RÉTTURINN TIL AÐ GLEYMAST OG TIL AFMÁUNAR

Heiðdís Lilja Magnúsdóttir

2014
ML í lögfræði

Höfundur: Heiðdís Lilja Magnúsdóttir
Kennitala: 071172-4659
Leiðbeinandi: Páll Þórhallsson
Lagadeild
School of Law

Ágrip

-Rétturinn til að gleymast og til afmáunar

Ritgerð þessi fjallar um þær reglur sem gilda um afmáun persónuupplýsinga á netinu í drögum framkvæmdastjórnar ESB að reglugerð um vernd persónuupplýsinga og frjálsa miðlun slíkra upplýsinga, frá 2012. Markmiðið er að gera úttekt á réttinum til að gleymast og til afmáunar í 17. gr. reglugerðardraganna, helstu álitaefnum um inntak hans og hverjir beri ábyrgð á framkvæmd hans.
Í upphafi er farið yfir helstu nýmæli í endurskoðaðri persónuverndarlöggjöf ESB. Fjallað er um núgildandi persónuvernarlöggjöf og alþjóðlegar reglur sem þýðingu hafa. Því næst er ítarleg umfjöllun um réttinn til að gleymast og til afmáunar og þær breytingar sem gerðar voru á 17. gr. reglugerðardraganna í meðförum Evrópuþingsins í mars 2014. Fjallað er um grundvallarréttindi sem skarast við réttinn til að gleymast og til afmáunar og undanþágur frá gildissviði laganna. Loks er sjónum beint að ábyrgð notenda, þjónustuveitenda og milligönguaðila, með áherslu á samfélagsmiðla og leitarvélar.
Meginniðurstaða ritgerðarinnar er að 17. gr. reglugerðardraga framkvæmdastjórnarinnar, og samspil þess ákvæðis við 19. gr. um andmælarétt, felur í sér aukinn rétt fyrir hinn skráða. Eigendur samfélagsmiðla teljast ábyrgðaraðilar þar sem þeir ákveða tilgang og vinnslu persónuupplýsinga. Hins vegar er ekki ljóst hvort réttur til afmáunar tekur til einstaklinga á samfélagsmiðlum eða hvort svokölluð heimilishaldsundantekning á þá við. Bent er á að varhugavert sé að stjórnendur samfélagsmiðla og leitarvélafyrirtækja fari með ritskoðunarvald í samfélaginu og að slíkt fyrirkomulag geti leitt til óeðlilegrar íhlutunar í tjáningarfrelsi. Loks er niðurstaðan sú að með úrskurði Evrópudómstólsins í máli C-131/12 frá 13. maí 2014, þess efnis að fyrirtæki sem reka leitarvélar á netinu teljist ábyrgðaraðilar, geti rétturinn til að gleymast og til afmáunar falið í sér skilvirkan rétt til að hindra aðgang að persónuupplýsingum eða fá þeim varanlega eytt af netinu.

Abstract

-The Right to be Forgotten and to Erasure

This thesis discusses the rules on erasing personal data from the Internet which are set forth by the European Commission in its 2012 legislative proposal for a Regulation on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data. The object of the thesis is to examine the right to be forgotten and to erasure which is stated in Article 17 of the draft regulation. The beginning of the thesis explains the pioneering aspects of the European Union's revised legal framework on personal data. There is an extensive treatment of the right to be forgotten and to erasure, including amendments which the European Parliament made to Article 17 of the proposed Regulation. The final focus is on the responsibility of users, service providers and intermediaries, with a particular emphasis on social media and search engines.
The main findings of the thesis are that Article 17 of the draft regulation incorporates extended rights for individuals. Furthermore, Article 19 strengthens the rights of data subjects with an extended right to object. Operators of social networking services are considered to be data controllers, since they determine the purposes and means of the processing of personal data. However, it remains unclear whether individual users of social networking services are also data controllers or whether they are entitled to the so called „household exemption“. The final conclusion is that following the judgment of the Court of Justice of the European Union in Case C-131/12 from 13 May 2014, where an internet search engine provider was considered to be a data controller in relation to search returns, the right to be forgotten and to erasure can provide for an effective right to block or erase personal data permanently off the internet.

Efnisyfirlit

Lagaskrá v

Dóma- og úrskurðaskrá vii

1 Inngangur: Endalok einkalífs eða öruggt skjól? 1

2 Endurskoðun persónuverndarlöggjafar ESB 5

2.1 Inngangur 5

2.2 Tilgangur og helstu nýmæli nýrrar reglugerðar 5

2.2.1 Einsleitni á EES svæðinu 6

2.2.2 Aukinn sjálfsákvörðunarréttur hins skráða, sérstaklega á netinu 6

2.2.3 Aukið gegnsæi og ábyrgð þeirra sem vinna með persónuupplýsingar 6

2.2.4 Styrking persónuverndarstofnana í hverju landi 7

2.2.5 Ein stofnun fer með mál 7

2.2.6 Vinnsla upplýsinga utan EES svæðisins 7

2.3 Staða mála í maí 2014 8

2.3.1 Evrópuþingið 8

2.3.2 Ráðið (Ráðherraráðið) 8

2.3.3 Evrópska ráðið 9

2.3.4 Næstu skref 9

2.4 Uppljóstranir Edwards Snowden og áhrif þeirra á framvindu mála 9

3 Lagaumgjörð og almenn hugtök 11

3.1 Meginreglur í persónuupplýsingalöggjöf 11

3.2 Almenn lög 12

3.3 Friðhelgi einkalífs og vernd persónuupplýsinga 13

3.4 Lagaleg staða persónuupplýsingaverndar í Evrópu 14

3.5 Almenn hugtök 16

3.5.1 Persónuupplýsingar 16

3.5.2 Vinnsla og skrá persónuupplýsinga 17

3.5.3 Ábyrgðaraðilar og vinnsluaðilar 17

3.5.4 Rafræn vöktun 19

3.5.5 Samþykki 19

3.5.6 Tilkynningarskylda 20

4 Rétturinn til að gleymast 21

4.1 Hvert er vandamálið? 21

4.2 Uppruni og þróun réttarins til að gleymast 23

4.2.1 Réttur til óminnis 25

4.2.2 Réttur til afmáunar 27

4.2.3 Réttur til að gleymast 30

4.3 Friðhelgi einkalífs og tjáningarfrelsi 33

4.3.1 Takmarkanir á grundvelli tjáningarfrelsis 35

4.3.1.1 Fréttamennska og bókmenntaleg og listræn starfsemi 35

4.3.1.2 Framlag til samfélagsumræðu og áhugi almennings 37

4.3.1.3 Opinberar persónur 38

4.3.2 Aðgangur að upplýsingum 40

4.3.3 Listrænt og vísindalegt frelsi 41

4.4 Áhrif hertrar persónuverndarlöggjafar í Evrópu á viðskiptahagsmuni bandarískra fyrirtækja 42

4.5 Ákvæði 17. greinar, tengd ákvæði og Albrecht-skýrslan 43

4.5.1 Aðgangur og leiðrétting 43

4.5.2 Rétturinn til að gleymast í 17. gr. 44

4.5.2.1 Skilyrði 17. gr. fyrir afmáun persónuupplýsinga 45
4.5.3 Andmælaréttur 45
4.6 Samanburður á 17. gr. reglugerðardraga framkvæmda-stjórnarinnar fyrir og eftir breytingar Evrópuþingsins 47
4.6.1 Yfirskrift 17. gr. 51
4.6.2 Ákvæði 1. mgr. 17. gr. 51
4.6.2.1 Vernd barna 51
4.6.2.2 Aðrar breytingar í 1. mgr. 51
4.6.3 Ákvæði 2. mgr. 17. gr: Vinnsla þriðju aðila 52
4.7 Takmarkanir og undanþágur 53
4.7.1 Undanþágur 3. mgr. 17. gr. 54
4.8 Samfélagsmiðlar og „heimilishaldsundantekningin“ 56
4.8.1 Albrecht-skýrslan um heimilishaldsundantekninguna 58
4.9 Ábyrgðaraðilar: Hverjum ber að eyða upplýsingunum? 59
4.9.1 Mál C-131/12 Google Spain SL og Google Inc. gegn spænsku Persónuverndarstofunni og Mario Costeja González 61
4.10 Takmörkun á ábyrgð milligönguaðila: Lög um rafræn viðskipti nr. 30/2002, sbr. tilskipun 2000/31 65
4.11 Hverjir geta farið fram á afmáun persónuupplýsinga á grundvelli réttarins til afmáunar? 66
4.12 Núgildandi réttur til afmáunar 69
4.12.1 Ísland 70
4.12.2 Noregur 71
4.12.3 Danmörk 72
4.12.4 Svíþjóð 73
4.12.5 Finnland 73
4.12.6 Ísland gekk lengst 73
4.13 Vernd barna 74
4.14 Viðurlög 76

5 Niðurstöður 77

Heimildaskrá 84

Lagaskrá

Íslensk lög

Lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga, með síðari breytingum.
Lög nr. 81/2003 um fjarskipti, fjarskiptaþjónustu og fjarskiptanet.
Lög nr. 30/2002 um rafræn viðskipti og aðra rafræna þjónustu.
Stjórnarskrá lýðveldisins Íslands nr. 33/1944, með áorðnum breytingum.

Erlend lög

Norræn löggjöf

LOV-2000-04-14-31 Lov om behandling af personopplysninger (personopplysningsloven).
L 2000-05-31 nr. 429 om behandling af personoplysninger.
Personuppgiftslag 1998:204.
Henkilötietolaki 22.4. 1999/523.

Evrópuréttur

Consolidated Version of the Treaty on European Union [2008] OJ C115/13.
Charter of Fundamental Rights of the European Union [2000] C 364/01.
Directive 95/46/EU of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1.
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2000] OJ L201/37.
Regulation (EC) nr. 1049 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission Documents [2001] OJ L145/43.

Alþjóðlegir sáttmálar

Samningur um verndun mannréttinda og mannfrelsis (Mannréttindasáttmáli Evrópu), (samþykktur 4. nóvember 1950, tók gildi 3. september 1953, undirritaður fyrir Íslands hönd 19. júní 1953, fullgiltur á Íslandi 3. september 1953 og lögfestur 30. maí 1994) Stjtíð. C, 11/1954.

Samningur um vernd einstaklinga varðandi vélræna vinnslu persónuupplýsinga nr. 108 (samþykktur 28. janúar 1981, tók gildi 1. október 1985, undirritaður fyrir Íslands hönd 27. september 1982 og fullgiltur á Íslandi 1. júlí 1991) Stjtíð. C, 5/1991.

Universal Declaration of Human Rights (10. desember 1948) UNGA Res 217 A(III) (UDHR).

Alþingistíðindi

Alþt. 1999-2000, A-deild, þskj. 399 – 280. mál.

Alþt. 1995-96, A-deild, þskj. – 361. mál.

Lög sem fallin eru úr gildi

Lög nr. 121/1989, um skráningu og meðferð persónuupplýsinga.

Dóma- og úrskurðaskrá

Íslenskir dómar og úrskurðir

Hæstaréttardómar

Ásbjörn Morthens g. 365 og Garðari Úlfarssyni, Hrd. 1. mars 2007 í máli nr. 278/2006.

Ásgeir Þór Davíðsson g. Björk Eiðsdóttur og Guðrúnu Elínu Arnardóttur, Hrd. 5. mars 2009 í máli nr. 328/2008.

Úrskurðir og álit Persónuverndar

Umfjöllun um morðmál í dagblaði: Álit Persónuverndar, [dagsetningu vantar] 2003.

Úrskurður Persónuverndar 18. apríl 2005 í máli nr. 2004/568.

Úrskurður Persónuverndar 22. júní 2011 í máli nr. 2011/231.

Ákvörðun Persónuverndar 10. maí 2011 í máli nr. 2011/73.

Ákvörðun Persónuverndar [dagsetningu vantar] 2012 í máli nr. 2011/1301.

Ákvörðun Persónuverndar 17. janúar 2012 í máli nr. 2011/1346.

Erlendir dómar

Dómar Evrópudómstólsins

Mál C-101/01 *Lindqvist* [2003] ECR I-12971.

Mál C-465/00, C-138/01 og C-139/01 *Rechnungshof g. Österreichischer Rundfunk and Others* [2003] ECR I-4989.

Mál C-73/07 *Tietosuojavaltuutettu g. Satakunnan Markkinapörssin Oy og Satamedia Oy* [2008] ECR I-9831.

Mál C-131/12 *Google Spain SL og Google Inc g. Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [ECR 13. maí 2014].

Dómar Mannréttindadómstóls Evrópu

Leander g. Svíþjóð (1987) Series A. 116, mgr. 48.

Muller og aðrir g. Sviss App no. 10737/84 (ECtHR, 24. maí 1988).

Editions Plon g. Frakklandi App no. 58148/00 (ECtHR, 18. maí 2004).

Von Hannover g. Þýskalandi App no. 59320/00 (ECtHR, 24. júní 2004).

Steel og Morris g. Bretlandi App no. 68416/01, 94. mgr. (ECtHR, 15. febrúar 2005).

Anghel g. Moldóvu App no. 42864/05, 34 mgr. (ECtHR, 27. nóvember 2007).

Copland g. Bretlandi ECHR App no. 62617/00 (ECtHR, 3. apríl 2007).

Mosley g. Bretlandi App no. 48009/08 (ECtHR, 10. maí 2011).

Von Hannover g. Þýskalandi App no. 40660/08 og 60641/08 (ECtHR, 7. febrúar 2012).

Björk Eiðsdóttir g. Íslandi App no. 46443/09, 68. mgr. (ECtHR, 10. júlí 2012).

Aðrir erlendir dómar

Snyder g. Millersville University, et al., 2008 WL 5093140 (E.D. Pa., 2008).

Högsta domstolen, dom 2001-06-12 i mål nr. B 293-00.

Sentencia Juz. 1.ª Inst. Amposta (núm. 1) 32/2012, de 23 de febrero.

BVerfGE 65, 1.

BverfG, 25.11.1999 - 1 BvR 348/98 og 1 BvR 755/98.

BGH, 10.11.2009 - VI ZR 217/08.

BGH 15.12.2009 - VI ZR 227/08 og 228/08.

BGH 09.02.2010 - VI ZR 243/08 og 244/08.

BGH apríl 2010 - VI ZR 245/08 og 246/08.

BGH 01.02.2011 - VI ZR 345/09.

BGH 01.02.2011 - VI ZR 346/09.

BGH 01.02.2011 - VI ZR 114/09.

1 Inngangur: Endalok einkalífs eða öruggt skjól?

Óhætt er að fullyrða að í síbreytilegum heimi samskipta- og upplýsingatækni hafi hallað á friðhelgi einkalífs á síðustu árum. Sumir tala um endalok einkalífs.[1] Tilkoma tölvuskýja,[2] þar sem upplýsingar um einstaklinga eru samkeyrðar í nafni markaðssetningar eða opinbers eftirlits, og hryllingssögur af því hvernig brotið hefur verið á friðhelgi fólks með myndbirtingum á netinu, hafa vakið spurningar um forræði netnotenda yfir eigin persónuupplýsingum.

Netið gleymir engu, er gjarnan sagt. Það sem eitt sinn fer á Netið á oft ekki afturkvæmt. Eðli Netsins, þar á meðal samfélagsmiðla á borð við Facebook og Twitter, er slíkt að auðvelt er að valda óbætanlegum skaða á augabragði. Hver sem er, á hvaða aldri sem er getur birt persónulegar upplýsingar um sjálfan sig eða aðra á netinu. Sannar sem ósannar upplýsingar, sem hingað til hefur verið erfitt eða ómögulegt að fá eytt eftir á.

Þessu vill framkvæmdastjórn Evrópusambandsins breyta. Til að bregðast við breyttum aðstæðum; tækniþróun, hnattvæðingu og nýjum ógnum við friðhelgi einkalífs, fer um þessar mundir fram allsherjarendurskoðun á persónuupplýsingatilskipun 95/46/EB og fleiri persónuverndarreglum Evrópusambandsins. Tilgangurinn er að vernda friðhelgi einkalífs á netinu, tryggja frjálst flæði upplýsinga á innri markaði ESB og styrkja rafrænt hagkerfi Evrópu.[3]

Fyrir liggja drög að nýrri reglugerð á sviði persónuupplýsingaréttar, um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga, sem hafa mun bein réttaráhrif innan ESB og sem EES-ríkin þurfa að lögfesta, taki hún gildi og verði tekin upp í EES-samninginn á vettvangi sameiginlegu EES-nefndarinnar. Samhliða þessu er unnið að nýrri tilskipun um vinnslu persónuupplýsinga í tengslum við varnir gegn afbrotum og rannsóknir á þeim.[4]

Tilskipun 95/46/EB er orðin 19 ára gömul. Sá tæknilegi veruleiki sem hún byggði á er liðin tíð. Ör tækniþróun á þessu sviði kallar á að reglur á sviði persónuupplýsingaréttar séu í stöðugri endurskoðun og að reglur um heimildir til vinnslu og meðferðar persónuupplýsinga séu skýrar.

---

[1] A. Michael Froomkin, „The Death of Privacy?“ (2000) 52 *Stanford Law Review* 1461.

[2] Tölvuský þýðir að gögn eru geymd á netþjóni („tölvuskýi“) en ekki á hörðum diski í staðartölvu.

[3] „LIBE Committee vote backs new EU data protection rules“ (*European Union*, 22. október 2013) <http://europa.eu/rapid/press-release_MEMO-13-923_en.htm> skoðað 29. apríl 2014.

[4] Björg Thorarensen og Sigrún Jóhannesdóttir, „Nýjar ógnir og ný úrræði í persónuvernd“ *Fréttablaðið* (Reykjavík, 17. október 2012) 16.

Endurskoðun persónuverndarlöggjafar Evrópusambandsins miðar að því að stemma stigu við brotum á friðhelgi einkalífs og færa einstaklingum ríkari rétt til sjálfsákvörðunar og ráðstöfunar á eigin persónuupplýsingum. Að bregðast við breyttri heimsmynd og tækniþróun sem snertir okkur flest. Á Íslandi teljast 95% landsmanna til reglulegra netnotenda, samkvæmt rannsókn Hagstofu Evrópusambandsins, Eurostat, og er það hærra hlutfall en í nokkru öðru Evrópuríki. Að meðaltali eru 72% landsmanna í ríkjum Evrópusambandsins reglulegir netnotendur.[5]

Í hinum nýju drögum ESB að reglugerð á sviði persónuupplýsingaréttar er sérstakt ákvæði sem kallast *réttur til að gleymast og til afmáunar* (á ensku: the right to be forgotten and to erasure). Ákvæðið, sem í umfjöllun fræðimanna og fjölmiðla hefur gengið undir nafninu *rétturinn til að gleymast*, felur í sér réttinn til að láta fjarlægja persónuupplýsingar um sig, þar á meðal af netinu, þegar þær hafa þjónað tilgangi sínum og þegar fólk krefst þess í málefnalegum og skýrt yfirlýstum tilgangi.[6]

Rétturinn til að gleymast og til afmáunar er ekki alveg nýr af nálinni. Forvera hans er að finna í almennu persónuupplýsingatilskipun Evrópusambandsins, 95/46/EB, sem innleidd var með lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.[7]

Í 17. gr. nýju reglugerðardraganna er að finna víðtækara ákvæði um réttinn til að gleymast og til afmáunar, þar sem hann er jafnframt orðaður skýrar en í núgildandi tilskipun. Í mars sl. samþykkti Evrópuþingið breytta útgáfu ákvæðisins og kallast það nú „right to erasure“ eða *réttur til afmáunar* og er umfjöllunarefni þessarar ritgerðar.

Rétturinn til að gleymast og til afmáunar, þar á meðal rétturinn til að láta fjarlægja persónuupplýsingar um sig af Netinu, er vandmeðfarinn og umdeildur. Deilt er um hversu víðtækur hann eigi að vera og hvort hugmyndin sé framkvæmanleg í raun, með hliðsjón af þeim óravíðáttum sem Netið hefur að geyma. Þá hefur verið deilt um það hvort rétturinn sé sjálfsagður hluti af friðhelgi einkalífs eða skerðing á tjáningar-, viðskipta- og fjölmiðlafrelsi.

Markmið þessarar ritgerðar er að gera úttekt á endurskoðun persónuverndarlöggjafar Evrópusambandsins, með áherslu á réttinn til að gleymast og til afmáunar: Hvað þýðir rétturinn til að gleymast og til afmáunar, til hvaða miðla tekur hann, hver á réttinn og hver ber

[5] „Tölvu- og netnotkun mest á Íslandi af öllum Evrópulöndum“ (*Hagstofa Íslands*, 27. janúar 2014) <http://hagstofa.is/Pages/95?NewsID=10778> skoðað 3. febrúar 2014.

[6] Commission, „Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and of the free movement of such data“ COM (2012)11 final (hér eftir reglugerðardrög framkvæmdastjórnarinnar), 17. gr.

[7] Directive 95/46/EU of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (hér eftir tilskipun 95/46/EB).

ábyrgð á framkvæmd hans? Sú rannsóknarspurning er viðfangsefni þessarar ritgerðar. Til að svara henni verður fjallað um uppruna og þróun réttarins til að gleymast og til afmáunar. Gerður verður samanburður á ákvæðum reglugerðardraganna, núgildandi tilskipunar 95/46/EB og laga nr. 77/2000 um rétt til afmáunar, auk þess sem fjallað verður um sambærileg ákvæði í löggjöf annarra Norðurlanda. Þá verður gerð ítarleg grein fyrir þeim breytingum sem gerðar voru á 17. gr. reglugerðardraganna í meðförum Evrópuþingsins í mars sl. Leitast verður við að skilgreina hvar mörk friðhelgi einkalífs og tjáningarfrelsis liggja og hversu mikið forræði almenningur hefur yfir þeim upplýsingum á Netinu sem varða þá sjálfa. Þá er sjónum beint að takmörkunum og undanþágum frá gildissviði laganna og fjallað um ábyrgð notenda, þjónustuveitenda og milligönguaðila, með sérstakri áherslu á samfélagsmiðla og leitarvélar. Í því skyni verður reifaður nýfallinn tímamótadómur Evrópudómstólsins um ábyrgð tölvufyrirtækisins Google frá 13. maí 2014.

