcont%2Fbeckokstpo.tkg.p113a.htm
besökt 2021-03-09.

Europeiska unionen

Europeiska kommissionen

Förslag till Europaparlamentets och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation) KOM (2017)10 slutlig 2017/03 (COD).

Förslag till Europaparlamentets och rådets direktiv om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG, KOM (2005) 438 slutlig – 2005/0182 (COD).

Förslag till RÅDETS BESLUT om bemyndigande för medlemsstaterna att i Europeiska unionens intresse underteckna protokollet om ändring av Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (CETS nr 108), KOM (2018) 449 slutlig 2018/0237(NLE).

Rättsfallsförteckning

EU-domstolen

C-399/11, Stefano Melloni mot Ministerio Fiscal, EU:C:2013:107.

Förenade målen C-293/12 och C-594/12 Digital Rights Ireland Ltd mot Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung m.fl. EU:C: 2014:238.

C-131/12 Google Spain SL och Google Inc. mot Agencia Española de Protección de Datos (AEPD) och Mario Costeja González EU:C: 2014:317

C-362/14 Maximillian Schrems mot Data Protection Commissioner EU:C: 2015:650

Tele2 Sverige AB v Post- och telestyrelsen och Secretary of State for the Home Department mot Tom Watson m.fl., EU:C:2016:970.

C-207/16, Ministerio Fiscal, EU:C:2018:788

C-623/17 Privacy International mot Secretary of State for Foreign and Commonwealth Affairs m.fl., EU:C:2020:790

Förenade målen C-511/18, C-512/18 och C-520/18.La Quadrature du Net m.fl. mot Premier ministre m.fl., EU:C:2020:791.

C-746/18, (H K/Prokuratuur), EU:C:2021:152

Europeiska domstolen för de mänskliga rättigheterna

von Hannover v. Germany, no 59320/00, ECHR 2004-VI

K.U. v. Finland, no. 2872/02, ECHR 2008-XII

Söderman v. Sweden, no 5786/08, ECHR 2013-XI

Big Brother Watch and others v. the United Kingdom, nos. 58170/13, 62322/14, 24960/15, ECHR 2018-IX

Övriga svenska domstolar och förvaltningsmyndigheter

Kammarrätten i Stockholm mål 7380–14, dom 2017-03-07.

Kammarrätten i Stockholm mål 2471–18, dom 2018-12-14.

Utländsk rättspraxis

Tyskland

Författningsdomstolen (Bundesverfassungsgericht)

BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983
- 1 BvR 209/83 -, Rn. 1-215,

BVerfG, Urteil des Ersten Senats vom 02. März 2010
- 1 BvR 256/08 -, Rn. 1-345,

Regional domstol för delstaten Nordrhein-Westfalen
(Oberverwaltungsgericht für das Land Nordrhein-Westfalen)

OVG Nordrhein-Westfalen, 22.06.2017 - (Az. 13 B 238/17)