Efnistök eru á þá leið sem hér segir:

Í öðrum kafla er fjallað um drög framkvæmdastjórnar ESB að nýrri reglugerð og tilskipun á sviði persónuverndar. Kaflinn byggir á frumgögnum og skrifum fræðimanna en einnig á útgefnum erindum sem finna má á heimasíðu framkvæmdastjórnarinnar, Evrópuþingsins og Evrópska ráðsins.
Í þriðja kafla verða grundvallarhugtök persónuverndarréttar skýrð til skilningsauka, auk þess sem þar er að finna stutta umfjöllun um lagaumgjörð, meginreglur og stöðu persónuupplýsingaverndar í Evrópu.
Í fjórða kafla er umfjöllun um *Réttinn til að gleymast* í víðu samhengi; uppruna og þróun réttarins, þá hugmyndafræði sem honum býr að baki og hvernig hann hefur verið túlkaður og útfærður í lögum. Fjallað verður um inntak og tilgang þess úrræðis sem framkvæmdastjórn ESB hefur lagt til í 17. gr. draga að reglugerð um vernd persónuupplýsinga og frjálsa miðlun slíkra persónuupplýsinga og farið ítarlega yfir þær breytingar sem gerðar voru á ákvæðinu í meðförum Evrópuþingsins. Þá verður farið yfir efnislegt gildissvið persónuverndarlöggjafar ESB og undanþágur og takmarkanir frá því. Þar á eftir verður skýrt nánar hverjir beri ábyrgð á því að upplýsingum sé eytt og hverjir eigi rétt á að krefjast þess en um hið fyrrnefnda verður meðal annars vísað til nýfallins dóms Evrópudómstólsins um rétt til afmáunar og ábyrgð leitarvélafyrirtækja. Sjónum verður beint að mörkum friðhelgi einkalífs og tjáningarfrelsis og öðrum grundvallarréttindum og hagsmunum sem skarast við réttinn til að gleymast. Því næst verður gerður samanburður á 17. gr. reglugerðardraganna, ákvæðum

tilskipunar 95/46/EB og ákvæðum laga nr. 77/2000 um rétt til afmáunar, og fjallað um sambærileg ákvæði í löggjöf annarra Norðurlanda. Loks er fjallað stuttlega um vernd barna og viðurlög. Kaflinn er fyrst og fremst byggður á frumgögnum, útgefnu efni fræðimanna, stofnana Evrópusambandsins og Evrópuráðsins og á sjálfstæðu framlagi höfundar.

Í fimmta kafla eru meginniðurstöður ritgerðarinnar dregnar saman og leitast við að draga ályktanir af umfjölluninni.

2 Endurskoðun persónuverndarlöggjafar ESB
2.1 Inngangur

> Þetta snýst um að tryggja að fólkið sem stýrir forritunum í snjallsímanum þínum viti ekki meira um líf þitt en fjölskylda þín. Þetta snýst um að afborganir af tryggingunum þínum hækki ekki í hvert skipti sem þú slærð inn sjúkdómsheiti í leitarvél. Þetta snýst um að myndir af þér á táningsárum verði ekki aðgengilegar á netinu að eilífu.[8]
>
> -*Viviane Reding, aðstoðarframkvæmdastjóri Evrópusambandsins, um drög framkvæmdastjórnar ESB að almennri reglugerð um vernd persónuupplýsinga og frjálsa miðlun slíkra upplýsinga, frá 25. janúar 2012.*

Vorið 2011 óskaði Evrópuþingið eftir endurskoðun persónuverndarlöggjafar ESB, þar á meðal tilskipunar 95/46/EB, sem þá var orðin 16 ára gömul og eðlilega í engu samræmi við þá miklu tækniþróun sem orðið hafði frá því hún tók gildi árið 1995. Gjörbreyttar aðstæður; hnattvæðing og ör tækniþróun, þóttu kalla á gagngerar breytingar á löggjöfinni.[9]

Þann 25. janúar 2012 lagði framkvæmdastjórn ESB fram tillögu að endurbótum á persónuverndarlöggjöf ESB, nánar tiltekið drög að almennri reglugerð um vernd persónuupplýsinga og frjálsa miðlun slíkra upplýsinga[10] og hins vegar drög að tilskipun um meðferð persónuupplýsinga í refsivörslukerfinu.[11] Verði reglugerðardrögin samþykkt er þeim ætlað að koma í stað persónuupplýsingatilskipunar 95/46/EB og rammaákvörðunar um upplýsingavinnslu við refsivörslu nr. 2008/977/JHA. Tilskipuninni um meðferð persónuupplýsinga í refsivörslukerfinu er ætlað að gilda bæði um vinnslu persónuupplýsinga innan aðildarríkjanna og um vinnslu persónuupplýsinga milli ríkja en ekki verður fjallað nánar um hana í þessari ritgerð.[12]

2.2 Tilgangur og helstu nýmæli nýrrar reglugerðar

Af ræðum og fréttatilkynningum Viviane Reding, varaforseta framkvæmdastjórnar Evrópusambandsins og dómsmálastjóra ESB, má ráða að framkvæmdastjórnin telji endurskoðun persónuverndarlöggjafar nauðsynlegan grundvöll þess að almenningur

[8] Viviane Reding, „A data protection compact for Europe“ (*European Union*, 28. janúar 2014) <http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm> skoðað 16. apríl 2014.
[9] Viviane Reding, „Making the EU Data Protection Reform irreversible“ (European Union, 11. mars 2014) <http://europa.eu/rapid/press-release_SPEECH-14-208_en.htm> skoðað 16. apríl 2014.
[10] Reglugerðardrög framkvæmdastjórnarinnar (n. 6).
[11] Commission, „Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data“ COM (2012)10 final.
[12] Sama heimild.

endurheimti traust til netviðskipta og netsamskipta og þess að tryggja öryggi persónuupplýsinga í því mikla flæði upplýsinga sem streymir milli Evrópu og Bandaríkjanna á degi hverjum.[13] Samkvæmt Reding er tilgangur endurskoðunar á persónuverndarlöggjöf ESB eftirfarandi:

2.2.1 Einsleitni á EES svæðinu

Löggjöf verður samræmd í öllum aðildarríkjum með reglugerð; einu samræmdu regluverki um persónuvernd sem gildir í öllum aðildarríkjum Evrópusambandsins og á EES svæðinu. Þetta þótti betri leið en að binda reglur í tilskipun, sem yrði útfærð með mismunandi hætti í löggjöf hvers aðildarríkis.[14]

2.2.2 Aukinn sjálfsákvörðunarréttur hins skráða, sérstaklega á netinu

Í reglugerðardrögunum er sérstakt ákvæði um **réttinn til að gleymast og til afmáunar** (e. right to be forgotten and to erasure), sem er sérstakt viðfangsefni þessarar ritgerðar.[15] Ítarlega verður fjallað um réttinn til að gleymast og til afmáunar í fjórða kafla.

Þá verður aðgengi fólks að eigin persónuupplýsingum einnig auðveldað með þeim hætti að einstaklingar öðlast sérstakan rétt til að flytja gögn milli ábyrgðaraðila (e. right to data portability). Þetta á við um gögn sem varðveitt eru hjá tilteknum ábyrgðaraðila, á grundvelli samþykkis eða samnings, og verður fólki gert kleift að afhenda gögnin öðrum ábyrgðaraðila. Gögnunum skal þá að meginreglu eytt hjá þeim sem upphaflega varðveitti þau. Þetta telur varaforseti framkvæmdastjórnar ESB að muni bæði auka rétt einstaklinga og einnig efla samkeppni meðal netþjónustufyrirtækja.[16]

Einnig er kveðið á um það í reglugerðardrögunum að hvar sem samþykki hins skráða fyrir vinnslu persónuupplýsinga sé skilyrði, verði samþykkið að vera skýrt og upplýst og hafa verið gefið sérstaklega. Ekki er nóg að ætla megi að samþykki hafi verið fengið.[17]

2.2.3 Aukið gegnsæi og ábyrgð þeirra sem vinna með persónuupplýsingar

Tilkynningaskylda, samkvæmt gildandi tilskipun, verður afnumin, þ.e. skylda þeirra sem vinna með persónuupplýsingar til að tilkynna það persónuverndarstofnun í viðkomandi aðildarríki. En þess í stað kemur inn skylda ábyrgðaraðila til að tilkynna um alvarleg

[13] Reding (n. 8).
[14] „Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses" (*European Union*, 25. janúar 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> skoðað 10. mars 2014.
[15] Reglugerðardrög framkvæmdastjórnarinnar (n. 6), 17. gr.
[16] Reding (n. 8).
[17] Sama heimild.

öryggisbrot til persónuverndarstofnana, eins fljótt og hægt er, helst innan 24 klukkustunda eftir að öryggisbrot á sér stað. Þá á einnig að tilkynna öryggisbrot til þeirra einstaklinga sem upplýsingarnar varða.[18]

2.2.4 Styrking persónuverndarstofnana í hverju landi

Loks er nýrri persónuverndarlöggjöf ætlað að efla burði persónuverndarstofnana til eftirlits og eftirfylgni og stórauka samvinnu þeirra á milli. Auk þess fær ESB tiltekið vald til að hlutast til um ákvarðanir þeirra. Persónuverndarstofnanir fá heimildir til að sekta fyrirtæki sem brjóta gegn persónuverndarlöggjöfinni en slíkar heimildir eru ekki til staðar í öllum löndum, auk þess sem algengt er að sektarheimildir nemi lágum fjárhæðum og skipti því ekki sköpum fyrir þau fyrirtæki sem fá þær. Samkvæmt reglugerðardrögum framkvæmdastjórnarinnar geta sektir hins vegar numið allt að einni milljón evra eða 2% af ársveltu fyrirtækja á heimsvísu. Í mars 2014 samþykkti Evrópuþingið að sektir yrðu hækkaðar í allt að 100 milljónir evra eða allt að 5% af ársveltu þegar um fyrirtæki er að ræða.[19]

2.2.5 Ein stofnun fer með mál

Kveðið er á um það í reglugerðardrögunum að fyrirtæki og stofnanir þurfi aðeins að eiga samskipti við eina eftirlitsstofnun, í því aðildarríki ESB þar sem þær hafa aðalstarfsstöð. Þetta hefur verið kallað *one stop shop principle* á ensku. Með sama hætti geti einstaklingar snúið sér með kvartanir til persónuverndarstofnunar í sínu heimalandi, jafnvel þótt unnið sé með persónuupplýsingar þeirra hjá fyrirtæki sem er með starfsstöð utan ESB.[20]

2.2.6 Vinnsla upplýsinga utan EES svæðisins

Þá taka reglugerðardrögin til mun *víðara landfræðilegs gildissviðs* en tilskipun 95/46/EB. Núgildandi persónuupplýsingatilskipun 95/46/EB tekur til vinnslu persónuupplýsinga sem fer fram á vegum aðila með staðfestu í einhverju aðildarríkja ESB en samkvæmt reglugerðardrögunum fellur vinnsla persónuupplýsinga einnig undir löggjöfina þegar hún hefur það að markmiði að bjóða einstaklingum í aðildarríkjunum vöru eða þjónustu, óháð því hvar viðkomandi þjónustuaðili hefur staðfestu. Hið sama á við ef tilgangurinn með

[18] Sama heimild.
[19] „Legislative Observatory 2012/0011(COD) - Text adopted by Parliament, 1st reading/single reading“ (*European Parliament*, 12. mars 2014) <www.europarl.europa.eu/oeil/popups/summary.do?id=1342337&t=d&l=en> skoðað 20. apríl 2014.
[20] Reding (n. 8); European Union (n. 14).

upplýsingavinnslunni er að vakta hegðun einstaklinga í umræddum ríkjum.[21] Tillaga framkvæmdastjórnarinnar hefur mætt mikilli mótspyrnu bandarískra markaðs- og netþjónustufyrirtækja en einnig í Ráðinu.[22]

2.3 Staða mála í maí 2014

Undanfarin tvö ár hafa drög framkvæmdastjórnar ESB að hinni nýju reglugerð og tilskipun verið til meðferðar hjá þeim stofnunum ESB sem fara sameiginlega með lagasetningarvald: Evrópuþinginu og Ráðinu.

2.3.1 Evrópuþingið

Þann 12. mars 2014 samþykkti Evrópuþingið reglugerðardrögin fyrir sitt leyti. Áður, eða þann 21. október 2013, hafði yfirgnæfandi meirihluti LIBE-þingnefndarinnar (nefnd um borgaraleg réttindi, dóms- og innanríkismál) samþykkt tillögu framkvæmdastjórnarinnar. Tillögurnar höfðu þá sætt nokkrum breytingum í meðförum nefndarinnar, sem settar voru fram í svokallaðri Albrecht-skýrslu.[23] Stærsta breytingin var sú að samþykki fyrir vinnslu persónuupplýsinga yrði að vera gefið sérstaklega en ekki mætti ganga út frá því að samþykki væri fengið.

2.3.2 Ráðið (Ráðherraráðið)

Í Ráðinu koma fagráðherrar frá öllum aðildarríkjum ESB saman. Endurbótatillaga framkvæmdastjórnarinnar hefur verið til umræðu oftar en einu sinni hjá innanríkis- og dómsmálaráðherrum í Ráðinu. Stuttu eftir að LIBE-nefndin gaf samþykki sitt var tillagan lögð fyrir Ráðið en einungis þrír ráðherrar greiddu henni atkvæði þar. Svo virðist sem ráðherrunum hafi þótt reglugerðardrögin skerða viðskiptafrelsi.[24] Ráðið náði þó samkomulagi um „one stop shop" regluna, það er tillöguna um að fyrirtæki og stofnanir þurfi aðeins að eiga samskipti við eina eftirlitsstofnun, í því aðildarríki ESB þar sem þær hafa aðalstarfsstöð.[25]

---

[21] „Umsögn um drög framkvæmdastjórnar ESB að reglugerð um vernd persónuupplýsinga" (*Persónuvernd*, maí 2013) <www.personuvernd.is/efst-a-baugi/Umsagnir/2013/greinar/nr/1645> skoðað 6. mars 2014.

[22] Christopher Kuner o.fl., „The Proposed EU Data Protection Regulation Two Years Later" Bloomberg BNA, Privacy and Security Law Report (2014) 1 <www.wsgr.com/eudataregulation/pdf/kuner-010614.pdf> skoðað 16. apríl 2014; Schechner, Sam, „Online Privacy Could Spark U.S.-EU Trade Rift" (*The Wall Street Journal*) <http://online.wsj.com/news/articles/SB10001424052702304361604579291041878017398> skoðað 10. mars 2014.

[23] „LIBE Committee vote backs new EU data protection rules" (*European Union*, 22. október 2013) <http://europa.eu/rapid/press-release_MEMO-13-923_en.htm> skoðað 19. mars 2014.

[24] Reding (n. 8).

[25] „Data Protection Day: Full Speed on EU Data Protection Reform",<http://europa.eu/rapid/press-release_MEMO-14-60_en.htm (*European Union*, 27. janúar 2014) http://europa.eu/rapid/press-release_MEMO-14-60_en.htm> skoðað 16. apríl 2014

Frumvarp framkvæmdastjórnarinnar var rætt aftur á fundi dómsmálaráðherra í Ráðinu í desember 2013[26] og á tveggja daga fundi dóms- og innanríkisráðherra í Aþenu 23.-24. janúar 2014. Nokkur ríki vildu draga úr vægi nýju reglnanna með því að breyta formi þeirra úr reglugerð í tilskipun. Kosið verður um frumvarpið í Ráðinu í júní 2014.[27]

2.3.3 Evrópska ráðið

Leiðtogar aðildarríkja ESB komu sér saman um að ljúka endurskoðun persónuverndarlöggjafarinnar „fljótlega“ á fundi ráðsins 24.-25. október 2013, þar sem sjónum var beint að rafrænu hagkerfi, nýsköpun og þjónustu.[28]

2.3.4 Næstu skref

Grikkir fara með forystu í Ráðherraráði ESB til 1. júlí 2014 en að því búnu taka Ítalir við. Grikkir hafa lagt áherslu á að samþykki nýju persónuverndarlöggjafarinnar verði fengið fyrir 1. júlí en kosningar í Ráðinu fara fram í júní 2014. Verði frumvarpið samþykkt af Ráðinu er gert ráð fyrir að reglugerðin geti tekið gildi í lok árs 2014 eða á árinu 2015.[29]

2.4 Uppljóstranir Edwards Snowden og áhrif þeirra á framvindu mála

Umræðan um endurskoðun persónuverndarlöggjafar ESB tók nýja stefnu árið 2013. Það ár bárust fyrstu fréttir í fjölmiðlum af PRISM, gagnagreiningarkerfi bandarískra stjórnvalda, fyrir tilstilli bandaríska uppljóstrarans Edwards Snowden, sem starfaði áður hjá Þjóðaröryggisstofnun Bandaríkjanna, NSA. Upplýst var að NSA og Alríkislögreglan, FBI, hefðu um langt skeið safnað persónuupplýsingum um fólk og samkeyrt þær, þ. á m. upplýsingar frá símafyrirtækjum og netveitum; Microsoft, Google, Facebook, Skype og YouTube. Þá var upplýst að bandaríska leyniþjónustan hefði um nokkurt skeið hlerað síma helstu þjóðarleiðtoga í Evrópu. Í desember 2013 kom svo upp úr kafinu, einnig fyrir tilstilli Edwards Snowden og fjölmiðla, að Bandaríkjamenn söfnuðu upplýsingum um

[26] Viviane Reding, „Justice Council: We need a simple solution for citizens and business on data protection“ (*European Union*, desember 2013) <http://europa.eu/rapid/press-release_SPEECH-13-1029_en.htm> skoðað 19. mars 2014.
[27] „Progress on EU data protection reform now irreversible following European Parliament vote“ (*European Union*, 12. mars 2014) <http://europa.eu/rapid/press-release_MEMO-14-186_en.htm> skoðað 29. apríl 2014
[28] General Secretariat of the Council, „Conclusions“ (European Council október 2013) EUCO 169/13 <www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf> skoðað 19. mars 2014.
[29] European Union (n. 26).

kreditkortagreiðslur í ríkjum innan ESB, hjá fyrirtækjum eins og VISA og greiðslumiðlunarfyrirtækinu Swift.[30]

Viðbrögð framkvæmdastjórnarinnar og Evrópuþingsins voru á einn veg. Í ræðu 28. janúar 2014 benti Viviane Reding á að eftirlit bandaríska ríkisins með nethegðun fólks og söfnun fyrirtækja á persónuupplýsingum, í markaðslegum tilgangi, væru nátengd fyrirbæri. Í báðum tilfellum væri gengið nærri eða brotið á friðhelgi einkalífs, sem hefði meðal annars þau áhrif að traust almennings til netnotkunar minnkaði.[31]

Þann 12. mars 2014 sendi Evrópuþingið frá sér ályktun, þar sem þingið fordæmdi njósnir Bandaríkjanna í gegnum gagnagreiningarkerfi og kallaði eftir tafarlausri afturköllun Safe Harbour samningsins[32] við Bandaríkin þar til samningurinn hefði verið endurskoðaður, allar glufur í honum lagfærðar og tryggt að flutningur upplýsinga í markaðslegum tilgangi til Bandaríkjanna væri í samræmi við ströngustu kröfur Evrópusambandsins.[33]

Erfitt er að fullyrða á þessari stundu hvort og hvaða áhrif uppljóstranir Edwards Snowden geti haft á örlög reglugerðardraga framkvæmdastjórnarinnar. Ekki er þó ólíklegt að þær hafi gefið þeim byr undir báða vængi sem telja þörf fyrir strangari persónuverndarreglur í Evrópu og hafi, að einhverju leyti, stuðlað að þeim breytingum sem Evrópuþingið gerði á reglugerðardrögunum og samþykktar voru í mars 2014. Vantraust almennings og evrópskra embættismanna í garð bandarískra stjórnvalda gæti einnig orðið til þess að auka stuðning við tillögur framkvæmdastjórnarinnar og flýta fyrir því að hin nýja reglugerð verði samþykkt.

[30] „SPIEGEL Exclusive: NSA Spies on International Bank Transactions“ *Spiegel Online* (15. september 2013) <www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html> skoðað 10. mars 2014.

[31] Reding (n. 8).

[32] Flutningur persónuupplýsinga til þriðju landa, sem ekki veita fullnægjandi vernd persónuupplýsinga, er bannaður Frá þessu eru þó undantekningar, m.a. svokallaðar *Safe Harbour* reglur, sem byggja á ákvörðun framkvæmdastjórnarinnar, frá 26. júlí 2000, sbr. 2. gr. auglýsingar Persónuverndar nr. 288/2010. Samkvæmt reglunum er fyrirtækjum í Bandaríkjunum heimilt að flytja persónuupplýsingar um evrópska borgara til Bandaríkjanna, að því gefnu að veitt sé fullnægjandi vernd í „öruggum höfnum en öruggar hafnir eru fyrirtæki sem undirgangast þar að lútandi reglur bandaríska viðskiptaráðuneytisins.

[33] „US NSA: stop mass surveillance now or face consequences, MEPs say“ (*European Parliament*, 12. mars 2014) <www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203> skoðað 21. apríl 2014.

3 Lagaumgjörð og almenn hugtök

3.1 Meginreglur í persónuupplýsingalöggjöf

Persónuupplýsingaréttur er réttarsvið þar sem umfjöllunarefnið er reglur um heimild til vinnslu og meðferðar persónuupplýsinga og um sjálfsákvörðunarrétt einstaklinga gagnvart eigin persónuupplýsingum. Löggjöf um vernd persónuupplýsinga, þar á meðal vernd rafrænna persónuupplýsinga, er tiltölulega ný viðbót við lagasöfn í Evrópu og annars staðar í heiminum. Hugtakinu persónuupplýsingalöggjöf má í stuttu máli lýsa sem löggjöf er hefur það að markmiði að koma sérstökum reglum yfir vinnslu ákveðinna upplýsinga. Lögin taka með beinum hætti á þeim aðferðum sem beitt er til að safna upplýsingum, skrá upplýsingar, vista þær, nota þær og eyða þeim. Lögin taka yfirleitt aðeins til persónuupplýsinga.[34] Helsti tilgangur og markmið slíkrar löggjafar er að stuðla að því að með persónuupplýsingar sé farið í samræmi við grundvallarsjónarmið og reglur um persónuvernd og friðhelgi einkalífs og að tryggja áreiðanleika og gæði slíkra upplýsinga, sbr. 1. mgr. 1. gr. laga nr. 77/2000.

Inntak persónuupplýsingalöggjafar kristallast í eftirfarandi meginreglum, sem segja má að séu leiðarstef í allri persónuupplýsingalöggjöf. [35] Margar þeirra er að finna í 7. gr. persónuverndarlaga, sem byggð er á 6. gr. tilskipunar 95/46/EB, en þessi ákvæði innihalda grundvallarkröfur um hvernig vinna má með persónupplýsingar.

1. *Sanngirnisreglan*: Persónuupplýsingar skal vinna með sanngjörnum, málefnalegum og lögmætum hætti og í samræmi við vandaða vinnsluhætti persónuupplýsinga.[36]

2. *Magnreglan/Meðalhófsreglan*: Magn persónuupplýsinga sem unnið er með skal ekki vera umfram það sem nauðsynlegt er til að ná þeim markmiðum sem stefnt er að með söfnun og/eða frekari vinnslu þeirra.[37]

3. *Tilgangsreglan*: Persónuupplýsingar skulu fengnar í yfirlýstum, skýrum og málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi. Í persónuverndarlögum og tilskipun 95/46/EB er jafnframt tekið fram að frekari vinnsla í sagnfræðilegum, tölfræðilegum eða vísindalegum tilgangi teljist ekki ósamrýmanleg tilganginum með öflun upplýsinganna, að því tilskildu að viðeigandi öryggis sé gætt.[38]

---

[34] L.A. Bygrave, Data protection law: approaching its rationale, logic, and limits (Kluwer Law International 2002) Kindle útgáfa, 3%.
[35] Sama heimild.
[36] 1. tölul. 1. mgr. 7. gr. pul.; tilskipun 95/46/EB (n. 7), a-liður 1. mgr. 6. gr.
[37] 3. tölul. 1. mgr. 7. gr. pul.; tilskipun 95/46/EB (n. 7), c-liður 1. mgr. 6. gr.
[38] 2. tölul. 1. mgr. 7. gr. pul.; tilskipun 95/46/EB (n. 7), b-liður 1. mgr. 6. gr.

4. *Samþykkis-/lögmætisregla.* Vinnsla og miðlun persónuupplýsinga í öðrum tilgangi er aðeins heimil ef hinn skráði hefur gefið samþykki sitt eða samkvæmt heimild í lögum.[39]
5. *Áreiðanleikareglan*: Persónuupplýsingar skulu vera viðeigandi, nákvæmar og fullnægjandi miðað við markmiðin sem réttlæta söfnun og/eða vinnslu þeirra.[40]
6. *Upplýsingaöryggi*: Grípa skal til viðeigandi öryggisráðstafana til að tryggja vernd persónuupplýsinga, svo þær verði ekki birtar, þeim eytt eða breytt án leyfis eða fyrir slysni.[41]
7. *Upplýsingaréttur og réttur hins skráða til aðgangs:* Upplýsa á hinn skráða og veita honum aðgang að þeim upplýsingum sem rekja má til hans og eru í vörslu annarra, svo hann eigi þess kost að uppfæra upplýsingarnar, séu þær ónákvæmar eða gefi ranga mynd að öðru leyti.[42]
8. *Persónugreiningarreglan.* Varðveita skal persónuupplýsingar í því formi að ekki sé unnt að bera kennsl á skráða aðila lengur en þörf krefur, miðað við tilgang vinnslu.[43]
9. Ábyrgðaraðila ber skylda til að tryggja að framangreindar reglur séu uppfylltar.[44]
Framangreindar meginreglur má finna í ýmsum útgáfum, bæði í persónuupplýsingalöggjöf og öðrum tegundum regluverks. Hins vegar teljast aðeins þær réttarheimildir, sem innihalda allar eða flestar meginreglurnar, til eiginlegrar persónuupplýsingalöggjafar.

3.2 Almenn lög

Um persónuupplýsingarétt er fjallað í lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga (hér eftir persónuverndarlög eða pul.). Lögin byggja á tilskipun Evrópuþingsins og Ráðsins nr. 95/46/EB, [45] sem hér verður einnig kölluð persónuupplýsingatilskipunin.
Þá gilda lög nr. 81/2003 um fjarskipti, fjarskiptaþjónustu og fjarskiptanet, þar með talið tal- og farsímanet, en með þeim voru innleiddar nokkrar Evróputilskipanir á sviði fjarskiptamála, þ. á m. tilskipun 2002/58/EB um vinnslu persónuupplýsinga og verndun einkalífs á sviði rafrænna fjarskipta (tilskipun um friðhelgi einkalífsins og rafræn fjarskipti). Um rafræn viðskipti og aðra rafræna þjónustu gilda lög nr. 30/2002. Með lögunum var innleidd tilskipun 2000/31/EB frá 8. júní 2000 sem kölluð hefur verið E-Commerce Directive (Electronic Commerce Directive) á ensku. Sérstaka umfjöllun um tilskipun 2000/31, sbr. lög nr. 30/2002,

[39] 1. og 3. tölul. 1. mgr. 8. gr. pul.; tilskipun 95/46/EB (n. 7), a- og b-liður 1. mgr. 7. gr.
[40] 4. tölul. 1. mgr. 7. gr. pul.; tilskipun 95/46/EB (n. 7), d-liður 1. mgr. 6. gr.
[41] 11. gr. pul.; tilskipun 95/46/EB (n. 7), 17. gr.
[42] 16. gr.,18. gr. og 25. gr. pul.; tilskipun 95/46/EB (n. 7), 12. gr.
[43] 5. tölul. 1. mgr. 7. gr. pul.; tilskipun 95/46/EB (n. 7), e-liður 1. mgr. 6. gr.
[44] 2. mgr. 7. gr. pul.; tilskipun 95/46/EB (n. 7), 2. mgr. 6. gr.
[45] Tilskipun 95/46/EB (n. 7).

er að finna í kafla 4.10. Um aðra almenna löggjöf, sem þýðingu hefur fyrir meðferð persónuupplýsinga, verður ekki fjallað hér.

Í ljósi þess að viðfangsefni þessarar ritgerðar telst til persónuupplýsingaréttar þykir rétt að hefja hana á stuttu yfirliti yfir grundvallarhugtök þess réttarsviðs og þær tillögur að breytingum á skilgreiningu þeirra, sem fram hafa komið í drögum framkvæmdastjórnarinnar og í meðförum Evrópuþingsins.

3.3 Friðhelgi einkalífs og vernd persónuupplýsinga

Vernd persónuupplýsinga þróaðist út frá réttinum til friðhelgi einkalífs og er hluti af þeim rétti. Friðhelgi einkalífs er víðara hugtak en vernd persónuupplýsinga en bæði hugtök fela í sér réttindi tengd einstaklingum.[46]

Björg Thorarensen hefur lýst hugtakinu friðhelgi einkalífs með þessum orðum:

> Kjarni hugtaksins felst í því að hver maður hefur rétt til þess að ráða yfir lífi sínu og líkama og til að njóta friðar um lífshætti sína og einkahagi, svo og að tilfinningalíf hans, samskipti og tilfinningasambönd við aðra skuli njóta sérstakrar verndar fyrir afskiptum hvort heldur annarra einstaklinga eða stjórnvalda.[47]

Mannréttindadómstóll Evrópu (hér eftir MDE) hefur túlkað friðhelgi einkalífs þannig að vernd persónuupplýsinga falli þar undir. Þetta var meðal annars staðfest í máli *Leander gegn Svíþjóð*, árið 1987, þar sem MDE úrskurðaði að leynileg söfnun og skráning persónulegra upplýsinga um einstakling hjá lögreglu, og synjun á aðgangi hans að slíkum upplýsingum, fæli í sér takmörkun á friðhelgi einkalífs.[48]

MDE komst að sömu niðurstöðu í máli *Copland gegn Bretlandi*[49] árið 2007 þar sem staðfest var að varðveisla upplýsinga um símtöl, tölvupóstsamskipti og netnotkun á vinnustað væri skerðing á friðhelgi einkalífs, sbr. 8. gr. Mannréttindasáttmála Evrópu (hér eftir MSE), þótt upplýsingarnar væru ekki notaðar gegn viðkomandi.

Af dómaframkvæmd MDE má því ráða að rétturinn til friðhelgi einkalífs felur meðal annars í sér rétt hvers einstaklings til að hafa ráðstöfunarrétt yfir upplýsingum sem varða hann sjálfan. Þessi réttur telst til borgaralegra og stjórnmálalegra rétttinda.

Rétturinn til friðhelgi einkalífs er verndaður af 71. gr. íslensku stjórnarskrárinnar (hér eftir stjskr.), 8. gr. Mannréttindasáttmála Evrópu, 17. gr. Alþjóðasamnings um borgaraleg og

[46] Sjá m.a. *Leander g. Svíþjóð* (1987) Series A. 116, mgr. 48.
[47] Björg Thorarensen, *Stjórnskipunarréttur: mannréttindi* (Bókaútgáfan Codex 2008) 288.
[48] *Leander g. Svíþjóð* (n. 46).
[49] *Copland g. Bretlandi* ECHR App no. 62617/00 (ECtHR, 3. apríl 2007).

stjórnmálaleg réttindi og 7. gr. Sáttmála Evrópusambandsins um grundvallarréttindi (hér eftir Réttindaskrá ESB). Réttindaskrá ESB hefur einnig að geyma sérstakt ákvæði um vernd persónuupplýsinga í 8. gr. Rétturinn til friðhelgi einkalífs, til verndar röskun annarra og þá sérstaklega ríkisins, hlaut fyrst alþjóðlega viðurkenningu með 12. grein Mannréttindayfirlýsingar Sameinuðu þjóðanna árið 1948[50] en hún hafði meðal annars mikil áhrif á mannréttindasáttmála í Evrópu.[51]

3.4 Lagaleg staða persónuupplýsingaverndar í Evrópu

Í Evrópu telst vernd persónuupplýsinga til grundvallarmannréttinda. Þetta hefur meðal annars verið staðfest í tímamótadómi þýska stjórnskipunardómstólsins (Bundesverfassungsgericht) frá 1983[52] þar sem fram kom að sjálfsákvörðunarréttur einstaklinga yfir upplýsingum sem þá varða væri grundvallarmannréttindi (*þ. Grundrecht auf informationelle Selbstbestimmung*.) Staða persónuupplýsingaverndar sem grundvallarmannréttinda var jafnframt staðfest af Dómstól Evrópusambandsins (Evrópudómstólnum) í máli *Rechnungshof* gegn austurríska ríkisútvarpinu 2003[53] og er viðurkennd í mörgum mannréttindasáttmálum sem þýðingu hafa í Evrópu, meðal annars í Réttindaskrá ESB frá árinu 2000, þar sem sérstakt ákvæði um vernd persónuupplýsinga er að finna í 8. grein. Réttindin sem talin eru upp í Réttindaskránni beinast að Evrópusambandinu og stofnunum þess en ekki að aðildarríkjunum, nema þegar þau framfylgja skuldbindingum á grundvelli Evrópusamstarfsins. Ákvæði 8. gr. endurspeglar engu að síður að vernd persónuupplýsinga er á meðal þeirra réttinda sem Evrópusambandsþjóðirnar telja á meðal mikilvægustu mannréttinda borgaranna.[54]

[50] Universal Declaration of Human Rights (10. desember 1948) UNGA Res 217 A(III) (UDHR), 12. gr. Þar segir að eigi megi eftir geðþótta raska heimilisfriði nokkurs manns, hnýsast í einkamál hans eða bréf, vanvirða hann eða spilla mannorði hans. Beri hverjum manni lagavernd gagnvart slíkum afskiptum eða árásum.

[51] European Union Agency for fundamental rights og Council of Europe, *Handbook on European Data Protection Law* (Publications Office of the European Union, Lúxemborg 2014) 61 <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law_en.pdf> skoðað 26. febrúar 2014

[52] BVerfGE 65, 1.

[53] Mál C-465/00, C-138/01 og C-139/01 *Rechnungshof g. Österreichischer Rundfunk and Others* [2003] ECR I-4989.

[54] Charter of Fundamental Rights of the European Union (Sáttmáli Evrópusambandsins um grundvallarréttindi), (2000) OJ C364/01; Páll Þórhallsson, „Andlitslyfting Evrópusambandsins“ (*mbl.is*, 11. febrúar 2001) <http://www.mbl.is/greinasafn/grein/588574/> skoðað 11. febrúar 2014.

8.gr.

Vernd persónuupplýsinga

1. Sérhver maður á rétt til verndar eigin persónuupplýsinga.

2. Vinna skal úr slíkum upplýsingum með sanngjörnum hætti, í yfirlýstum tilgangi og með samþykki hlutaðeigandi eða á einhverjum öðrum réttmætum grundvelli sem mælt er fyrir um í lögum. Sérhver maður á rétt til aðgangs að upplýsingum sem teknar hafa verið saman um hann og rétt á að fá þær leiðréttar.

3. Óháð yfirvald skal hafa eftirlit með því að þessum reglum sé fylgt.[55]

Með 6. gr. Lissabonsáttmálans frá 1. desember 2009 var Mannréttindayfirlýsing ESB gerð að fullgildum hluta ESB-réttar.[56] Þar með fékk hún sömu réttarheimildarlegu stöðu og stofnsáttmálarnir sem ESB byggir á.[57] Sú breyting og tengdar breytingar á réttarheimildarlegri stöðu annarra réttarreglna ESB hafa enn frekar styrkt stöðu persónuupplýsingaverndar sem grundvallarmannréttinda í ESB-rétti,

Í 16. gr. sáttmála um starfshætti Evrópusambandsins (áður 286. gr. stofnsáttmála Evrópubandalagsins) er jafnframt að finna ákvæði um að allir eigi rétt á að persónuupplýsingar um þá njóti verndar. Vernd persónuupplýsinga sem grundvallarmannréttinda er þar að auki stjórnarskrárvarin í nokkrum Evrópuríkjum.[58]

[55] Charter of Fundamental Rights of The European Union (n. 54).

[56] Sigurður Líndal og Skúli Magnússon, *Réttarkerfi Evrópusambandsins og Evrópska efnahagssvæðisins: megindrættir* (Hið íslenska bókmenntafélag 2011) 31.

[57] Sama heimild, 86.

[58] Christopher Kuner, *European data protection law: corporate compliance and regulation* (2. útg., Oxford University Press 2007) 49; 22. gr. belgísku stjskr. frá 7. febrúar 1831,15. gr. kýpversku stjskr. frá 16. ágúst 1960, 12. gr. frönsku stjskr. frá 26. ágúst 1789, 26. gr. portúgölsku stjskr. frá 2. apríl 1976, 18. gr. spænsku stjskr. frá 27. desember 1978 og 2. gr. sænsku stjskr. frá 1. janúar 1975.

3.5 Almenn hugtök

3.5.1 Persónuupplýsingar

Hugtakið *persónuupplýsingar* er kjarni og meginviðfangsefni persónuupplýsingaréttarins. Almennt eru persónuupplýsingar skilgreindar sem hvers kyns persónugreindar eða persónugreinanlegar upplýsingar, sem beint eða óbeint má rekja til tiltekins einstaklings („hins skráða"), óháð aðferð við vinnslu, formi eða tilgangi. Sem dæmi um persónuupplýsingar má nefna nafn, símanúmer, netfang, fæðingarstað, fæðingardag, myndir, myndbönd og IP-tölur.[59] Persónuupplýsingar geta verið á rafrænu formi eða á pappír, skrifleg eða munnleg samskipti og jafnvel lífsýni.[60] Einungis upplýsingar sem tengjast einstaklingum, en ekki lögaðilum, teljast persónuupplýsingar.

Nokkur munur er á skilgreiningu hugtaksins í íslensku persónuverndarlögunum og tilskipun 95/46/EB að því leyti að íslensku lögin taka til upplýsinga um lifandi og látna einstaklinga en tilskipun 95/46/EB tekur einungis til upplýsinga um lifandi menn.[61]

3.5.1.1 Persónugreindar og persónugreinanlegar upplýsingar

Gerður er greinarmunur á *persónugreindum* og *persónugreinanlegum upplýsingum* en báðar tegundir upplýsinga falla undir gildissvið laganna. Persónugreindar upplýsingar eru merktar með nafni eða auðkenni hins skráða og þær má rekja beint til hins skráða. Persónugreinanlegar upplýsingar er líka unnt að rekja til hins skráða en óbeint. Dulkóðaðar persónuupplýsingar sem hægt er að afkóða teljast því persónuupplýsingar í skilningi laganna. Upplýsingar sem ekki er hægt að rekja til nafngreinds einstaklings með neinum hætti teljast hins vegar ekki til persónuupplýsinga og falla þar með ekki undir gildissvið persónuverndarlaganna eða tilskipunar 95/46/EB.

3.5.1.2 Viðkvæmar persónuupplýsingar

Bæði í lögum nr. 77/2000 og tilskipun 95/46/EB er greint á milli *viðkvæmra persónuupplýsinga* og annarra persónuupplýsinga.

---

[59] Í máli C-101/01 *Lindqvist* [2003] ECR I-12971 taldi Evrópudómstóllinn upplýsingar um nöfn samstarfsmanna, símanúmer og áhugamál, sem L hafði fært á heimasíðu sína, falla undir tilskipun 95/46/EB þar sem um væri að ræða persónuupplýsingar sem unnið væri með á rafrænan hátt.

[60] European Union Agency for fundamental rights (n. 51) 43.

[61] 1. tölul. 1. mgr. 2. gr. pul.; „Opinion 4/2007 on the concept of personal data" (Article 29 Data Protection Working Party, jún 2007)
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> skoðað 14. mars 2014.

Viðkvæmar persónuupplýsingar eru meðal annars upplýsingar um uppruna, litarhátt, trúarskoðanir, kynhegðun, heilsuhagi og fyrri afbrot. Um þær gilda strangari reglur en um aðrar persónuupplýsingar. Tilskipun 95/46/EB byggir á þeirri meginreglu að vinnsla ákveðinna tegunda viðkvæmra persónuupplýsinga sé bönnuð, en veitir eigi að síður svigrúm til þess að víkja frá meginreglunni í mörgum tilvikum. Þannig er til dæmis heimilt að vinna með viðkvæmar persónuupplýsingar ef sá aðili sem upplýsingarnar varðar samþykkir vinnsluna og eins geta aðildarríkin heimilað frávik frá meginreglunni ef slíkt er nauðynlegt með tilliti til almannahagsmuna.

3.5.2 Vinnsla og skrá persónuupplýsinga

Hugtakið *vinnsla* merkir sérhverja aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn.[62] Samkvæmt 1. mgr. 3. gr. persónuverndarlaga gilda þau um sérhverja rafræna vinnslu persónuupplýsinga og einnig um handvirka vinnslu persónuupplýsinga, sem eru eða eiga að verða hluti af skrá. Í máli C-101/01 (Bodil Lindqvist)[63] taldi ESB-dómstóllinn það til dæmis til rafrænnar vinnslu persónuupplýsinga þegar einstaklingur birti persónuupplýsingar um aðra á heimasíðum sínum; nöfn samstarfsmanna, símaúmer og áhugamál.

Hugtakið *skrá* er í persónuverndarlögum skilgreint sem sérhvert skipulagsbundið safn persónuupplýsinga þar sem finna má upplýsingar um einstaka menn. Út frá 1. mgr. 3. gr. pul. má gagnálykta að lögin gildi ekki um *handvirka* vinnslu persónuupplýsinga sem er ekki eða á ekki að verða hluti af skrá.

3.5.3 Ábyrgðaraðilar og vinnsluaðilar

Ábyrgðaraðili er sá sem ákveður tilgang vinnslu persónuupplýsinga, þann búnað sem notaður er, aðferð við vinnsluna og aðra ráðstöfun upplýsinganna. Ábyrgðaraðila, sem safnar persónuupplýsingum, ber skylda til þess að veita hinum skráða að eigin frumkvæði ákveðna vitneskju. Er hér um að ræða viðbótarrétt hins skráða, þ.e. til viðbótar rétti hans til aðgangs að upplýsingum um sjálfan sig. Beiðni um eyðingu persónuupplýsinga ætti að beina til ábyrgðaraðila, það er þess aðila sem ákvað að unnið yrði með upplýsingarnar. Í athugasemdum með frumvarpi því sem varð að lögum nr. 77/2000 segir að þegar ágreiningur verður milli hins skráða og ábyrgðaraðila um hvort

[62] 2. tölul. 1. mgr. 2. gr. pul.
[63] C-101/01 *Lindqvist* (n. 59).

grundvöllur sé fyrir eyðingu upplýsinga eða banni við notkun þeirra sé það hlutverk Persónuverndar að skera úr þeim ágreiningi.[64]

Hvað varðar hlutverk *einstaklinga sem ábyrgðaraðila* segir í persónuverndarlögum að þau gildi ekki um meðferð einstaklings á persónuupplýsingum sem eingöngu varða einkahagi hans eða eru einvörðungu ætlaðar til persónulegra nota.[65] Samkvæmt lögunum geta einstaklingar í slíkum tilfellum ekki talist ábyrgðaraðilar. Hins vegar kom fram í fyrrnefndu Lindqvist-máli að það teljist til rafrænnar vinnslu persónuupplýsinga þegar einstaklingar birta persónuupplýsingar um aðra á heimasíðum sínum á Netinu og að undantekningar frá gildissviði laganna, vegna vinnslu upplýsinga til persónulegra nota, eigi þá ekki við.[66]

Sameiginleg ábyrgð er þegar tveir eða fleiri ábyrgðaraðilar ákveða í sameiningu að vinna upplýsingar í sameiginlegum tilgangi. Notandi og eigandi samfélagsmiðils geta sem dæmi borið sameiginlega ábyrgð, líkt og nánar verður fjallað um síðar í ritgerðinni. Sameiginleg ábyrgð þýðir meðal annars að ábyrgðaraðilar eru báðir eða allir ábyrgir fyrir tjóni. Nokkur óvissa er þó um skiptingu sameiginlegrar ábyrgðar í slíkum tilvikum.[67]

Vinnsluaðili er sá sem vinnur persónuupplýsingar á vegum ábyrgðaraðila. Vinnsluaðila er einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila og lög nr. 77/2000. Ábyrgðaraðila ber að kanna hvort vinnsluaðili uppfylli skilyrði 11. og 12. gr. laganna. Ábyrgðar- og vinnsluaðili gera vinnslusamning sín á milli þar sem fram koma fyrirmæli ábyrgðaraðila til vinnsluaðila.

Væri ákvæði í slíkum samningi þess efnis að ábyrgðaraðilinn mætti ekki skipta sér af ákvörðunum vinnsluaðila myndi það líklega jafngilda því að sameiginleg ábyrgð teldist hafa skapast, þar sem báðir aðilar teldust ábyrgðaraðilar.[68] Hið sama ætti við ef vinnsluaðili virti ekki þau takmörk sem ábyrgðaraðili hefði sett honum við vinnslu upplýsinga. Þá teldist vinnsluaðili líkast til vera orðinn ábyrgðaraðili, að minnsta kosti gagnvart þeirri vinnslu sem fól í sér brot gegn fyrirmælum ábyrgðaraðilans.[69]

---

[64] Alþt. 1999-2000, A-deild, þskj. 399 - 280. mál, athugasemdir við 2. mgr. 26. gr.
[65] 2. mgr. 3. gr. pul.
[66] C-101/01 *Lindqvist* (n. 59).
[67] European Union Agency for fundamental rights (n. 51) 52.
[68] Sama heimild, 53-54.
[69] Sama heimild.

3.5.4 Rafræn vöktun

Hugtakinu *rafræn vöktun* er lýst í 6. tl. 1. mgr. 2. gr. pul. en það felur í sér eftirlit með einstaklingum með fjarstýrðum eða sjálfvirkum búnaði, þegar eftirlitið er viðvarandi, endurtekið reglulega og fer fram á almannafæri eða á svæði sem takmarkaður hópur fólks fer um að jafnaði. Hugtakið tekur annars vegar til vöktunar sem leiðir, á að leiða eða getur leitt til vinnslu persónuupplýsinga, og hins vegar til sjónvarpsvöktunar sem fer fram með notkun sjónvarpsmyndavéla, vefmyndavéla eða annars samsvarandi búnaðar, án þess að fram fari söfnun myndefnis eða aðrar aðgerðir sem jafngilda vinnslu persónuupplýsinga.

3.5.5 Samþykki

Hugtakið samþykki er skilgreint svo í 7. tl. 2. gr. pul:

> Sérstök, ótvíræð yfirlýsing sem einstaklingur gefur af fúsum og frjálsum vilja um að hann sé samþykkur vinnslu tiltekinna upplýsinga um sig og að honum sé kunnugt um tilgang hennar, hvernig hún fari fram, hvernig persónuvernd verði tryggð, um að honum sé heimilt að afturkalla samþykki sitt o.s.frv.

Í tilskipun 95/46/EB er hugtakinu lýst í h-lið 2. gr. með orðunum „óþvinguð, sértæk og upplýst viljayfirlýsing skráðs aðila um að hann samþykki vinnslu persónuupplýsinga sem varða hann sjálfan.“

Samkvæmt þessu þurfa eftirfarandi þrjú skilyrði að vera uppfyllt til að samþykki teljist gilt.

1. *Samþykki gefið af fúsum og frjálsum vilja.* Hinn skráði má ekki hafa verið beittur þrýstingi þegar hann gaf samþykki sitt.
2. *Sérstakt samþykki.* Samþykkið verður að beinast að tilgreindri vinnslu upplýsinga.
3. *Upplýst samþykki.* Upplýsa verður hinn skráða um tilgang og afleiðingar þess að veita samþykki sitt.

Tekið er fram í persónuverndarlögum að hinum skráða sé heimilt að afturkalla samþykki sitt. Ekki er minnst á þann rétt í persónuupplýsingatilskipun ESB en engu að síður er almennt talið að hann sé fyrir hendi í Evrópurétti og að hinn skráði þurfi ekki að réttlæta það sérstaklega eða óttast neikvæðar afleiðingar þess að draga samþykki sitt til baka.[70]

[70] European Union Agency for fundamental rights (n. 51) 61.

Í reglugerðardrögum framkvæmdastjórnarinnar er kveðið á um að hvar sem samþykki hins skráða fyrir vinnslu persónuupplýsinga sé skilyrði, verði samþykkið að vera skýrt og upplýst og hafa verið gefið sérstaklega. Ekki er nóg að ætla megi að samþykki hafi verið fengið, heldur verður hinn skráði að gefa samþykki sitt með virkum hætti, t.d. með því að haka í reit á tölvuskjá.[71]

3.5.6 Tilkynningarskylda

Samkvæmt núgildandi tilskipun ESB og íslenskum persónuverndarlögum ber ábyrgðaraðila *skylda til að tilkynna* viðkomandi persónuverndarstofnun um fyrirhugaða vinnslu persónuupplýsinga þegar vinnslan mun fara fram með rafrænum hætti í heild eða að hluta. Hér á landi ber að tilkynna slíkt til Persónuverndar, sbr. 1. mgr. 31. gr. pul. Heimilt er að víkja frá ákvæðum um tilkynningarskyldu, annars vegar þannig að um ákveðnar tegundir vinnslu gildi vægari tilkynningarreglur eða þær séu með öllu undanþegnar tilkynningarskyldunni og hins vegar þannig að um enn aðrar tegundir vinnslu gildi strangari reglur, þ.e. leyfisskylda í stað tilkynningarskyldu. Þessi tilkynningarskylda leggst af, verði drög að nýrri reglugerð ESB samþykkt, en í staðinn kemur skylda ábyrgðaraðila til að tilkynna um alvarleg öryggisbrot.[72]

[71] Reglugerðardrög framkvæmdastjórnarinnar (n. 6) 25. liður inngangsorða.
[72] Tilskipun 95/46/EB (n. 7); lög nr. 77/2000; reglugerðardrög framkvæmdastjórnarinnar (n. 6).

4 Rétturinn til að gleymast

4.1 Hvert er vandamálið?

Rétturinn til að gleymast og til afmáunar í 17. gr. reglugerðardraga framkvæmdastjórnar ESB[73] er á meðal þess sem hefur vakið hvað mesta athygli almennings, embættismanna og fyrirtækja og jafnframt á meðal þess sem vakið hefur hvað stærstar spurningar. En hver er hugmyndafræðin á bak við hann? Af hverju ættu einstaklingar að eiga slíkan rétt?

Gleymska; að atburðir fortíðar falli í gleymsku, er hið sjálfgefna ástand. Okkur er auðvelt og eðlislægt að gleyma. Fyrir tilstilli bókmennta, myndlistar, ljósmynda og kvikmynda hefur okkur reyndar tekist að festa í minni tiltekin atriði úr lífi okkar og sögu mannkyns. En við munum ekki allt. Til dæmis munum við væntanlega ekki hvað við fengum í hádegismat þriðjudaginn 21. maí 1985 eða hverju við klæddumst í vinnunni fimm árum síðar.

Á þetta hefur fræðimaðurinn Victor Mayer-Schönberger, kennari við Oxford háskóla, meðal annars bent en hann hefur haft mikil áhrif á umræðuna um *réttinn til að gleymast*, eins og rétturinn til afmáunar persónuupplýsinga, í 17. gr. reglugerðardraga framkvæmdastjórnarinnar, er oftast kallaður í fræðilegri umfjöllun. Árið 2009 kom út bók hans Delete: The Virtue of Forgetting in the Digital Age, þar sem Mayer-Schönberger bendir á að manninum sé almennt ekki eðlislægt að muna allar upplýsingar úr lífi sínu og leggur til að persónuupplýsingar fái eins konar „síðasta neysludag“, þ.e. að þeim verði eytt af netinu að ákveðnum tíma liðnum.[74]

Mayer-Schönberger bendir einnig á að aðeins örfáir einstaklingar í öllum heiminum geti kallað fram allar minningar úr lífi sínu; einstaklingar sem haldnir séu sjaldgæfu taugafræðilegu ástandi sem kallast *hyperthymesia*. [75] Þetta fólk muni hvern einasta dag í lífi sínu í smáatriðum og minningar líði því stjórnlaust fyrir sjónir við minnsta tilefni. Ástandið sé bölvun, en ekki blessun: Að vera svo ofsóttur af fortíðinni að það aftri manni að njóta líðandi stundar. Þetta sé jafnframt undantekning, því frá örófi alda hafi gleymska verið eðlilegur hluti mannlegrar tilveru. Fullkomið minni ekki. Á stafrænni

[73] Reglugerðardrög framkvæmdastjórnarinnar (n. 6). Íslensk þýðing höfundar.
[74] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2009) 71-73.
[75] Viktor Mayer-Schönberger, „The Right to be Forgotten - Events - IIEA - The Institute of International and European Affairs“ (Dublin, Ireland, október 2011) <http://www.iiea.com/events/the-right-to-be-forgotten?gclid=CIrbrKChkr0CFeXLtAodgHUAHg> skoðað 29. apríl 2014.

upplýsingaöld hafi þetta snúist við. Með örri tækniþróun og framförum í vistun rafrænna gagna sé stafrænt, fullkomið minni orðið hið sjálfgefna ástand. Gleymskan undantekning.[76]

Sem dæmi um afleiðingarnar segir Mayer-Schönberger sögu konu að nafni Stacey Snyder, fyrrum kennaranema við Millersville-kennaraháskólann í Pennsylvaníu í Bandaríkjunum. Þegar Stacey var 25 ára birti hún mynd af sjálfri sér á MySpace-síðu sinni þar sem hún hélt á drykkjarmáli úr plasti og bar sjóræningjahatt á höfði. Undir myndina hafði hún skrifað „drukkinn sjóræningi". Kennara við skólann fannst þetta ámælisvert, þar sem Stacey var æfingakennari við skólann og hafði komið því á framfæri við nemendur að hún notaði MySpace. Kennarinn kvartaði til skólayfirvalda, sem komu í veg fyrir að Stacey fengi að útskrifast. Rökin voru þau að með myndbirtingunni hefði Stacey hvatt ungmenni til áfengisdrykkju og sýnt af sér ófagmannlega framkomu. Stacey reyndi að fá ákvörðun skólayfirvalda hnekkt fyrir dómi með vísan til tjáningarfrelsis en tapaði málinu.[77] Mayer-Schönberger nefnir sögu Staceyar sem dæmi um það hvernig upplýsingar úr fortíð, sem ættu eðli málsins samkvæmt að falla í gleymsku, geti haft neikvæð áhrif á nútíð og framtíð. Bara af því að þær eru geymdar á netinu.

Jafnvel þótt við sjálf munum ekki allt, þá muna aðrir fyrir okkur: Google, Amazon, Facebook og fleiri. Rót þess er meðal annars að rekja til þess að tölvukerfi byggja í auknum mæli á tækni sem kallast tölvuský. Það þýðir að öll persónuleg gögn; tölvupóstar, skrár og skjöl eru geymd á netinu en ekki í tölvunum sjálfum. Eitt fremsta fyrirtækið á þessu sviði er Google, sem býður upp á alls kyns þjónustu, tölvupóst, dagatöl, samskiptasíður og myndvinnsluforrit á netinu. Á móti fær Google að geyma persónuleg gögn á netþjónum sínum - sem þýðir að fyrirtækið hefur undir höndum gríðarlegt magn nákvæmra persónuupplýsinga um almenning og netvenjur hans. Upplýsingar sem hinn almenni borgari gerir sér ekki endilega grein fyrir að verið sé að safna, hvað þá að þær séu greindar, geymdar og áframsendar. Jafnvel þótt facebook-reikningnum sé eytt eru myndir og upplýsingar á facebook geymdar áfram. Jafnvel þótt flugið til Barcelona sé ekki bókað, heldur bara skoðað, eru upplýsingar um netleitina geymdar - og oft líður ekki á löngu þar til auglýsingar um flug og gistingu í Barcelona taka að birtast á tölvuskjánum, eins og fyrir hreina tilviljun.

[76] Mayer-Schönberger (n. 74) 1-2.
[77] *Snyder g. Millersville University, et al.*, 2008 WL 5093140 (E.D. Pa., 2008); Mayer-Schönberger (n. 74).

Að mati Mayer-Schönberger gæti vald ríkis og einkafyrirtækja yfir upplýsingum þróast yfir í vald yfir einstaklingum. Hann líkir þessu við völd kaþólsku kirkjunnar á miðöldum. Kirkjan hafi meðal annars byggt völd sín á þeirri forsendu að hún bjó yfir upplýsingum og þekkingu; bókum og handritum. Upplýsingum sem hjálpuðu fólki til að muna. Þetta hafi skapað valdaójafnvægi sem ekki hafi breyst fyrr en með prenttækninni, þegar almenningur öðlaðist sjálfur greiðari aðgang að upplýsingum.[78]

Á meðal neikvæðra hliða þessarar tækniþróunar er vaxandi óöryggi og efasemdir netnotenda um að friðhelgi einkalífs þeirra og vernd persónuupplýsinga á netinu sé tryggð.[79] Annar galli er að með tilkomu netsins má segja að fólk fái ekki lengur að gleyma, eins og því er eðlislægt að gera. Neikvæðir, sorglegir og vandræðalegir atburðir fortíðar birtast ofarlega í leitarniðurstöðum netsins, í hvert sinn sem nöfn fólks, fyrirtækja eða bæjarfélaga eru slegin þar inn, og færast ekki endilega neðar í netleitinni þótt áratugir hafi liðið frá atburðunum.[80]

Til að leysa þetta vandamál hefur Mayer-Schönberger talað fyrir þeirri hugmynd að einstaklingar eignist rétt til að gleymast á netinu. Hann hefur jafnframt stungið upp á öðrum og mildari leiðum, þar á meðal því að leitarniðurstöðum leitarvéla verði raðað í tímaröð, með þeim hætti að yngstu niðurstöðurnar birtist efst en færist svo neðar með tímanum. Í bók sinni varar hann við því að verði fullkomið, stafrænt minni hið sjálfgefna ástand, sem við reiðum okkur á, geti tæknin fært þeim sem geyma upplýsingarnar of mikið vald í hendur: Vald til að breyta sögunni og vald yfir okkur sjálfum. Mikilvægt sé að almenningur taki valdið aftur í sínar hendur.[81]

4.2 Uppruni og þróun réttarins til að gleymast

Framkvæmdastjórn Evrópusambandsins hefur skilgreint hugtakið réttinn til að gleymast svo: „réttur einstaklinga til að vinnslu persónupplýsinga þeirra verði hætt og að upplýsingunum verði eytt þegar þeirra er ekki þörf af lögmætum ástæðum.“[82] Í grein Meg Leta Ambrose og Jef Ausloos, *The right to be forgotten across the Pond*, er hugtakið rétturinn til að gleymast, sbr. 17. gr. reglugerðardraga framkvæmdastjórnar ESB, skilgreint með eftirfarandi orðum:

[78] Mayer-Schönberger (n. 74) 37-39; Mayer-Schönberger (n. 75).
[79] European Union (n. 23).
[80] *Alfacs Vacances S.L. g. Google Spain S.L.* Sentencia Juz. 1.ª Inst. Amposta (núm. 1) 32/2012, de 23 de febrero.
[81] Mayer-Schönberger (n. 74) 92-127.
[82] European Union (n. 27).

> Rétturinn til að gleymast hefur verið túlkaður bæði sem lagalegur réttur og sem gildi eða hagsmunir sem verja þarf með lögum. Rétturinn hefur verið talinn falla undir réttinn til friðhelgi einkalífs, jafnvel þótt hann taki til upplýsinga sem eru, að minnsta kosti að hluta til, opinberar. Hann stendur fyrir forræði einstaklinga yfir eigin persónuupplýsingum, stýringarnálgun á hugtakið friðhelgi einkalífs og viðleitni til að flytja upplýsingar af opinberum vettvangi yfir á einkasvæði. Franska hugtakið oubli felur bæði í sér réttinn til að gleymast (réttinn til að láta þriðju aðila gleyma fortíð þinni) og réttinn til að gleyma (réttinn til að komast hjá árekstrum við eigin fortíð) og lýsir neikvæðum rétti einstaklingsins til þess að stýra fortíð sinni og framtíð.[83]

Ekki er fullkomlega ljóst af reglugerðardrögum framkvæmdastjórnarinnar hvernig hugtakið rétturinn til að gleymast og til afmáunar skuli túlkað og hvert inntak þess á í raun að vera. Í upphaflegu drögunum var yfirskrift 17. gr. *rétturinn til að gleymast og til afmáunar*. Eftir breytingar Evrópuþingsins kallast ákvæðið nú eingöngu *réttur til afmáunar*. Í fljótu bragði kann þetta að virðast lítils háttar breyting en sumir fræðimenn telja að í raun sé um tvenn ólík hugtök að ræða, eins og nánar verður greint frá síðar í kaflanum.

Þótt rétturinn til að gleymast og til afmáunar í tillögum framkvæmdastjórnarinnar hafi vakið hvað mesta athygli og hvað hörðust viðbrögð hefur Viviane Reding, framkvæmdastjóri ESB talað á þeim nótum að rétturinn í 17. gr. reglugerðardraganna sé ekki algjörlega nýr réttur, heldur sé í raun verið að útfæra og skýra þann rétt sem þegar sé fyrir hendi í b-lið 12. gr. tilskipunar 95/46/EB.[84]

Einhverjir hafa haldið því fram að í 17. gr. sé engin nýmæli að finna, eins og David Lindsay bendir á í grein sinni, *The right to be forgotten in European Data Protection Law.*[85] Þar vísar hann meðal annars í W.J. Maxwell sem telur réttinn til að gleymast vera „sama hlutinn með nýjum merkimiða.“[86] Fræðimaðurinn Christopher Kuner sagði árið 2012 að 17. gr. virtist vera útvíkkun á þeim rétti sem fyrir væri í 12. gr. núgildandi

[83] Meg Leta Ambrose og Jef Ausloos, „The Right to be Forgotten Across the Pond“ (2013) 3 Journal of Information Policy 1, 14. Íslensk þýðing höfundar.
[84] Viviane Reding, „The Upcoming Data Protection Reform for the European Union“ (2011) 1 (1) International Data Privacy Law 3.
[85] David Lindsay, „The Right to be forgotten in European Data Protection Law“. Witzleb, N. (ritstj.), *Emerging challenges in privacy law: comparative perspectives* (Kindle útg. Cambridge University Press 2014) 64%.
[86] W.J. Maxwell, „Data Privacy: the European Comission Pushes for Total Harmonisation“ (2012) 18 (6) Computer and Telecommunications Law Review; David Lindsay (n. 85) 64%.

tilskipunar og ekki væri ljóst af hverju þyrfti að stofna til nýs réttar undir nýju nafni.[87] Munurinn á þeim rétti sem fyrir hendi er í núgildandi tilskipun og lögum nr. 77/2000, og þeim rétti sem framkvæmdastjórn ESB hefur kynnt með 17. gr. reglugerðardraga sinna, er því ekki skýr að mati fræðimanna.

Lindsay segir nauðsynlegt að greina á milli þriggja lagalegra hugtaka sem oft sé steypt saman í eitt fyrir misskilning: Réttar til óminnis (e. *right to oblivion,* f. *droit à l'oubli*), réttar til afmáunar og réttar til að gleymast.[88] Svipuð aðgreining er gerð í grein Ambrose og Ausloos en þar er greint á milli réttar til óminnis (e. *right to oblivion*) og réttar til afmáunar (e. *right to erasure*) sem höfundar segja oft ruglað saman undir heitinu rétturinn til að gleymast.[89]

Samkvæmt Lindsay vísar *réttur til óminnis* í fyrsta lagi til þess réttar sem fyrir hendi er í nokkrum löndum sem tilheyra „civil law" réttarkerfinu: réttar einstaklinga til að fá nöfn sín tengd afbrotum úr fortíð afmáð og þá fyrst og fremst umfjöllun fjölmiðla um þau. Í öðru lagi þýði hugtakið *réttur til afmáunar* rétt til að fjarlægja eða láta eyða persónuupplýsingum á grundvelli núgildandi persónuverndarlaga. Í þriðja lagi feli hugtakið *rétturinn til að gleymast* í sér rétt til að fá persónuupplýsingar af netinu fjarlægðar eða aðgengi að þeim takmarkað, sérstaklega á notendastýrðum miðlum eins og samfélagsmiðlum, auk þess sem í hugtakinu geta falist réttindi til fá persónuupplýsingar fjarlægðar úr leitarniðurstöðum leitarvéla og úr rafrænum gagnabönkum.

Þessi þrenn hugtök, eins og Lindsay setur þau fram, verða útskýrð nánar í eftirfarandi köflum, þar sem farið verður yfir uppruna og þróun réttarins og mismunandi afbrigði hans, í sögulegu samhengi. Tilgangurinn er meðal annars að kanna hvort 17. gr. reglugerðardraga framkvæmdastjórnarinnar felur í sér nýmæli og aukinn rétt hins skráða eða hvort um „gamalt vín á nýjum belgjum" er að ræða.

4.2.1 Réttur til óminnis

Réttur til óminnis er elsta tegund þessara réttinda og á rót að rekja til Frakklands, þar sem hann kallast *droit à l'oubli*. Rétturinn til óminnis byggist meðal annars á því að glæpamenn geta óskað eftir því að fá syndir sínar afmáðar af spjöldum sögunnar, þ.e.

[87]Christopher Kuner, „The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law" [2012] *Bloomberg BNA Privacy and Security Law Report* <http://ico.org.uk/news/events/~/media/documents/future_of_dp_in_europe_2012/ico_event_future_of_dp_in_europe_2012_Chris_Kuner_article.ashx> skoðað 29. apríl 2014.
[88] David Lindsay (n. 85) 63-65%.
[89] Ambrose og Ausloos (n. 83), 2, 14.

geta mótmælt birtingu nafna sinna í fjölmiðlum, í tengslum við glæpinn, eftir að hafa afplánað dóm sinn. Þessi réttur einstaklinga, til að koma í veg fyrir að aðrir geti tengt nöfn þeirra við glæpi sem framdir voru í fortíð, stríðir eðli málsins samkvæmt á móti upplýsingarétti almennings og tjáningarfrelsi fjölmiðla. Rökin fyrir réttinum til óminnis eru að réttur til friðhelgi einkalífs sé grundvallarmannréttindi, sem í þessu samhengi feli í sér rétt til að halda mannlegri reisn og vernda orðspor sitt.[90]

Samsvarandi réttur hinum franska *droit à l'oubli* er einnig fyrir hendi í þýskum lögum. Í máli *Lebach I*[91] fjallaði þýski stjórnlagadómstóllinn um réttinn til óminnis en málið snerist um lögbannskröfu sem lögð hafði verið fram vegna sýningar heimildarmyndar í sjónvarpi. Myndin fjallaði um rán úr vopnabúri hersins þar sem fjórir hermenn létu lífið. Sá sem óskaði eftir lögbanninu hafði verið dæmdur samsekur þeim sem ránið frömdu og taldi dómstóllinn að hann ætti að njóta þess grundvallarréttar að hafa forræði yfir eigin persónuupplýsingum, þ.e. rétt til að ákveða hvort og að hversu miklu leyti öðrum væri heimilt að greina frá ævisögu hans, bæði almennt og einstökum atburðum úr lífi hans.[92] Taldi dómurinn að þessi réttur vægi þyngra en tjáningarfrelsi fjölmiðilsins og áréttaði í dómsniðurstöðu mikilvægi þess að fangar ættu kost á endurhæfingu eftir afplánun dóma sinna. Í dómnum var jafnframt tekið tillit til þess að tuttugu og fjögur ár höfðu liðið síðan brotið var framið og taldi dómstóllinn að áhugi almennings á umfjöllun því tengdu hefði dvínað í tímans rás.

Hvað umfjöllun á netinu varðar létu hálfbræðurnir Wolfgang Werlé og Manfred Lauber reyna á réttinn til að óminnis fyrir þýskum dómstólum árið 2009. Þeir höfðu verið dæmdir fyrir morð á þekktum leikara árið 1993, höfðu afplánað dóma sína og vildu að nöfn þeirra í tengslum við umfjöllun um glæpinn yrðu afmáð af síðum tiltekinna vefmiðla. Töldu þeir nafnbirtinguna skaða framtíðarmöguleika sína á endurhæfingu og nýju lífi utan fangelsismúranna og vísuðu þar meðal annars til Lebach-málsins. Bræðurnir unnu málið á fyrsta dómstigi fyrir þýskum dómstólum og voru nöfn þeirra afmáð úr þýsku Wikipediu og fleiri miðlum.[93] Þýski stjórnlagadómstóllinn sneri dómnum hins vegar við á þeim forsendum að fjarlæging nafnanna bryti gegn

[90] Ambrose og Ausloos (n. 83) 15.
[91] BverfG, 25.11.1999 - 1 BvR 348/98 og 1 BvR 755/98.
[92] Sama heimild.
[93] BGH, 10.11.2009 - VI ZR 217/08 (rainbow.at); 15.12.2009 - VI ZR 227/08 og 228/08 (Deutschlandradio); 09.02.2010 - VI ZR 243/08 og 244/08 (Spiegel Online); apríl 2010 - VI ZR 245/08 og 246/08 (morgenweb.de); J. Schwartz, „Two German Killers Demanding Anonymity Sue Wikipedia's Parent" *The New York Times* (13. nóvember 2009) <http://www.nytimes.com/2009/11/13/us/13wiki.html> skoðað 14. apríl 2014.

stjórnarskrárvörðu tjáningarfrelsi fjölmiðla og að Werlé og Lauber yrðu að þola brot á friðhelgi einkalífs upp að ákveðnu marki.[94] Eftir að dómurinn féll endurbirti Wikipedia nöfn bræðranna í gagnagrunni sínum.[95]

Þrátt fyrir að rétturinn til óminnis eigi upphaflega rætur að rekja til Frakklands hefur hann ekki verið óumdeildur þar í landi og er lagaleg túlkun réttarins á reiki.[96] Frakkland tók þó forystu í þessum máli árið 2009 þegar þáverandi ráðherra stafræns hagkerfis, Kosciusko-Morizet, stóð að útgáfu viðmiðunarreglna um góða starfshætti í fyrirtækjum, með áherslu á réttinn til að gleymast á samfélagsmiðlum og leitarvélum.[97] Reglurnar voru staðfestar og undirritaðar af nokkrum frönskum fyrirtækjum, þar á meðal franska Microsoft. Segja má að þetta franska frumkvæði, rétturinn til óminnis, geti talist mikilvægur forveri og áhrifavaldur þess að rétturinn til að gleymast og til afmáunar var kynntur til sögunnar í þeim reglugerðardrögum framkvæmdastjórnarinnar sem nú eru til umfjöllunar hjá Evrópusambandinu.

4.2.2 Réttur til afmáunar

Einn helsti munurinn á réttinum til óminnis og réttinum til afmáunar er að rétturinn til óminnis beinist aðallega að fjölmiðlum, vegna efnis sem þar hefur birst. Í þeim rétti til afmáunar, sem til staðar er í persónuverndarlögum og byggir á tilskipun 95/46/EB, er fréttamennska hins vegar undanþegin gildissviði laganna, sbr. 9. gr. tilskipunarinnar, sem innleidd var með 5. gr. pul.[98]

Fyrstu persónuverndarlögin tóku gildi upp úr 1970 í Hessen í Þýskalandi en fyrstu landslögin á sviði persónuverndar voru sett í Svíþjóð árið 1973. Nú má víða finna löggjöf og leiðbeinandi tilmæli á þessu sviði. Mikilvægustu réttarheimildirnar í Evrópu eru *Samningur Evrópuráðsins um vernd persónuupplýsinga* frá 28. janúar 1981,[99]

---

94 BGH 01.02.2011 - VI ZR 345/09 (Kölner Stadtanzeiger, ksta.de); 01.02.2011 - VI ZR 346/09 (Frankfurter Allgemeine Zeitung faz.net); 01.02.2011 - VI ZR 114/09 (Süddeutsche Zeitung sz-online.de); 10.04.2010 - VI ZR 245/08 & 246/06 (morgenweb.de); 15.12.2009 - VI ZR 227/08 & 228/08 (Deutschlandradio); nóvember 2009 - VI ZR 217/08 (rainbow.at).

95 M.L. Ambrose, „It's about time: Privacy, information life cycles and the right to be forgotten" (2013) 16 (2) Stanford Technology Law Review 101.

96 B. Markesinis, B., „Concerns and Ideas about the Developing English Law of Privacy (and How Knowledge of Foreign Law Might Be of Help)" (2004) 52 American Journal of Comparative Law 133, 69; David Lindsay (n. 85) 63%.

97 M. Kuschewsky, „The right to be forgotten - the Fog Finally Lifts" (2012) 12 Privacy & Data Protection 10; David Lindsay (n. 85) 63%.

98 Um skilgreiningu á hugtakinu fréttamennska vísast m.a. til dóms MDE, Steel og Morris g. Bretlandi, App. no. 68416/01, 94. mgr. (ECtHR, 15. febrúar 2005).

99 Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [1981] ETS 108 (tók gildi 1. október 1985, undirritaður fyrir Íslands hönd 27. september 1982 og fullgiltur á Íslandi 1. júlí 1991 (hér eftir Samningur Evrópuráðsins).

Tilskipun Evrópuþingsins og Ráðsins nr. 95/46/EB um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og frjálsa miðlun slíkra upplýsinga, frá 24. okóber 1995,[100] og auk þess *Leiðbeinandi tilmæli OECD* frá 23. september 1980,[101] endurskoðuð árið 2013.[102]

Strax á upphafsárum evrópskrar persónuverndarlöggjafar mátti greina að sjónum væri beint að þeim vandamálum sem því gæti fylgt að varðveita persónuupplýsingar í ótakmarkaðan tíma. Í fyrstu drögum að leiðbeinandi reglum OECD frá 1980 var að finna reglu um ákveðin tímamörk varðandi varðveislu þeirra persónuupplýsinga sem unnt væri að rekja til hins skráða. Hins vegar rataði sú regla ekki inn í lokaútgáfu OECD-reglnanna þar sem reglur um öryggi og takmörkuð not upplýsinga þóttu veita nægilega vernd.[103] Finna má samhljóm með þessum hugmyndum og tillögum Mayer-Schönberger um síðasta „neysludag" eða notkunardag persónuupplýsinga, sem áður var minnst á.[104]

Rétt til afmáunar er því ekki að finna í OECD-reglunum frá 1980, þess utan að í skýringum við tilgangsregluna segir að þegar upplýsingar þjóni ekki tilgangi sínum lengur geti verið nauðsynlegt að eyða þeim eða gera þær ópersónugreinanlegar. Í hinum uppfærðu reglum frá 2013 er hins vegar að finna ákvæði undir yfirskriftinni „individual participation principle" þar sem segir meðal annars að einstaklingar skuli hafa rétt til að vefengja upplýsingar sem þeim tengjast og - ef sú vefenging reynist á rökum reist - öðlist þeir rétt til að láta eyða upplýsingunum, leiðrétta þær, fullkomna eða lagfæra.[105]

Samningur Evrópuráðsins um vernd persónuupplýsinga frá 1981 gekk lengra en leiðbeinandi reglur OECD, með eftirfarandi ákvæði um gæði upplýsinga í 5. gr:

> Persónuupplýsingar sem unnar eru vélrænt skulu vera:
> a) fengnar og unnar á heiðarlegan og lögmætan hátt,
> b) geymdar í tilgreindum og lögmætum tilgangi og ekki notaðar á hátt sem ósamrýmanlegur er þeim tilgangi.
> c) hæfilegar, viðeigandi og eigi umfangsmeiri en tilgangur geymslu þeirra gefur efni til,
> d) nákvæmar og, þegar nauðsyn er, framfærðar,
> e) varðveittar í þeirri mynd að ekki verði unnt að

[100] Tilskipun 95/46/EB (n.7).
[101] OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [1980] C(80)58/FINAL (Hér eftir Leiðbeiningarreglur OECD).
[102] Leiðbeiningarreglur OECD (n. 101), uppfærðar 11. júlí 2013, með C(2013) 79.
[103] M. Kirby: Transborder Data Flows and the „Basic Rules" of Data Privacy (1980)16 Stanford Journal of International Law, 58-9; David Lindsay (n. 85) 64%.
[104] Mayer-Schönberger (n. 74) 171-173.
[105] Leiðbeiningarreglur OECD, uppf. 2013 (n. 102).

> sérgreina skráðan aðila lengur en þörf er á með tilliti til tilgangs geymslu upplýsinganna.[106]

Ákvæði 5. gr. Evrópuráðssamningsins fær stoð í c-lið 8. gr. hans, sem gefur rétt til að fá upplýsingar leiðréttar eða afmáðar hafi með þær verið unnið gagnstætt ákvæðum samningsins. Í 5. gr., sbr. c-lið 8. gr., er þó einungis fjallað um þann möguleika að fá upplýsingar afmáðar en enginn skýr réttur þar að lútandi staðfestur.[107]

Sú hugmynd að setja tímamörk á heimild til varðveislu persónuupplýsinga fékk aukinn hljómgrunn á níunda áratugnum og í byrjun þess tíunda, sérstaklega í Evrópu.[108] Árið 1986 mælti ráðherranefnd Evrópuráðsins með því að sett yrðu skilyrði um geymslutíma persónuupplýsinga í þjóðaröryggisstofnunum, þar sem tímalengd færi eftir mikilvægi upplýsinganna og því hversu viðkvæmar þær væru.[109]

Mikilvægt skref hvað réttinn til afmáunar varðar var síðan stigið með núgildandi tilskipun 95/46/EB.[110] Samkvæmt henni er vinnsla persónuupplýsinga einungis heimil í tilteknum tilvikum, svo sem þegar hinn skráði hefur gefið óþvingað og upplýst samþykki sitt og vinnslan er nauðsynleg til að uppfylla samningskyldu hins skráða eða lagaskyldu ábyrgðaraðila.[111]

Ákvæði um eyðingu persónuupplýsinga koma fyrir á þremur stöðum í tilskipun 95/46/EB: Í 1. mgr. 6. gr. (um meginreglur um gæði gagna),[112] 12. gr. (um rétt til aðgangs)[113] og 14. gr. (um andmælarétt).[114]

Sá réttur til afmáunar sem lögfestur er í tilskipun 95/46/EB er þó ekki fullkomlega skýr, eins og sjá má af áliti Lögsögumanns Evrópudómstólsins í máli sem nýlega var rekið fyrir dómstólnum: Google Spain SL og Google Inc. gegn spænsku Persónuverndarstofunni og Mario Costeja González. Þar komst Lögsögumaðurinn að þeirri niðurstöðu að almennur réttur til að gleymast væri ekki fyrir hendi, samkvæmt tilskipun 95/46/EB, þegar um væri að ræða sannar og réttar upplýsingar. Lögsögumaðurinn sagði tilskipun 95/46/EB veita einstaklingum rétt til að andmæla

[106] Samningur Evrópuráðsins (n. 99).
[107] Sama heimild; David Lindsay (n. 85) 64%.
[108] O. Pastukhov: The Right to Oblivion: What's in a Name? (2013)19 Computer and Telecommunications Law Review 13,16; David Lindsay (n. 85) 64%.
[109] Council of Europe, „Recommendation R(86)1 of the Committee of Ministers to Member States on the Protection of Personal Data used for Social Security Purposes“, (23. janúar 1986) <*https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1894447&SecMode=1&DocId=688622&Usage=2*> skoðað 12. apríl 2014.
[110] Tilskipun 95/46/EB (n. 8).
[111] Tilskipun 95/46/EB (n. 7), 7. gr.
[112] Tilskipun 95/46/EB (n. 7), 1. mgr. 6. gr.
[113] Tilskipun 95/46/EB (n. 7), b-liður 12. gr.
[114] Tilskipun 95/46/EB (n. 7), 14. gr.

vinnslu upplýsinga um þá sjálfa, hafi þeir til þess lögmætar og knýjandi ástæður vegna sérstakra aðstæðna, nema kveðið sé á um annað í innlendum lögum, sbr. a-lið 1. mgr. 14. gr. tilskipunarinnar. Hins vegar taldi lögsögumaðurinn að huglægt mat eða vilji gæti ekki einn og sér talist vera lögmætar og knýjandi ástæður. Evrópudómstóllinn komst hins vegar að þveröfugri niðurstöðu í málinu, í dómi sem féll 13. maí sl., en nánar verður fjallað um hann síðar í ritgerðinni.[115]

4.2.3 Réttur til að gleymast

Rétturinn til að gleymast er, samkvæmt Lindsay, rétturinn til að fá persónuupplýsingar á netinu fjarlægðar eða til að aðgengi að slíkum upplýsingum verði torveldað.[116]

Jafnvel þótt rétturinn til að gleymast hafi verið í forgrunni í kynningum framkvæmdastjórnar ESB á hugmyndum í hinni nýju Evrópulöggjöf í persónuverndarmálum, hafa útfærslur réttarins í reglugerðinni sjálfri verið tiltölulega varkárar. Í minnisblaði til útskýringar með reglugerðardrögunum segir til dæmis að 17. grein útfæri og skýri rétt til afmáunar sem til staðar sé í b-lið 12. gr. tilskipunar 95/46/EB. Í umsögn Persónuverndar um 17. gr. reglugerðardraganna, frá 8. maí 2013, er tekið undir þetta en þar segir að ákvæði um eyðingu persónuupplýsinga hafi lengi verið í gildi en að rétturinn til að gleymast hafi ekki verið orðaður í löggjöf fyrr. Þar sé nánar tiltekið um að ræða réttinn til að upplýsingar á netinu séu fjarlægðar þannig að þær verði ekki aðgengilegar aftur.[117]

Skiptar skoðanir hafa verið um hvort rétturinn til að gleymast, sbr. 17. gr., sé frábrugðinn núgildandi rétti, hvort hann eigi við um persónuupplýsingar sem birst hafa á samfélagsmiðlum[118] og ennfremur hvort hann innifeli réttinn til að láta fjarlægja persónuupplýsingar úr leitarniðurstöðum leitarvéla á netinu.[119] Þrátt fyrir varfærið orðalag hefur framkvæmdastjórnin einmitt helst réttlætt nauðsyn nýrrar löggjafar með því að nýtt landslag í persónuverndarmálum, og þá sérstaklega tilkoma samfélagsmiðla, kalli á nýjar reglur til verndar friðhelgi einkalífs netnotenda. Í áliti framkvæmdastjórnarinnar frá 2010 er til dæmis sérstaklega minnst á samfélagsmiðla í þessu samhengi:

---

[115] Mál C-131/12 *Google Spain SL og Google Inc g. Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [ECR 13. maí 2014].
[116] David Lindsay (n. 85) 64%.
[117] Persónuvernd (n. 21).
[118] Xavery Konarski, o.fl., *Reforming the Data Protection Package.* (European Parliament 2012) 60.
[119] David Lindsay (n. 85) 67%.

> Með tilkomu nútímatækni geta einstaklingar auðveldlega deilt upplýsingum um athafnir sínar og áhugasvið og gert þær opinberar á alþjóðlegum vettvangi, með hætti sem áður hefur ekki þekkst. Samfélagsmiðlar, með hundruðum milljóna meðlima um allan heim, eru kannski augljósasta, en ekki eina, dæmið um þetta fyrirbrigði.[120]

Af þessu má draga þá ályktun að reglugerðardrögunum sé ætlað að taka til samfélagsmiðla. Persónuvernd bendir á, í umsögn sinni, að af tæknilegri uppbyggingu Netsins leiði að erfiðleikum geti verið háð að fjarlægja upplýsingar af netinu, þannig að þær verði ekki aðgengilegar aftur. Ákvæði 3. mgr. 17. gr. afmarki hins vegar réttinn með þeim hætti að ábyrgðaraðili, sem gert hefur upplýsingar opinberar, geri allar viðeigandi ráðstafanir til að hlekkjum á netinu og afritum verði eytt, það er með því að senda þeim sem ábyrgð bera á viðkomandi hlekkjum eða afritum skilaboð um ósk hins skráða þar að lútandi, enda kosti slíkt ekki óhóflega fyrirhöfn. Þá hafi í 147. breytingatillögu Albrecht-skýrslunnar verið lagt til að framangreint eigi aðeins við þegar persónuupplýsingar hafi verið birtar án samþykkis. Gerir Persónuvernd ekki athugasemd við þá afstöðu, að því gefnu að hinn skráði hafi verið lögráða þegar samþykki var veitt.

Í þessu ljósi má segja að raddir þeirra, sem vöruðu við því að með orðalaginu „réttur til að gleymast“ væru skapaðar óraunhæfar væntingar meðal netnotenda, hafi átt einhvern rétt á sér, enda urðu þær til þess að yfirskrift ákvæðisins var breytt í meðförum Evrópuþingsins og heitir það nú einungis „réttur til afmáunar“. Ekki verður annað séð af framangreindu að rétturinn í 17. gr. reglugerðardraganna frá 2012 feli annað í sér en skyldu ábyrgðaraðila til að reyna, með kurteislegum skilaboðum, að fá efni og hlekkjum á tiltekið efni eytt af Netinu, með þeim fyrirvara að það kosti ekki óhóflega fyrirhöfn. Í meðförum Evrópuþingsins í mars 2014 var orðalagi 2. mgr. 17. gr. þó breytt á þá vegu að hafi ábyrgðaraðili gert persónuupplýsingar opinberar, án þess að réttlætanlegar ástæður séu fyrir hendi, beri honum að stíga öll raunhæf skref til að afmá upplýsingarnar, ekki einungis til að upplýsa þriðja aðila um að hinn skráði óski eftir því að það verði gert.[121] Nánar er fjallað um þessar breytingar í kafla 4.6.3.

Í umsögn, sem gerð var fyrir dómsmálanefnd neðri deildar breska þingsins, sagði David Smith, varaframkvæmdastjóri upplýsingamála hjá Persónuverndarstofnun

---

[120] „Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses“ (*European Union*, 25. janúar 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> skoðað 17. apríl 2014.

[121] „Legislative Observatory 2012/0011(COD) - Text adopted by Parliament, 1st reading/single reading“ (*European Parliament*, 12. mars 2014), 2. mgr. 17. gr.

Bretlands (Information Commissioner's Office), að stór hluti réttarins til að gleymast væri í raun endurtekning á ákvæðum núgildandi tilskipunar þess efnis persónuupplýsingar skuli ekki geyma lengur en nauðsyn krefji og hafi verið unnið með þær í trássi við lög skuli þeim eytt. Að hans mati er meira nýmæli fólgið í ákvæði 19. gr. reglugerðardraganna um andmælarétt hins skráða en um þann rétt er fjallað í kafla 4.5.3 í þessari ritgerð.[122]

Breska dómsmálanefndin ályktaði að það væri villandi að tala um „rétt til að gleymast" í tengslum við rétt borgara til að láta eyða persónuupplýsingum, sem varðveittar væru án heimildar eða þar sem varðveislu væri ábótavant. Taldi nefndin að slíkt orðalag gæti skapað óraunhæfar væntingar, sérstaklega í tengslum við leitarvélar og samfélagsmiðla.[123]

Gagnstæð sjónarmið koma fram í áliti Konarski o.fl. sem samið var fyrir Evrópuþingið en þar segir að rétturinn til að gleymast feli í sér aukinn rétt fyrir neytendur.[124]

Í reglugerðardrögum framkvæmdastjórnarinnar er ekki tekið á því hvort rétturinn til að gleymast og til afmáunar eigi eingöngu við um efni sem búið er til og/eða birt af notandanum sjálfum eða einnig um efni sem aðrir netnotendur setja inn, til dæmis þegar einstaklingur birtir mynd af öðrum einstaklingi á facebook. Í grein Ambrose og Ausloos, þar sem einungis er gerður greinarmunur á rétti til óminnis og rétti til afmáunar, túlka höfundar 17. gr. þannig að afmáun (í merkingunni „gleymska", sbr. greiningu Lindsays) eigi ekki við um efni sem búið er til eða birt af öðrum en notandanum sjálfum og að hugtakið réttur til afmáunar (eða rétturinn til að gleymast) sé þannig þrengra hugtak en hugtakið réttur til óminnis. Þetta er þó ekki tekið fram í reglugerðardrögunum sjálfum, eins og fyrr segir.

Samkvæmt Ambrose og Ausloos verndar réttur til óminnis einstaklinga fyrir því að orðspor þeirra skaðist vegna upplýsinga sem birtast á netinu og eru geymdar þar lengur en nauðsynlegt er. Réttur til afmáunar felur hins vegar í sér tilfærslu valds frá ábyrgðaraðila til hins skráða, með þeim rökum að torvelt sé að öðlast ótvírætt samþykki netnotenda og þar af leiðandi ættu þeir hvenær sem er að geta afturkallað samþykki fyrir vinnslu eigin persónuupplýsinga. Annar munur á þessum tveimur hugtökum segja Ambrose og Ausloos að sé tími. Hugtakið óminni þýði að upplýsingarnar verði síður aðgengilegar eftir ákveðinn tíma en hugtakið afmáun feli ekki í sér nein tímamörk.[125]

---

[122] House of Commons Justice Committee, *The Committee's Opinion on the European Union Data Protection Framework Proposals*, (HC 2012-13, 572-I) 26-7; David Lindsay (n. 85) 65%.
[123] House of Commons Justice Committee (n. 122), 27-8.
[124] Xavery Konarski o.fl. (n. 118).

Með 17. gr. reglugerðardraga framkvæmdastjórnarinnar um réttinn til að gleymast og til afmáunar má því segja að gerð sé tilraun til að leysa þau vandamál sem til hafa komið með „rafrænni eilífð“ upplýsinga, með því að bræða saman réttinn til óminnis og núgildandi rétt til afmáunar og með því að styrkja núgildandi rétt til afmáunar í persónuverndarlögum. Hvort og hvernig sá réttur styrkist nákvæmlega með tilkomu 17. gr. reglugerðardraganna er útskýrt nánar í kafla 4.5.

4.3 Friðhelgi einkalífs og tjáningarfrelsi

Ekki eru allir sannfærðir um nauðsyn þess að lögfesta sérstakan rétt fólks til að fá eigin persónuupplýsingum eytt af netinu. Deilt hefur verið um hvort rétturinn til að gleymast eigi rétt á sér og ef svo er, hversu víðtækur hann eigi að vera; hvort hann verði til að hefta tjáningar- og fjölmiðlafrelsi og hvort með honum sé verið að heimila sögufalsanir með því að leitarvélum verði til dæmis gert að fjarlægja sannar, sögulegar staðreyndir úr gagnagrunnum sínum. Í þessu sambandi hefur verið talað um alhliða ritskoðun internetsins[126] og rafrænar bókabrennur, sem líkja megi við bókabrennur nasista 1933 og bókabrennu munksins Savonarola og fylgimanna hans í Flórens 1497.[127]

Peter Fleischer, yfirráðgjafi friðhelgismála hjá Google, hefur meðal annars velt þeirri spurningu upp hvort rafrænar „bókabrennur“ í nafni friðhelgi einkalífs séu frekar réttlætanlegar en bókabrennur í nafni kynþáttar, trúar eða pólitíkur.[128]

Tjáningarfrelsi er oftast nefnt sem dæmi um mannréttindi sem settar yrðu skorður fengju netnotendur vald til að fá upplýsingum um sjálfa sig eytt af netinu. Tjáningarfrelsið er varið í 73. gr. stjórnarskrár og 10. gr. Mannréttindasáttmála Evrópu. Sé notast við víðtæka skilgreiningu á hugtakinu tjáningarfrelsi felast í því þrír meginþættir:

1. málfrelsi
2. skoðanafrelsi (sem greina má í sannfæringarfrelsi og birtingarfrelsi, þ. á m. prentfrelsi) - og
3. upplýsingafrelsi (réttur manna til að afla sér upplýsinga og dreifa þeim).[129]

---

[125] Ambrose og Ausloos (n. 83).
[126] Adam Thierer, „Europe's „Right to Be Forgotten“: Privacy as Internet Censorship“ (*The Technology Liberation Front*, 23. janúar 2012) <http://techliberation.com/2012/01/23/europes-right-to-be-forgotten-privacy-as-internet-censorship/> skoðað 15. apríl 2014.
[127] Peter Fleischer, „Book Burning, updated for the Digital Age“ <http://peterfleischer.blogspot.com/2012/11/book-burning-updated-for-digital-age.html> skoðað 15. apríl 2014.
[128] Sama heimild.

Samsvarandi ákvæði er í 11. gr. Réttindaskrár ESB um tjáningar- og upplýsingafrelsi þar sem tekið er fram að tjáningarfrelsi nái einnig til frelsis til að hafa skoðanir, taka við og skila áfram upplýsingum heima og erlendis, án afskipta stjórnvalda. Ákvæði 11. gr. er túlkað með hliðsjón af 3. mgr. 52. gr. Réttindaskrárinnar þar sem segir að að svo miklu leyti sem í Réttindaskránni felist réttindi sem samsvari réttindum í MSE skuli þau réttindi hafa sömu merkingu og gildissvið og mælt sé fyrir um í þeim sáttmála. Takmarkanir sem réttindum 11. gr. Réttindaskrárinnar eru sett mega því ekki vera umfangsmeiri en þær takmarkanir sem mælt er fyrir um í 2. mgr. 10. gr. MSE. Skilyrði er að lög mæli fyrir um takmarkanirnar og að þær séu nauðsynlegar í lýðræðislegu þjóðfélagi „til verndar heilsu eða siðgæði manna, mannorði eða réttindum“.[130]

Við túlkun 8. gr. MSE, sem vernd persónuupplýsinga fellur undir, þarf að taka mið af grundvallarréttindum sem réttlæta skerðingu á friðhelgi einkalífs. Þetta kemur fram í 2. mgr. 8. gr. MSE þar sem segir að opinber stjórnvöld skuli eigi ganga á rétt manna til friðhelgi einkalífs og fjölskyldu nema samkvæmt því sem lög mæli fyrir um og nauðsyn beri til í lýðræðislegu þjóðfélagi [...] til verndar heilsu manna eða siðgæði eða réttindum og frelsi annarra. Hið sama á við um 71. gr. stjórnarskrár um friðhelgi einkalífs, sbr. 3. mgr., þar sem segir að með sérstakri lagaheimild megi takmarka friðhelgi einkalífs ef brýna nauðsyn beri til vegna réttinda annarra. Mannréttindadómstóll Evrópu, Evrópudómstóllinn og Hæstiréttur Íslands hafa margsinnis kveðið á um að við túlkun á 8. gr. MSE, sbr. 71. gr. stjskr., verði að taka mið af réttindum sem setja friðhelgi einkalífs skorður.[131]

Af 1. mgr. 52. gr. Réttindaskrár Evrópusambandsins má einnig ráða að réttindi, eins og þau sem varin eru í 7. og 8. gr. hennar, má skerða, svo lengi sem þær skorður byggja á lagaákvæðum og virða eðli og frelsi réttindanna sem um ræðir, eru nauðsynlegar með hliðsjón af meðalhófsreglunni og uppfylla markmið á sviði almannahagsmuna sem Evrópusambandið viðurkennir eða þörfina á að vernda mannréttindi og mannfrelsi.[132]

---

[129] Páll Sigurðsson, *Fjölmiðlaréttur: meginþættir réttarumhverfis fjölmiðlanna* (Háskólaútgáfan 1997) 52.

[130] Samningur um verndun mannréttinda og mannfrelsis (Mannréttindasáttmáli Evrópu), (samþykktur 4. nóvember 1950, tók gildi 3. september 1953, undirritaður fyrir Íslands hönd 19. júní 1953, fullgiltur á Íslandi 3. september 1953 og lögfestur 30. maí 1994) Stjtíð. C, 11/1954 (MSE), 10. gr.

[131] Sjá m.a. Hrd. 30. október 1968 í máli nr. 159/968 (Læknatalsdóm), Hrd. 1. mars 2007 í máli nr. 278/2006 (Bubbamál), Mál C-73/07 *Tietosuojavaltuutettu g. Satakunnan Markkinapörssin Oy og Satamedia Oy* [2008] ECR I-9831 og *Editions Plon gegn Frakklandi* App no. 58148/00 (ECtHR, 18. maí 2004).

[132] Charter of Fundamental Rights of The European Union (n. 54), 52. gr.

4.3.1 Takmarkanir á grundvelli tjáningarfrelsis

4.3.1.1 Fréttamennska og bókmenntaleg og listræn starfsemi

Þótt megintilgangur tilskipunar 95/46/EB og reglugerðardraga framkvæmdastjórnarinnar sé vernd persónuupplýsinga, í samræmi við 8. gr. Réttindaskrár ESB og 8. gr. MSE, sætir verndin meðal annars takmörkunum vegna tjáningarfrelsis, eins og fram kemur í 9. gr. tilskipunar 95/46/EB, þar sem fjallað er um samspil tjáningarfrelsis og réttarins til verndar persónuupplýsinga/vinnslu persónuupplýsinga. Í 9. gr. segir að aðildarríkin skuli aðeins kveða á um undanþágur eða frávik frá ákvæðum II., IV. og VI. kafla „vegna vinnslu persónuupplýsinga sem fer einungis fram vegna fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi, að það sé nauðsynlegt til að samræma réttinn til friðhelgi einkalífs og reglur um tjáningarfrelsi.“[133] Af ákvæðinu má ráða að tilteknar takmarkanir og frávik frá persónuupplýsingavernd og friðhelgi einkalífs séu nauðsynlegar til að vernda önnur réttindi og þá sérstaklega tjáningarfrelsið.

Ákvæðið var innleitt með 5. gr. íslensku persónuverndarlaganna þar sem segir að víkja *megi* frá ákvæðum laganna í þágu fjölmiðlunar, lista eða bókmennta að því marki sem nauðsynlegt sé til að samræma sjónarmið um rétt til einkalífs annars vegar og tjáningarfrelsis hins vegar. Þegar persónuupplýsingar séu einvörðungu unnar í þágu fréttamennsku[134] eða bókmenntalegrar eða listrænnar starfsemi gildi aðeins tiltekin ákvæði laganna.[135]

Athygli vekur að á meðan í 5. gr. pul. segir að víkja *megi* frá ákvæðum laganna í þágu fjölmiðlunar, lista eða bókmennta segir í 37. gr. inngangsorða tilskipunar 95/46/EB að víkja *beri (e. shall)* frá ákvæðum laganna í sama tilgangi.[136] Íslenska ákvæðið er því einungis heimildarákvæði, ólíkt ákvæði tilskipunarinnar, sem gefur tilefni til að álykta að íslensku lögunum sé ætlað rýmra gildissvið, meðal annars gagnvart fjölmiðlum, en þeirri tilskipun sem þau byggja á. Þessi orðalagsmunur er þó ekki skýrður nánar í frumvarpi til pul.

Sem dæmi um túlkun 9. gr. tilskipunar 95/46/EB má nefna dóm Evrópudómstólsins í máli nr. C-73/07, *Tietosuojavaltuutettu gegn Satakunnan Markkinapörssin Oy og*

[133] Tilskipun 95/46/EB (n. 7), 9. gr.
[134] Um það álitaefni hvað telst til fréttamennsku má m.a. vísa til *Steel og Morris g. Bretlandi* App no. 68416/01, 94. mgr. (ECtHR, 15. febrúar 2005).
[135] Nánar tiltekið 4. gr., 1. og 4. tölul. 7. gr., 11.-13. gr. og 24., 28., 42. og 43. gr. laga nr. 77/2000.
[136] Herdís Þorgeirsdóttir, „Þröng skýring á fjölmiðlafrelsi og vafasamt eftirlit opinberrar stofnunar?“ *mbl.is* (Reykjavík, júlí 2005) <http://www.mbl.is/greinasafn/grein/1029789/> skoðað 8. maí 2014.

Satamedia Oy.[137] Þar skilgreindi Evrópudómstóllinn samspil persónuupplýsingaverndar og fjölmiðlafrelsis út frá 9. gr. tilskipunarinnar. Málið snerist um að fyrirtækið Markkinapörssin hafði aflað upplýsinga um skattgreiðslur 1,2 milljón einstaklinga, á lögmætan hátt frá finnskum skattyfirvöldum í þeim tilgangi að birta hluta upplýsinganna í landshlutaútgáfu dagblaðs. Annað fyrirtæki, sem var hluti af sömu fyrirtækjasamsteypu, bauð farsímaeigendum þá þjónustu að senda þeim þessar upplýsingar með sms-skilaboðum. Dómstóllinn lagði mat á hvort vinnsla þessara opinberu persónuupplýsinga í þessum tilgangi teldist fara fram einungis í þágu fréttamennsku. Eftir að hafa slegið því föstu að um vinnslu persónuupplýsinga, í skilningi 1. mgr. 3. gr. tilskipunar 95/46/EB væri að ræða, fjallaði dómstóllinn um málið út frá 9. gr. tilskipunarinnar. Í fyrsta lagi benti hann á mikilvægi tjáningarfrelsis í lýðræðissamfélagi og að túlka ætti athafnir tengdar tjáningarfrelsi, eins og fréttamennsku, með víðum hætti. Þá sagði dómstóllinn að til að ná jafnvægi milli þessara tveggja grundvallarréttinda, persónuupplýsingaverndar og tjáningafrelsis, mætti aðeins takmarka réttinn til persónuupplýsingaverndar ef brýna nauðsyn bæri til. Dómstóllinn taldi að þær athafnir fyrirtækjanna að taka upplýsingar úr opinberum skjölum gætu talist fréttamennska í skilningi 9. gr. ef tilgangurinn væri að birta almenningi upplýsingarnar, skoðanir eða hugmyndir, óháð því hvaða miðlar væru notaðir til að koma þeim á framfæri. Dómstóllinn taldi einnig að þessar athafnir ættu ekki bara við um skráða fjölmiðla og að þær mætti framkvæma í gróðaskyni. Dómstóllinn lét finnskum landsdómstólum hins vegar eftir að álykta um hvort þetta mat ætti við í þessu ákveðna tilviki.

Annað dæmi um túlkun 9. gr. tilskipunar 95/46/EB er dómur sem féll við Hæstarétt Svíþjóðar árið 2001 í svokölluðu *Ramsbro-máli*.[138] Dómurinn varpar ljósi á þýðingu hugtaksins „einvörðungu unnar í þágu fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi“ í 9. gr. tilskipunar 95/46/EB og 7. gr. sænsku persónuverndarlaganna, sbr. 5. gr. pul. Í Ramsbro-málinu tókust á andstæð sjónarmið, tjáningarfrelsi, sbr. 10 gr. MSE, og reglur um lögmæta skerðingu þess. Hæstiréttur Svíþjóðar taldi að undantekningin hvað fréttamennsku varðar tæki ekki bara til formlegrar skilgreiningar á fjölmiðli, heldur einnig tjáningar sem ekki teldist til atvinnufjölmiðlunar. Þá ætti undantekningin einnig við um ærumeiðandi tjáningu.

[137] Mál C-73/07 *Tietosuojavaltuutettu g. Satakunnan Markkinapörssin Oy og Satamedia Oy* [2008] ECR I-9831, málsgr. 56, 61 og 62.
[138] Högsta domstolen, dom 2001-06-12 i mål nr. B 293-00.

Dómstóllinn komst að þeirri niðurstöðu að tilgangur löggjafans með orðinu „eingöngu“ í lögunum hefði verið sá að undanskilja ekki frá gildissviði laganna upplýsingar sem unnar væru af blaðamönnum og fjölmiðlum í öðrum tilgangi en í þágu fréttamennsku (til dæmis þegar tilgangurinn væri innheimta, bein markaðssetning eða kortlagning notendaupplýsinga („prófila“) viðskiptavina sinna).[139]

4.3.1.2 Framlag til samfélagsumræðu og áhugi almennings

Mannréttindadómstóll Evrópu hefur, við skýringar á markalínunni milli friðhelgi einkalífs og tjáningarfrelsis, lagt mikið upp úr því hvort sú tjáning sem um ræðir feli í sér framlag til samfélagsumræðu sem varði hagsmuni almennings.

Sem dæmi um þetta má nefna mál *Mosley gegn Bretlandi*.[140] Málið snerist um hvort breskum stjórnvöldum hefði borið að setja lög þess efnis að fjölmiðlar tilkynntu fólki fyrir fram ef birta ætti greinar um það, þannig að fólk gæti gert ráðstafanir til að stöðva birtinguna. Max Rufus Mosley, breskur ríkisborgari, sat í stjórn Formúlu 1 árið 2008, þegar breska vikublaðið News of the World birti frétt um hann með forsíðufyrirsögninni „F1 boss has sick Nazi orgy with 5 hookers“. Inni í blaðinu voru nokkur skjáskot af myndbandi sem einn þátttakenda í kynlífsorgíunni hafði tekið. Myndirnar birtust einnig á netsíðu blaðsins. Mosley fór í skaðabótamál og krafðist þess einnig að greinin yrði fjarlægð af netsíðu blaðsins. Hæstiréttur Bretlands (*High Court*) hafnaði því á þeim forsendum að efnið væri þegar orðið opinbert. Á hinn bóginn væri engar tengingar við nasista að finna á myndunum og því engir almannahagsmunir fyrir hendi sem réttlættu birtingu þeirra. Málalyktir urðu þær að dagblaðið var dæmt til greiðslu skaðabóta.

Mosley áfrýjaði málinu til MDE á grundvelli 8. gr., 9. gr. og 13 gr. MSE, og vísaði meðal annars til þess að réttur hans til friðhelgi einkalífs hefði verið brotinn, þar sem í Bretlandi bæri fjölmiðlum engin skylda til að upplýsa fólk fyrirfram um birtingu greina þar sem um það er fjallað. Honum hafi ekki gefist kostur á að stöðva birtingu greinarinnar, til dæmis með því að krefjast lögbanns.

MDE féllst ekki á þau sjónarmið og sagði í niðurstöðu sinni að jafnvel þótt tilgangur myndbirtingarinnar hafi almennt meira verið til skemmtunar en fræðslu nyti hún verndar 10. gr. MSE um tjáningarfrelsi. Vissulega væri um viðkvæmar

[139] Sama heimild.
[140] *Mosley gegn Bretlandi* App no. 48009/08 (ECtHR, 10. maí 2011).

persónuupplýsingar að ræða og efnið varðaði ekki almannahagsmuni. Hins vegar yrði að gæta varúðar við takmarkanir á tjáningarfrelsinu og með hliðsjón af þeim heftandi áhrifum sem ákvæði um fyrirfram tilkynningaskyldu útgefenda gæti haft væri ekki hægt að gera þá kröfu til stjórnvalda að lögfesta skyldu fjölmiðla til að tilkynna einstaklingum fyrirfram um greinar sem til stæði að birta um þá.

4.3.1.3 Opinberar persónur

Oft getur verið erfitt að finna hið fullkomna jafnvægi á milli friðhelgi einkalífs, þar með talið vernd persónuupplýsinga, og tjáningarfrelsis. Persónuupplýsingar eru misviðkvæmar og vekja mismikinn áhuga almennings. Ljósmynd af gangandi vegfarendum á Ingólfstorgi gengur augljóslega ekki eins nærri friðhelgi einkalífs og kynlífsmyndband. Á sama máta hefur almenningur mismikinn áhuga á ólíkum tegundum persónuupplýsinga: myndband af alþingismanni að þiggja mútur væri til dæmis líklegra til að vekja meiri áhuga almennings en ljósmyndir frá Skagfirðingakvöldi á skemmtistaðnum Spot.

Svokallaðar opinberar persónur, frægt fólk, stjórnmálamenn, kóngafólk, auðmenn, tónlistarmenn og aðrir sem eru áberandi í þjóðlífinu hafa þurft að sæta því að um einkamál þeirra sé að einhverju leyti fjallað á nærgöngulli hátt í fjölmiðlum en gengur og gerist um almenna borgara.[141] Um þetta má nefna svokallaðan *Karólínudóm II*, þar sem þýskir dómstólar og MDE töldu réttlætanlegt að birta myndir af fjölskyldu Mónakóprinsessu í skíðafríi, á meðan Rainer fursti lá banaleguna. Að mati MDE var það lögmætt fréttaefni og ekki brot á 8. gr. MSE um friðhelgi einkalífs að fjalla um það hvernig börn furstans samræmdu skyldur gagnvart fjölskyldunni við lögmætar þarfir einkalífsins, þar á meðal þá löngun að fara í skíðafrí.[142] Áður hafði MDE snúið við dómi þýskra dómstóla og talið það brot á friðhelgi einkalífs, sbr. 8. gr. MSE, að birta myndir af Karólínu Mónakóprinsessu á hestbaki, á þeim forsendum að hún væri þar ekki í opinberu hlutverki og að frægt fólk ætti líka tilkall til friðhelgi einkalífs. Almenningur hefði enga lögvarða hagsmuni af því að vita hvar prinsessan væri stödd, jafnvel þótt hún væri þekkt og birtist á stöðum sem væru ekki lokaðir almenningi.[143]

[141] Páll Sigurðsson (n. 129) 119-120.
[142] *Von Hannover gegn Þýskalandi* App no. 40660/08 og 60641/08 (ECtHR, 7. febrúar 2012) og *Von Hannover gegn Þýskalandi*, App no. 59320/00 (ECtHR, 24. júní 2004).
[143] *Von Hannover gegn Þýskalandi*, App no. 59320/00 (ECtHR, 24. júní 2004).

Fyrri Karólínudómurinn vakti hörð viðbrögð í Þýskalandi og víðar og þótti gróf íhlutun í tjáningarfrelsi fjölmiðla.[144]

Í dómi MDE frá 18. maí 2004 í máli *Editions Plon gegn Frakklandi*, var líflæknir Mitterands Frakklandsforseta talinn hafa verið í fullum rétti til að gefa út bók þar sem fram kom að læknirinn hefði falsað heilbrigðisvottorð Mitterands að hans beiðni um skeið, til að koma í veg fyrir að fréttir af veikindum hans spyrðust út. Lagt hafði verið bann við útgáfu bókarinnar á þeim forsendum að hún stríddi gegn friðhelgi einkalífs forsetans. MDE taldi aftur á móti að áhugi almennings og hagsmunir af almennri umræðu um sögu forsetatíðar Mitterands vægu þyngra en hagsmunir af því að vernda trúnað um þessar upplýsingar.[145]

Hér á landi hefur einnig verið deilt um jafnvægið milli friðhelgi einkalífs opinberra persóna og tjáningarfrelsis fjölmiðla fyrir dómstólum. Þar má nefna *Bubbamálið* svokallaða, þar sem tónlistarmaðurinn Ásbjörn Morthens, Bubbi, taldi að brotið hefði verið á friðhelgi einkalífs síns með því að birta mynd af sér á forsíðu tímaritsins Hér og nú, með sígarettu í munni, inni í bíl sínum, undir fyrirsögninni „Bubbi fallinn". Vörn stefnanda byggðist meðal annars á tilvísun í fyrra Karólínumálið um friðhelgi einkalífs opinberra persóna en stefndu báru fyrir sig að Bubbi væri almannapersóna sem hefði tjáð sig um einkamálefni sín í fjölmiðlum og ætti því minni rétt á friðhelgi einkalífs í þessu samhengi. Hæstiréttur féllst á rök stefnanda í málinu.[146]

Í máli blaðamannsins *Bjarkar Eiðsdóttur gegn Íslandi* fyrir Mannréttindadómstól Evrópu var deilt um birtingu viðtals við nektardansmær í tímaritinu Vikunni en í viðtalinu staðhæfði kona að vændi færi fram inni á nektarstaðnum Goldfinger. Hæstiréttur hafði í meiðyrðamáli fyrir dómnum dæmt Björk til greiðslu miskabóta, þar sem hún taldist, skv. þágildandi prentlögum, bera ábyrgð á ummælum í viðtalinu.[147] Hún vann hins vegar málið fyrir MDE, sem nefndi í dómsniðurstöðu að með því að hefja rekstur nektardansstaðar hefði þáverandi eigandi Goldfinger næturklúbbsins, Ásgeir Þór Davíðsson, vísvitandi og óhjákvæmilega gengið inn á opinberan vettvang þar sem hann mátti búast við óvæginni gagnrýni. Þolmörk fyrir því hvað talist geti ásættanleg gagnrýni yrðu að teljast víðari en þegar um almenna borgara eða venjulega

[144] Sjá m.a. Frauka Schmid Petersen, „The press as public watch dogs and the privacy of public figures" [2004] International Law Office.
[145] *Editions Plon gegn Frakklandi* App no. 58148/00 (ECtHR, 18. maí 2004).
[146] Hrd. 1. mars 2007 í máli nr. 278/2006.
[147] Hrd. 5. mars 2009 í máli nr. 328/2008.

starfsmenn væri að ræða.[148] Um þetta vísaði MDE einnig til mála *Steel og Morris gegn Bretlandi*[149] og *Anghel v. Moldova.*[150]

Framangreind mál sneru flest að birtingu efnis í prentmiðlum. Í dómsmálum sem tengjast óvæginni umfjöllun á netinu og friðhelgi einkalífs hafa dómstólar einnig vísað í sjónarmið um að skerða megi einkalífsvernd þegar opinberar persónur eiga í hlut. Í dómi Evrópudómstólsins frá 13. maí 2014,[151] þar sem deilt var um rétt einstaklings til að fá sannar og réttar persónuupplýsingar afmáðar af netinu, sagði að þegar beiðni um afmáun berist ábyrgðaraðila verði að fara fram hagsmunamat, þar sem metið sé jafnvægi milli upplýsingafrelsis, það er áhuga annarra netnotenda á upplýsingunum, og hagsmuna hins skráða, sérstaklega réttar til friðhelgi einkalífs og verndar persónuupplýsinga. Evrópudómstóllinn sagði í niðurstöðu sinni að jafnvel þótt almennt séð trompi réttur hins skráða áhuga almennings á persónlegum upplýsingum um hann, verði slíkt hagsmunamat líka að fara eftir eðli upplýsinganna. Þar á meðal þurfi að líta til þess hversu viðkvæmar upplýsingarnar séu fyrir hinn skráða og áhuga almennings á því að fá upplýsingarnar. Sá áhugi fari fyrst og fremst eftir því hlutverki sem hinn skráði gegnir á opinberum vettvangi. Verður sú niðurstaða Evrópudómstólsins ekki skilin öðruvísi en svo að opinberar persónur þurfi frekar að sæta því að persónuupplýsingar um þær séu aðgengilegar á netinu, í óþökk þeirra sjálfra. Um niðurstöðu Evrópudómstólsins verður fjallað nánar í kafla 4.9.1.

4.3.2 Aðgangur að upplýsingum

Réttur til upplýsingafrelsis er varinn í tjáningarfrelsisákvæðum 10. gr. MSE, 73. gr. stjórnarskrár og 11. gr. Réttindaskrár ESB. Ákvæðin vernda bæði réttinn til að afla sér upplýsinga og dreifa þeim. Vaxandi vitundarvakning um mikilvægi gegnsærrar stjórnsýslu í lýðræðisþjóðfélögum hefur orðið til þess að upplýsingaréttur almennings; rétturinn til aðgangs að opinberum gögnum, hefur verið tryggður, meðal annars með íslenskum upplýsingalögum, fyrst nr. 50/1996 og síðar með núgildandi upplýsingalögum nr. 140/2012. Í frumvarpi til laga nr. 50/1996 segir:

> ... í nútíma lýðræðisþjóðfélagi er það talið sjálfsagt að almenningur eigi þess kost að fylgjast með því sem stjórnvöld hafast að, ýmist beint eða fyrir milligöngu fjölmiðla. Liður í því er að hver og einn geti fengið

[148] *Björk Eiðsdóttir g. Íslandi* App no. 46443/09, 68. mgr. (ECtHR, 10. júlí 2012).
[149] *Steel og Morris g. Bretlandi* App no. 68416/01, 94. mgr. (ECtHR, 15. febrúar 2005).
[150] *Anghel g. Moldóvu* App no. 42864/05, 34 mgr. (ECtHR, 27. nóvember 2007).
[151] Mál C-131/12 *Google Spain* (n. 115).

> aðgang að upplýsingum um mál sem til meðferðar eru hjá stjórnvöldum, jafnvel þótt það snerti ekki hann sjálfan.[152]

Sambærilegar áherslur má sjá hjá Evrópusambandinu, sbr. reglugerð Evrópuþingsins og ráðsins (EB) nr. 1049/2001,[153] 42. gr. Réttindaskrár ESB og 3. mgr. 15. gr. sáttmála um starfshætti Evrópusambandsins.[154]

Komið getur til togstreitu á milli upplýsingafrelsis og friðhelgi einkalífs ef aðgangur að upplýsingum eða skjölum hjá stjórnvöldum myndi fela í sér aðgengi að persónupplýsingum annarra en þess sem krefst aðgangsins. Verði einstaklingum heimilað að eyða upplýsingum sem varða þá sjálfa, er ljóst að aðgangur annarra að sömu upplýsingum skerðist að sama skapi.

4.3.3 Listrænt og vísindalegt frelsi

Einnig getur komið til skörunar á milli verndar persónuupplýsinga og réttar til friðhelgi einkalífs annars vegar og frelsis í listum og vísindum, sem verndað er í 13. gr. Réttindaskrár ESB, hins vegar. Þar segir að virða skuli frelsi fræðimanna í störfum sínum en réttur þessi á rót að rekja til hugsana- og tjáningarfrelsis og er túlkaður með hliðsjón af 1. gr. Réttindaskrárinnar um friðhelgi mannlegrar reisnar. Í MSE fellur réttur til frelsis í vísindum og listum undir 10. gr.[155] Rétturinn getur einnig sætt takmörkunum í 10. gr. MSE.[156]

Í reglugerðinni eru undanþágur sem snúa að listrænni starfsemi og vísindalegum rannsóknum, sambærilegar undanþágum frá gildissviði tilskipunar 95/46/EB. Í 1. mgr. 80. gr. er kveðið á um undanþágur vegna starfsemi sem eingöngu fer fram vegna fréttamennsku eða í listrænum tilgangi. Um þetta má einnig vísa til 121. gr. inngangsorða reglugerðarinnar. Í c-lið 3. mgr. 17. gr. er kveðið á um undanþágur sem snúa að sagnfræðilegum, tölfræðilegum og vísindalegum rannsóknum. Af því má ætla að rétturinn til að gleymast taki ekki til upplýsinga sem teljast nauðsynlegar í slíkum tilgangi.

---

[152] Alþt. 1995-96, A-deild, þskj. --361. mál.
[153] Regulation (EC) nr. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission Documents, OJ 2001 L 145.
[154] Charter of Fundamental Rights of The European Union (n. 54); Consolidated versions of the Treaty of European Union and the Treaty on the Functioning of the European Union [2012] C 326/01.
[155] European Union Agency for fundamental rights (n. 51) 31; *Muller og aðrir gegn Sviss* App no. 10737/84 (ECtHR, 24. maí 1988).
[156] Sama heimild; skýringar við Réttindaskrá ESB, OJ 2007 C 303.

4.4 Áhrif hertrar persónuverndarlöggjafar í Evrópu á viðskiptahagsmuni bandarískra fyrirtækja

Nýjar reglur um persónuvernd, þar á meðal um réttinn til afmáunar og útfærslu hans, og andstöðu við þær, innan og utan Evrópusambandsins, verður einnig að skoða í ljósi þess hversu mikil áhrif þær hafa á hagsmuni þeirra fyrirtækja sem byggja afkomu sína á markaðssetningu persónuupplýsinga; upplýsinga sem fengnar eru með kortlagningu rafrænna spora sem notendur skilja eftir sig á netinu, til dæmis á samfélagsmiðlum, sölusíðum og leitarvélum. Mörg slík fyrirtæki eru með starfsemi í Evrópu, þ. á m. Google og Facebook. Fyrirtækin búa yfir gríðarlegu magni persónuupplýsinga og eru þannig í aðstöðu til að selja auglýsendum aðgang að skýrt afmörkuðum markhópum. The Wall Street Journal greindi frá því 8. janúar sl. að tekjur upplýsingaveita í bandarískri eigu, af viðskiptum með persónuupplýsingar í Evrópu árið 2011, hefðu verið vel yfir 100 milljarðar dollara en tekjur af sambærilegum viðskiptum í öðrum löndum (utan Bandaríkjanna) rétt um 50 milljarðar dollara. Bandarískir hagsmunaaðilar, fyrirtæki og stjórnmálamenn, hafa lýst yfir áhyggjum af hertum reglum innan Evrópusambandsins á sviði persónuverndar og þeim áhrifum sem þær hafi á viðskipti með persónuupplýsingar.[157]

Á grundvelli svokallaðs Safe Harbour samnings[158] hafa yfir 3000 bandarísk fyrirtæki mátt flytja upplýsingar um evrópska borgara til Bandaríkjanna.[159] En eins og greint er frá í 2. kafla þessarar ritgerðar höfðu uppljóstranir Edwards Snowden þau áhrif að þann 12. mars 2014 kallaði Evrópuþingið eftir tafarlausri afturköllun Safe Harbour samningsins þar til hann hefði verið endurskoðaður og tryggt að flutningur persónuupplýsinga í markaðslegum tilgangi til Bandaríkjanna væri í samræmi við ströngustu kröfur Evrópusambandsins. Í The Wall Street Journal var því haldið fram að fyrirtæki sem vinna með persónuupplýsingar, allt frá kreditkortafyrirtækjum til „tölvuskýjafyrirtækja“, íhugi að koma á fót gagnaverum í Evrópu, fari svo að flutningi persónuupplýsinga frá Evrópu til Bandaríkjanna verði of strangar skorður settar.[160]

---

[157] Sam Schechner, „Online Privacy Could Spark U.S.-EU Trade Rift“ (*The Wall Street Journal*) <http://online.wsj.com/news/articles/SB10001424052702304361604579291041878017398> skoðað 10. mars 2014.

[158] „Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU“ (nóvember 2013) COM (2013) 847 <http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf> skoðað 29. apríl 2014.

[159] Sam Schechner (n. 157).

[160] Sam Schechner (n. 157).

Um leið og Evrópuþingið kallaði eftir afturköllun Safe Harbour samningsins hótaði þingið því að samþykkja ekki lokaútgáfu fríverslunarsamnings milli Evrópu og Bandaríkjanna, sem hefur verið í burðarliðnum síðan 2013 (oftast nefndur Transantlantic Trade and Investment Partnership, TTIP).[161] Safe Harbour samningurinn og TTIP fríverslunarsamningurinn eru skilyrði þess að áfram verði frjálst flæði gagna milli Evrópu og Bandaríkjanna. Þá ályktaði Evrópuþingið um nauðsyn þess að Evrópa komi sér upp eigin „tölvuskýi", þ.e. þrói eigin lausnir í upplýsingatækni og netöryggismálum. Hvort að hertar persónuverndarreglur í Evrópu og harðnandi afstaða Evrópuþingsins í garð bandarískra tölvuskýjafyrirtækja sé fyrirboði þess að einhvers konar viðskiptastríð með persónuupplýsingar sé í uppsiglingu milli Evrópu og Bandaríkjanna verður tíminn að leiða í ljós.

4.5 Ákvæði 17. greinar, tengd ákvæði og Albrecht-skýrslan

Hér á eftir verður fjallað um 17. gr. reglugerðardraga framkvæmdastjórnar ESB og tengd ákvæði, þ.e. samspil 17. gr. og annarra ákvæða í löggjöfinni, sem þýðingu hafa í sambandi við rétt til afmáunar, eins og þau eru sett fram í reglugerðardrögunum. Einnig verður fjallað um núgildandi rétt og tengd ákvæði í tilskipun 95/46/EB og pul. Þar er í fyrsta lagi um að ræða ákvæði um aðgang og leiðréttingu í 12. gr. tilskipunar 95/46/EB, 25. gr. pul. og 16. gr. reglugerðardraganna, sem borin verða saman við ákvæði 26. gr. pul. og 17. gr. reglugerðardraganna. Einnig verður fjallað um andmælarétt hins skráða, sem varinn er í 14. grein tilskipunar 95/46/EB, 28. gr. pul. og 19. gr. reglugerðardraganna. Þá verður farið yfir ákvæði um skyldur ábyrgðaraðila tengdar vinnslu þriðju aðila, sem upplýsingum hefur verið miðlað til, í 12. gr tilskipunar 95/46/EB, 25. gr. pul. og 2. mgr. 17. gr. reglugerðardraganna. Loks verður fjallað um þær breytingar sem lagðar eru til á 17. gr. og framangreindum ákvæðum í Albrecht-skýrslu Evrópuþingsins.

4.5.1 Aðgangur og leiðrétting

Í a-lið 1. mgr. 12. gr. tilskipunar 95/46/EB, er fjallað um rétt til aðgangs en ákvæðið var innleitt með 18. gr. pul. Í b-lið 1. mgr. 12. gr. tilskipunarinnar er fjallað um rétt til leiðréttingar, afmáunar eða aðgangstakmarkana á upplýsingum. Skilyrði er að vinnsla

[161] „US NSA: stop mass surveillance now or face consequences, MEPs say" (*European Parliament*, 12. mars 2014) <http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203> skoðað 21. apríl 2014.

þeirra uppfylli ekki ákvæði tilskipunarinnar, einkum ef þær eru ófullkomnar eða óáreiðanlegar. Sambærilegt ákvæði er að finna í 25. gr. pul. um leiðréttingu og eyðingu rangra og villandi persónuupplýsinga. Skilyrði 25. gr. pul. er að upplýsingarnar séu rangar, villandi, ófullkomnar eða hafi verið skráðar án tilskilinnar heimildar.
Í reglugerðardrögum framkvæmdastjórnarinnar frá 2012 er gerður greinarmunur á rétti til leiðréttingar (í 16. gr.) og rétti til afmáunar (í 17. gr.) Ákvæði 16. gr. innifelur rétt til leiðréttingar á ónákvæmum og ófullkomnum upplýsingum en ákvæðið er efnislega samhljóða ákvæðum 25. gr. pul. og hluta b-liðar 12. gr. tilskipunar 95/46/EB. Í stað þess að innifela rétt til afmáunar í sama ákvæði, eins og í tilskipun 95/46/EB er síðan sérstakt ákvæði um rétt til afmáunar í 17. gr. reglugerðardraganna. Ástæða þess er væntanlega sú að hér er verið að kynna nýjan rétt til sögunnar, sem ekki lýtur sömu lögmálum og fyrri réttur til afmáunar. Í íslenskum lögum var hins vegar farin sú leið árið 2000 að kveða á um sérstakan rétt til afmáunar upplýsinga sem hvorki eru rangar né villandi, í 26. gr. pul. Skilyrði 26. gr. pul. er að ekki sé lengur málefnaleg ástæða til að varðveita upplýsingarnar, til dæmis að ekki sé mælt fyrir um varðveislu þeirra í lögum eða að ábyrgðaraðili vinni ekki lengur með upplýsingarnar í samræmi við upphaflegan tilgang með söfnun þeirra. Íslensku lögin ganga því lengra en tilskipun 95/46/EB og orða skýrar heimildina til eyðingu réttra og sannra upplýsinga, með framangreindum skilyrðum þó.

4.5.2 Rétturinn til að gleymast í 17. gr.

Rétturinn til að gleymast og til afmáunar, sbr. 17. gr. reglugerðardraga framkvæmdastjórnarinnar, felur í sér rétt einstaklinga til að krefjast þess að persónuupplýsingum um þá verði eytt af netinu, ef ekki eru lengur málefnalegar ástæður til að varðveita þær. Ber ábyrgðaraðila þá að fjarlægja persónuupplýsingarnar af netinu, eftir því sem unnt er, þannig að þær verði ekki aðgengilegar aftur. Þannig geta einstaklingar haft áhrif á opinbera birtingu og miðlun upplýsinga um þá sjálfa. Þessar upplýsingar gætu til dæmis verið sjálfsævisögulegar upplýsingar, fjárhagsupplýsingar, upplýsingar um ólögmætt athæfi og ljósmyndir. Ekki er skilyrði að upplýsingarnar séu rangar, ófullkomnar eða óáreiðanlegar, heldur getur verið um sannar og réttar upplýsingar að ræða, sem einstaklingurinn kærir sig ekki um að séu aðgengilegar öðrum á netinu.[162]

[162] Reglugerðardrög framkvæmdastjórnarinnar (n. 6), 17. gr.

Þótt ákvæði um eyðingu persónuupplýsinga séu fyrir hendi í tilskipun 95/46/EB og pul. hefur rétturinn til að gleymast og til afmáunar ekki verið orðaður skýrt í Evrópurétti fyrr en í 17. gr. þeirra reglugerðardraga sem nú eru til umræðu og meðferðar hjá ESB.[163] Rétturinn í 17. gr. er auk þess mun víðtækari en sá sem fyrir er, eins og fram hefur komið.

4.5.2.1 Skilyrði 17. gr. fyrir afmáun persónuupplýsinga

Í 1. mgr. 17. gr. reglugerðardraga framkvæmdastjórnarinnar eru eftirfarandi skilyrði fyrir afmáun persónuupplýsinga talin upp í liðum a) til d):

- þegar upplýsingarnar eru ekki lengur nauðsynlegar í tengslum við þann tilgang sem söfnun þeirra eða vinnslu var upphaflega ætlaður;
- þegar lögmæti vinnslunnar byggist á samþykki hins skráða og það samþykki hefur verið dregið til baka;
- þegar samþykktur geymslutími upplýsinganna er runninn út eða;
- vinnsla upplýsinganna fer í bága við ákvæði reglugerðarinnar af öðrum ástæðum.

Lindsay bendir á að ákvæði um ofangreind réttindi gangi lengra en núgildandi réttur í tilskipun 95/46/EB með því að styrkja regluna um gæði gagna (sem finna má í e-lið 1. mgr. 6. gr. tilskipunarinnar) og með því að mæla fyrir um heimild til eyðingar þegar lögmæti vinnslunnar byggir á samþykki hins skráða og hann hefur dregið það til baka.[164] Auk þess gildir rétturinn til afmáunar ef hinn skráði nýtir sér andmælaréttinn í 19. gr.

4.5.3 Andmælaréttur

Andmælaréttur hins skráða er varinn í 14. grein núgildandi tilskipunar 95/46/EB, 28. gr. pul. og 19. gr. reglugerðardraganna, líkt og áður hefur komið fram. Rétturinn í 1. mgr. 19. gr. reglugerðardraganna gefur hinum skráða rétt til að mótmæla vinnslu eigin persónuupplýsinga „hvenær sem er“ sé vinnslan einungis lögmæt af því að hún sé nauðsynleg:

- til að vernda mikilvæga hagsmuni hins skráða;
- vegna framkvæmdar í þágu almannahagsmuna eða í krafti opinbers valds;
- vegna lögmætra hagsmuna ábyrgðaraðilans.

[163] Umsögn Persónuverndar (n. 21).
[164] David Lindsay (n. 85), 65%.

Lindsay bendir á að í tillögu framkvæmdastjórnarinnar, um andmælarétt hins skráða í 19. gr., sé tekið á þeim takmörkunum sem sama rétti séu settar í núgildandi tilskipun. Í fyrsta lagi sé andmælarétturinn víkkaður út og taki nú til þess þegar vinnsla sé nauðsynleg til að vernda mikilvæga hagsmuni hins skráða. Í öðru lagi þurfi hinn skráði ekki lengur að bera sönnunarbyrðina fyrir því að „lögmætar og knýjandi ástæður“ til andmæla séu fyrir hendi, sbr. 12. gr. tilskipunar 95/46/EB, heldur beri ábyrgðaraðilinn sönnunarbyrðina fyrir því að til staðar séu „lögmætar og knýjandi ástæður“fyrir vinnslunni, sem trompi grundvallarréttindi hins skráða. Síðast en ekki síst tengist andmælaréttur 19. gr. nú réttinum til að fá persónuupplýsingum eytt, með þeim hætti að beri andmæli hins skráða, á grundvelli 19. gr., árangur virkjar það réttinn í 17. gr., til að fá persónuupplýsingum eytt. Þar að auki sé kveðið á um það í 2. mgr. 19. gr. að beiting andmælaréttarins skuli vera hinum skráða að kostnaðarlausu, sé bein markaðssetning tilgangur vinnslunnar.[165]

[165] David Lindsay (n. 85), 65 %.

4.6 Samanburður á 17. gr. reglugerðardraga framkvæmda-stjórnarinnar fyrir og eftir breytingar Evrópuþingsins

LIBE-nefndin, þingnefnd Evrópuþingsins á sviði borgaralegra réttinda, dóms- og innanríkismála, gerði margar breytingartillögur á ákvæðum reglugerðardraga framkvæmdastjórnarinnar, þar á meðal 17. gr. Breytingartillögurnar voru settar fram í svokallaðri Albrecht-skýrslu. Frumvarpið sem Evrópuþingið samþykkti 12. mars 2014 var því nokkuð ólíkt þeim drögum sem framkvæmdastjórnin lagði fyrst fram.

Reglugerðardrög framkvæmdastjórnar ESB, 25. janúar 2012[166]	**Frumvarp samþykkt af Evrópu-þinginu, 12. mars 2014**[167]
Réttur til að gleymast og til afmáunar	**Réttur til afmáunar**
1. Hinn skráði skal hafa rétt til að fara fram á að ábyrgðaraðili eyði persónuupplýsingum sem rekja má til hans og komi í veg fyrir frekari dreifingu þeirra , **sérstaklega þegar um er að ræða perónuupplýsingar sem hinn skráði gerði opinberar þegar hann eða hún var barn að aldri,** þegar eitt af eftirfarandi atriðum á við:	1. Hinn skráði skal hafa rétt til að fara fram á að ábyrgðaraðili eyði persónuupplýsingum sem rekja má til hans og komi í veg fyrir frekari dreifingu þeirra, ***og rétt til að fara fram á að þriðji aðili afmái sérhverjan hlekk á, eða afrit þeirra gagna*****,** þegar eitt af eftirfarandi atriðum á við:
(a) upplýsingarnar eru ekki lengur nauðsynlegar í tengslum við þann tilgang sem upphaflega var með því að safna þeim eða vinna þær á annan hátt;	(a) upplýsingarnar eru ekki lengur nauðsynlegar í tengslum við þann tilgang sem upphaflega var með því að safna þeim eða vinna þær á annan hátt;
(b) hinn skráði dregur samþykki, sem vinnslan byggði á, til baka sbr. a-lið 1. mgr. 6. gr., eða þegar geymslutími er útrunninn eða þegar engin önnur lögmæt ástæða er fyrir vinnslu upplýsinganna;	(b) hinn skráði dregur samþykki, sem vinnslan byggði á, til baka sbr. a-lið 1. mgr. 6 .gr., eða þegar samþykktur geymslutími er útrunninn, og þegar engin önnur lögmæt ástæða er fyrir vinnslu upplýsinganna;
(c) hinn skráði mótmælir vinnslu persónuupplýsinga skv. 19. gr.	(c) hinn skráði mótmælir vinnslu persónuupplýsinga, skv. 19. gr;
	(ca) dómstóll eða úrskurðaraðili á stjórnsýslustigi, með staðfestu í EES ríki, hefur komist að endanlegri og afgerandi niðurstöðu

[166] Reglugerðardrög framkvæmdastjórnarinnar (n. 6), 17. gr. Íslensk þýðing höfundar.

[167] „Legislative Observatory 2012/0011(COD) - Text adopted by Parliament, 1st reading/single reading" (*European Parliament*, 12. mars 2014), 17. gr. <www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN> skoðað 20. apríl 2014. Íslensk þýðing höfundar.

	um að afmá eigi viðkomandi gögn
(d) vinnsla persónuupplýsinga samræmist ekki ákvæðum þessarar reglugerðar af öðrum ástæðum	**(d)** ***unnið hefur verið með persónuupplýsingarnar á ólögmætan hátt***
	1a. Beiting 1. mgr. skal vera háð því að ábyrgðaraðili fái staðfest að sá sem óskar eftir að upplýsingar verði afmáðar sé hinn skráði.
2. Þegar ábyrgðaraðili, sem sem vísað er til í 1. gr., hefur gert persónuupplýsingar opinberar, á hann að stíga öll raunhæf skref, ***þar á meðal tæknileg skref, tengdar þeim upplýsingum sem hann ber ábyrgð á að birta, til að upplýsa þriðju aðila, sem vinna slík gögn, um að hinn skráði óski eftir því að þeir afmái alla tengla að þeim persónuupplýsingum eða afritum af þeim. Þegar ábyrgðaraðilinn hefur gefið þriðja aðila leyfi til að birta persónuupplýsingar telst ábyrgðaraðilinn bera ábyrgð á þeirri birtingu.***	2. Þegar ábyrgðaraðili sem vísað er til í 1. mgr. hefur gert persónuupplýsingar opinberar ***án þess að heimildir 1. mgr. 6. gr. eigi við,*** skal hann stíga öll raunhæf skref ***til að afmá upplýsingarnar, þar á meðal hjá þriðju aðilum, án tillits til 77. gr. Ábyrgðaraðilinn skal upplýsa hinn skráða, þegar mögulegt er, um þær aðgerðir sem viðkomandi þriðju aðilar hafa gripið til.***
3. Ábyrgðaraðilinn skal framkvæma afmáunina án tafar, nema í þeim tilvikum þegar varðveisla gagnanna er nauðsynleg:	3. Ábyrgðaraðilinn, ***og þriðji aðili þegar það á við,*** skal framkvæma afmáunina án tafar, nema í þeim tilvikum þegar varðveisla gagnanna er nauðsynleg:
(a) vegna réttar til tjáningarfrelsis, sbr. 80. gr.;	(a) vegna réttar til tjáningarfrelsis, sbr. 80. gr.;
(b) vegna almannahagsmuna á sviði lýðheilsu, sbr. 81. gr.;	(b) vegna almannahagsmuna á sviði lýðheilsu, sbr. 81. gr.;
(c) vegna sagnfræðilegra, tölfræðilegra eða vísindalegra rannsóknarhagsmuna, sbr. 83. gr.;	(c) vegna sagnfræðilegra, tölfræðilegra eða vísindalegra rannsóknarhagsmuna, sbr. 83. gr.;
(d) til að uppfylla lagaskyldu um varðveislu persónuupplýsinga samkvæmt Evrópusambandslöggjöf eða þeim landslögum aðildarríkis sem ábyrgðaraðili heyrir undir; landslög aðildarríkis skulu hafa almannahagsmuni að leiðarljósi, virða **kjarna** réttarins til verndar persónuupplýsinga og gæta meðalhófs við að uppfylla þann lögmæta tilgang og markmið sem þeim er ætlað að ná.	(d) til að uppfylla lagaskyldu um varðveislu persónuupplýsinga samkvæmt Evrópusambandslöggjöf eða þeim landslögum aðildarríkis sem ábyrgðaraðili heyrir undir; landslög aðildarríkis skulu hafa almannahagsmuni að leiðarljósi, virða réttinn til verndar persónuupplýsinga og gæta meðalhófs við að uppfylla þann lögmæta tilgang og markmið sem þeim er ætlað að ná.
(e) í þeim málum sem vísað er til í 4. mgr.	(e) í þeim málum sem vísað er til í 4. mgr.
4. Í stað afmáunar skal ábyrgðaraðili takmarka vinnslu persónuupplýsinga þegar:	4. Í stað afmáunar skal ábyrgðaraðili takmarka vinnslu persónuupplýsinga ***þannig að ekki sé***

	veittur aðgangur að þeim eða unnið með þær á almennan hátt og að ekki sé hægt að breyta þeim frekar, þegar:
(a) hinn skráði vefengir nákvæmni þeirra, í ákveðinn tíma á meðan ábyrgðaraðili kannar og staðfestir nákvæmni upplýsinganna;	(a) hinn skráði vefengir nákvæmni þeirra, í ákveðinn tíma á meðan ábyrgðaraðili kannar og staðfestir nákvæmni upplýsinganna;
(b) ábyrgðaraðilinn þarfnast upplýsinganna ekki lengur til að ljúka því verkefni sem unnið er að en upplýsingarnar þarf að varðveita til sönnunar;	(b) ábyrgðaraðilinn þarfnast upplýsinganna ekki lengur til að ljúka því verkefni sem unnið er að en upplýsingarnar þarf að varðveita til sönnunar;
(c) vinnsla upplýsinga er ólögmæt og hinn skráði mótmælir því að þær verði afmáðar en krefst takmörkunar á notkun þeirra í staðinn;	(c) vinnsla upplýsinga er ólögmæt og hinn skráði mótmælir því að þær verði afmáðar en krefst takmörkunar á notkun þeirra í staðinn;
	(ca) dómstóll eða eftirlitsyfirvald, með staðfestu í Sambandinu, hefur kveðið upp endanlegan úrskurð þess efnis að takmarka eigi notkun viðkomandi upplýsinga.
(d) hinn skráði krefst þess að fá að flytja persónuupplýsingar sínar yfir í annað netþjónustukerfi í samræmi við **2. mgr. 18. gr.**	(d) hinn skráði krefst þess að fá að flytja persónuupplýsingar sínar yfir í annað netþjónustukerfi í samræmi við a-lið 2. mgr. 15. gr.;
	(da) ákveðin tegun varðveislutækni heimilar ekki eyðingu og var innleidd áður en reglugerð þessi tók gildi.
5. Persónuupplýsingar sem vísað er til í 4. mgr. má, með undantekningu um geymslu þeirra, einungis vinna í sönnunarskyni eða með samþykki hins skráða, eða til verndar réttindum annarrar náttúrulegrar persónu eða lögaðila eða í þágu almannahagsmuna.	5. Persónuupplýsingar sem vísað er til í 4. mgr. má, með undantekningu um geymslu þeirra, einungis vinna í sönnunarskyni eða með samþykki hins skráða, eða til verndar réttindum annarrar náttúrulegrar persónu eða lögaðila eða í þágu almannahagsmuna.
6. Þegar vinnsla persónuupplýsinga er takmörkuð í samræmi við 4. mgr. skal ábyrgðaraðili tilkynna hinum skráða fyrirfram um að til standi að aflétta takmörkun á vinnslu upplýsinga.	6. Þegar vinnsla persónuupplýsinga er takmörkuð í samræmi við 4. mgr. skal ábyrgðaraðili tilkynna hinum skráða fyrirfram um að til standi að aflétta takmörkun á vinnslu upplýsinga.
7. **Ábyrgðaraðili skal innleiða ferla til að tryggja að tímatakmörkunum, sem settar hafa verið um eyðingu persónuupplýsinga og/eða til reglubundinnar endurskoðunar á nauðsyn þess að geyma upplýsingarnar, sé fylgt.**	
8. Þegar eyðing fer fram skal ábyrgðaraðilinn ekki vinna viðkomandi persónuupplýsingar á annan hátt.	8. Þegar eyðing fer fram skal ábyrgðaraðilinn ekki vinna viðkomandi persónuupplýsingar á annan hátt.
	8a. Ábyrgðaraðili skal innleiða tækniferla til að tryggja að tímamörk varðandi eyðingu

	persónuupplýsinga séu virt og/eða til að tryggja reglubundna endurskoðun þess hvort varðveisla upplýsinganna sé nauðsynleg.
9. Framkvæmdastjórninni er heimilt að setja frekari reglur í samræmi við 86. gr. til þess að útfæra nánar:	9. Framkvæmdastjórninni er heimilt***, eftir að hafa óskað eftir áliti Evrópsku Persónuverndar-stjórnarinnar (European Data Protection Board)*** að setja frekari reglur í samræmi við 86. gr. til þess að útfæra nánar:
(a) viðmið og kröfur varðandi beitingu 1. mgr. fyrir ákveðna geira og í ákveðnum aðstæðum þar sem unnið er með persónuupplýsingar.;	(a) viðmið og kröfur varðandi beitingu 1. mgr. fyrir ákveðna geira og í ákveðnum aðstæðum þar sem unnið er með persónuupplýsingar.;
(b) skilyrði fyrir að eyða hlekkjum eða afritum persónuupplýsinga af samskiptaþjónustum sem opnar eru almenningi, eins og vísað er til í 2. mgr.;	(b) skilyrði fyrir að eyða hlekkjum eða afritum persónuupplýsinga af samskiptaþjónustum sem opnar eru almenningi, eins og vísað er til í 2. mgr.;
(c) viðmið og skilyrði fyrir að takmarka vinnslu persónuupplýsinga sem vísað er til í 4. mgr.	(c) viðmið og skilyrði fyrir að takmarka vinnslu persónuupplýsinga sem vísað er til í 4. mgr.

Hér á eftir verður farið nánar yfir þær breytingar sem lagðar voru til í Albrecht-skýrslunum frá 17. desember 2012[168] og 16. janúar 2013[169] um réttinn til að gleymast og til afmáunar, breytingatillögur LIBE-þingnefndarinnar[170] og þær breytingar sem samþykktar voru af Evrópuþinginu 12. mars 2014.[171]

---

168 Jan Philipp Albrecht, „Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ (European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 17. desember 2012), hér eftir Albrecht-skýrslan frá 2012. <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf> skoðað 2. apríl 2014.

169 Jan Philipp Albrecht, „Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ (European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 16. janúar 2013), hér eftir Albrecht-skýrslan frá 2013. <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Data%20Protection%20Reform/13-01-16_Albrecht_draft_report.pdf> skoðað 2. apríl 2014.

170 Jan Philipp Albrecht „Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“, amendments tabled in committee (European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 6. mars 2013), hér eftir breytingatillögur LIBE-nefndarinnar frá 2013. <www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE506.147> skoðað 20. apríl 2014.

171 „Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ (*European Parliament*, 12. mars 2014) <www.europarl.europa.eu/oeil/popups/summary.do?id=1342337&t=d&l=en> skoðað 20. apríl 2014.

4.6.1 Yfirskrift 17. gr.

Í upphaflegu reglugerðardrögunum frá 25. janúar 2012 var ákvæðið nefnt *réttur til að gleymast og til afmáunar*. Frumvarpið tók breytingum í meðförum þingsins og var heiti ákvæðisins stytt í *réttur til afmáunar*. Tillaga að þessari breytingu kom úr ýmsum áttum, þar á meðal frá meðlimum LIBE-nefndarinnar, nefnd um innri markaðinn og neytendavernd og iðnaðar-, rannsókna- og orkumálanefnd. Í skýringum með breytingunum segja álitsgjafar að yfirskriftin *rétturinn til að gleymast* sé villandi.[172] Réttur til að gleymast sé ekki tryggður í reglugerðinni. Með því að nota það hugtak sé réttindum lofað sem einstaklingar hafi í raun ekki. Réttur til afmáunar verði að vera eins ríkur og hægt er en taka mið af hugsanlegum erfiðleikum tengdum því að afmá upplýsingar af netinu. Styrkja þurfi réttinn til afmáunar í stað þess að lofa einstaklingum réttindum sem ekki séu fyrir hendi, með villandi yfirskrift ákvæðisins.[173]

4.6.2 Ákvæði 1. mgr. 17. gr.

4.6.2.1 Vernd barna

Í 1. mgr. var fellt út úr textanum ákvæði sem vísaði sérstaklega til persónuupplýsinga sem börn hafa birt á netinu. Vivian Reding, aðstoðarframkvæmdastjóri ESB, hafði áður talað fyrir því að rétturinn til að gleymast og til afmáunar snerist ekki hvað síst um vernd barna. Börn átti sig ekki á þeirri hættu sem því geti fylgt að birta alls kyns persónuupplýsingar á netinu. Í slíkum aðstæðum þurfi fólk að eiga þess kost að fá upplýsingum eytt af netinu, kjósi það svo. Í Albrecht-skýrslunni frá 2012 er breytingin réttlætt með því að réttur til afmáunar eigi að gilda um alla jafnt. Það að vísa sérstaklega til verndar barna mætti skilja svo að rétti fullorðinna einstaklinga væru takmörk sett.[174]

4.6.2.2 Aðrar breytingar í 1. mgr.

Evrópuþingið jók við rétt hins skráða með heimild til að fara fram á að þriðji aðili afmái hlekki á gögn eða afrit þeirra í 1. mgr. Tekið var út víðtækt ákvæði d-liðar 1. mgr. um að hinn skráði eigi rétt á að fá upplýsingum eytt þegar vinnsla þeirra samræmist ekki

[172] Lara Comi, „Opinion on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ (European Parliament, Internal Market and Consumer Protection, 28. janúar 2013), leiðréttingar 1380-1383.
<www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE496.497&secondRef=02> skoðað 2. apríl 2014.
[173] Breytingatillögur LIBE-nefndarinnar (n. 170) nr. 1380-1383.
[174] Albrecht-skýrslan frá 2012 (n. 168).

ákvæðum reglugerðarinnar af öðrum ástæðum. Þess í stað var réttur hins skráða styrktur með þeim hætti að gera þriðju aðilum skylt, að beiðni hins skráða, að eyða öllum tenglum, afritum og endurgerðum af upplýsingum þegar eitt af eftirfarandi atriðum á við:

- dómur eða eftirlitsyfirvald með staðfestu í Sambandinu hefur kveðið upp endanlegan dóm eða úrskurð um að viðkomandi persónuupplýsingum skuli eytt
- unnið hefur verið með upplýsingarnar með ólögmætum hætti.[175]

Þá var bætt við öryggisákvæði í málsgrein 1a) þess efnis að beiting 1. mgr. skuli einungis eiga við ef ábyrgðaraðili fái staðfest að sá sem óski eftir afmáun upplýsinga sé í raun hinn skráði. Þannig er tryggt að engir aðrir en hinn skráði geti farið fram á eyðingu upplýsinganna, eins og útskýrt er í Albrecht-skýrslunni.[176]

4.6.3 Ákvæði 2. mgr. 17. gr: Vinnsla þriðju aðila

Samkvæmt 12. gr. núgildandi tilskipunar getur hinn skráði farið þess á leit við ábyrgðaraðila að hann tilkynni þriðju aðilum, sem fengið hafa upplýsingarnar áframsendar, um allar leiðréttingar, afmáanir eða aðgangstakmarkanir sem farið hafa fram í samræmi við b-lið 12. gr., „nema það sé ekki unnt eða kosti óhóflega fyrirhöfn.“[177]

Eðli internetsins; það hversu auðvelt er að áframsenda og endurbirta upplýsingar í einu vetfangi, gerði þetta ákvæði erfitt í framkvæmd. Í reglugerðardrögunum er gerð tilraun til að taka á þessu vandamáli, með því að leggja ábyrgðaraðilum ríkari skyldur á herðar í tengslum við vinnslu þriðju aðila. Í 2. mgr. 17. gr. draganna sagði að þegar ábyrgðaraðili hafi gert persónuupplýsingar opinberar eigi hann að stíga öll raunhæf skref:

> þar á meðal tæknileg skref, tengdar þeim upplýsingum sem hann ber ábyrgð á að birta, til að upplýsa þriðju aðila, sem vinna slík gögn, um að hinn skráði óski eftir því að þeir afmái alla tengla að þeim persónuupplýsingum eða afritum af þeim. Þegar ábyrgðaraðilinn hefur gefið þriðja aðila leyfi til að birta persónuupplýsingar telst ábyrgðaraðilinn bera ábyrgð á þeirri birtingu.[178]

Með ákvæði 2. mgr. 17. gr. var gengið lengra en í núgildandi tilskipun þar sem tilkynningarskylda ábyrgðaraðila til þriðju aðila kviknar sjálfkrafa þegar réttur til

[175] European Parliament (n. 19).
[176] Albrecht-skýrslan frá 2013 (n. 169).
[177] Tilskipun 95/46/EB (n. 7), c-liður 12. gr.
[178] Reglugerðardrög framkvæmdastjórnarinnar (n. 6), 2. mgr. 17. gr.

afmáunar er virkjaður og ábyrgðaraðilinn telst þar að auki ábyrgur fyrir birtingu þriðju aðila.

Eftir breytingar Evrópuþingsins á 2. mgr. 17. gr. var ákvæði um ábyrgð ábyrgðaraðila á vinnslu þriðju aðila tekið út. Nú segir í ákvæðinu að þegar ábyrgðaraðili hefur gert persónuupplýsingar opinberar, án þess að réttlætanlegar ástæður séu fyrir hendi (sbr. 1. mgr. 6. gr.), skuli hann stíga öll raunhæf skref til að afmá upplýsingarnar, þar á meðal til að þær verði afmáðar af þriðju aðilum. Í upphaflegu drögunum var einungis gerð sú krafa að ábyrgðaraðili stigi hin raunhæfu skref til að *upplýsa* þriðju aðila um að hinn skráði óski eftir að upplýsingarnar og afrit þeirra verði afmáð.[179]

Þá segir í ákvæðinu, eftir breytingar Evrópuþingsins, að ábyrgðaraðili skuli jafnframt upplýsa hinn skráða, þegar mögulegt er, um þær aðgerðir sem viðkomandi þriðju aðilar hafi gripið til.

Í skýrslu umsagnaraðila frá 6. mars 2013, sem unnin var fyrir Evrópuþingið, kemur fram að margir þeirra vildu að ákvæði 2. mgr. 17. gr. yrði alfarið fellt út úr reglugerðinni. Í skýringum við breytingartillögur þeirra segir meðal annars: „*Þegar horft er til eðlis internetsins og hversu auðvelt er að birta upplýsingar á ýmsum vefsíðum um allan heim er þetta ákvæði óframkvæmanlegt*.“[180] Evrópuþingið ákvað hins vegar að halda ákvæðinu inni en breyta því með þeim hætti sem að framan greinir.

Ákvæði 1. og 2. mgr. 17. gr., eftir breytingar LIBE-þingnefndarinnar og Evrópuþingsins, virðist því að mörgu leyti leggja ábyrgðaraðilum meiri skyldur á herðar og færa hinum skráða meiri rétt en upphaflegu ákvæðin í tillögum framkvæmdastjórnar ESB.

4.7 Takmarkanir og undanþágur

Undantekningar frá gildissviði tilskipunar 95/46/EB og reglugerðardrögum framkvæmdastjórnarinnar eru nokkrar. Hið sama á við um lög nr. 77/2000, eðli málsins samkvæmt. Sem dæmi ná reglur tilskipunarinnar ekki yfir vinnslu þjóðaröryggisstofnana á persónuupplýsingum og heldur ekki vinnslu fjölmiðla á slíkum upplýsingum, sé fréttamennska tilgangur vinnslunnar.

[179] Albrecht-skýrslan frá 2012 (n. 168), nr. 147.

[180] Seán Kelly, „Opinion of the Committe on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs“ (European Parliament, Committee on Industry, Research and Energy, 26. febrúar 2013), nr. 162 <www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-496.562+02+DOC+PDF+V0//EN&language=EN> skoðað 3. apríl 2014.

Undantekningar frá efnislegu gildissviði pul. eru taldar upp í 2. mgr. 3. gr. pul., þar sem segir að ákvæði 16., 18.-21., 24., 26., 31. og 32. gr. laganna gildi ekki um vinnslu persónuupplýsinga sem varði almannaöryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu.

Þá gilda tilskipun 95/46/EB og lög nr. 77/2000 heldur ekki um meðferð einstaklings á persónuupplýsingum sem eingöngu varða einkahagi hans eða eru einvörðungu ætlaðar til persónulegra nota. Ákveðin óvissa ríkir um það hvar mörk þessara undantekninga liggja nákvæmlega, þótt dómstólar hafi að einhverju leyti skilgreint þau á síðustu árum, sbr. Lindqvist-málið.[181]

4.7.1 Undanþágur 3. mgr. 17. gr.

Áþekk undanþáguákvæði og er að finna í 9. gr. tilskipunar 95/46/EB eru nú í 3. mgr. 17. gr. reglugerðardraga framkvæmdastjórnarinnar. Jafnvel þótt reglugerðardrögin styrki og auki réttindi hins skráða eru í 3. mgr. viðurkennd takmörk fyrir því að gengið sé á andstæð réttindi og hagsmuni. Hvað réttinn til að gleymast varðar sérstaklega er gert ráð fyrir að ákveðnar undanþágur frá þeim rétti verði lögfestar.

Í 3. mgr. 17. gr. reglugerðadraga framkvæmdastjórnarinnar frá 2012 segir að þar sem réttur til að gleymast sé fyrir hendi verði að afmá upplýsingarnar án tafar, nema þegar varðveisla gagnanna sé nauðsynleg á grundvelli einnar af tilteknum undantekningum. Ábyrgðaraðila er heimilt að varðveita persónuupplýsingar áfram sé það nauðsynlegt vegna:

- *réttar til tjáningarfrelsis*, sbr. 80. gr. reglugerðardraganna. Í 80. gr. er kveðið á um skyldu aðildarríkja til að koma á fót takmörkunum til verndar vinnslu persónuupplýsinga sem fer „eingöngu fram vegna fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi.“
- *almannahagsmuna á sviði lýðheilsu*, sbr. 81. gr. Í 81. gr. er kveðið á um að ESB eða aðildarríki þess geri ráðstafanir til að vernda lögmæta hagsmuni hins skráða á sviði lýðheilsu.
- *sagnfræðilegra, tölfræðilegra eða vísindalegra rannsóknarhagsmuna*, sbr. 83. gr. Í 83. gr. segir að vinnsla persónuupplýsinga í þeim tilgangi sé aðeins heimil ef ekki er hægt að vinna að þessum tilteknu rannsóknarhagsmunum með því að vinna nafnlausar eða ópersónugreinanlegar upplýsingar; og

[181] C-101/01 *Lindqvist* (n. 59).

- *skyldu til að uppfylla lagakröfu um varðveislu persónuupplýsinga samkvæmt Evrópusambandslöggjöf eða þeim landslögum aðildarríkis sem ábyrgðaraðili heyrir undir.* Tekið er fram að landslög aðildarríkis skulu hafa almannahagsmuni að leiðarljósi, virða kjarna réttarins til verndar persónuupplýsinga og gæta meðalhófs við að uppfylla þann lögmæta tilgang og markmið sem þeim sé ætlað að ná.

Helsta breytingin sem gerð var á framangreindum undanþágum í Albrecht-skýrslunni var sú að undanþágur frá réttinum í 17. gr. voru víkkaðar út. Í drögum framkvæmdastjórnarinnar sneru undanþágur vegna tjáningarfrelsis eingöngu að fréttamennsku og bókmenntalegri eða listrænni starfsemi, sbr. tilvísun í 80. gr. reglugerðardraganna. Í Albrecht-skýrslunni er lagt til að breyta 80. gr. með þeim hætti að í stað þess að takmarka undanþágur tengdar tjáningarfrelsi við fréttamennsku og bókmenntalega eða listræna starfsemi skuli veita undanþágur vegna tjáningarfrelsis „og sérstakra aðstæðna við vinnslu upplýsinga, sbr. kafla 9, hvenær sem nauðsynlegt er“ til að samræma rétt til verndar persónuupplýsinga og reglur sem vernda tjáningarfrelsi.

Fyrir utan sérgreindar undanþágur frá réttinum til að gleymast og til afmáunar er ákvæði í 21. gr. reglugerðardraganna sem heimilar ESB og aðildarríkjum að takmarka með lögum umfang tiltekinna réttinda og skyldna í reglugerðinni, þegar nauðsyn ber til og meðalhófs er gætt, svo standa megi vörð um réttindi og hagsmuni, eins og almannaöryggi, baráttu gegn glæpum og fleiru. Í umsögn um reglugerðardrögin benti embætti Yfirmanns persónuverndarmála í Evrópu (EDPS) á að almennar undanþágur 21. gr. og undanþága d-liðar 3. mgr. 17. gr. væru af sama bergi brotnar. Í d-lið 3. mgr. 17. gr. er heimild til að láta landslög trompa réttinn til að gleymast ef fyrir hendi er lagaleg skylda til að varðveita persónuupplýsingar, að því skilyrði uppfylltu að landslög hafi almannahagsmuni að leiðarljósi, virði réttinn til verndar persónuupplýsinga og gæti meðalhófs við að uppfylla þann lögmæta tilgang og markmið sem lögunum er ætlað að ná. [182] Í Albrecht-skýrslunni er minnst á að undantekningar 3. mgr. 17. gr. séu endurtekning á ákvæði 21. gr. og þannig gefið í skyn að 3. mgr. sé óþörf. Hins vegar bendir Lindsay á það í grein sinni að sá munur sé á 3. mgr. 17. gr. og 21. gr. að á meðan

[182] European Data Protection Supervisor, „Stellungnahme des Europäischen Datenschutzbeauftragten zum Datenschutzreformpaket“ (Brussel 7. mars 2012), mgr. 66-67, 149 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf> skoðað 2. apríl 2014; David Lindsay (n. 85), 66%.

undanþágur 3. mgr. 17. gr. takmarki réttinn til að gleymast veiti 21. gr. aðildarríkjum aðeins heimild til takmarkana.

4.8 Samfélagsmiðlar og „heimilishaldsundantekningin“

Í 2. tl. 3. gr. núgildandi tilskipunar 95/46/EB segir að lögin gildi ekki um vinnslu persónuupplýsinga af hálfu einstaklings sé vinnslan hluti af starfsemi sem eingöngu er í þágu hans sjálfs eða fjölskyldu hans. Ákvæðið var innleitt með 2. mgr. 3. gr. pul. þar sem segir að lögin gildi ekki um meðferð einstaklings á persónuupplýsingum sem eingöngu varða einkahagi hans eða eru einvörðungu séu ætlaðar til persónulegra nota. Í d-lið 2. mgr. 2. gr. reglugerðardraga framkvæmdastjórnarinnar er efnislega samhljóða ákvæði.

ESB-dómstóllinn hefur að nokkru skýrt hvað fellur undir þessa svokölluðu heimilishaldsundantekningu í máli C-101/01 (*Bodil Lindqvist*)[183] þar sem dómstóllinn taldi það flokkast undir rafræna vinnslu persónuupplýsinga þegar einstaklingur birti persónuupplýsingar um aðra á heimasíðu sinni á Netinu; nöfn samstarfsmanna, símaúmer og áhugamál. Málavextir voru þeir að Bodil, kirkjurækin kona, hafði birt upplýsingar á vefsíðu sinni sem áttu að hjálpa öðrum sóknarbörnum kirkjunnar við fermingarundirbúning. Á vefsíðunni birti hún spaugilegar persónuupplýsingar og í einhverjum tilfellum upplýsingar um fjölskylduaðstæður og símanúmer. Bodil var í undirrétti dæmd til sektargreiðslu fyrir vinnslu persónuupplýsinga og flutning persónuupplýsinga til þriðja lands í heimildarleysi, svo og fyrir vinnslu viðkvæmra persónuupplýsinga. Hún áfrýjaði dómnum til Hæstaréttar Svíþjóðar, sem leitaði álits Evrópudómstólsins. Niðurstaða hans var að sú athöfn að birta á netinu persónuupplýsingar, myndir eða myndbönd af öðrum, án samþykkis þeirra sem upplýsingarnar vörðuðu, færi í bága við sænsk persónuverndarlög, sem byggðu á tilskipun 95/46/EB. Af dómnum mátti ráða að heimilishaldsundantekningin frá gildissviði laganna, þ.e. undantekning vegna vinnslu upplýsinga til persónulegra nota, á ekki við þegar upplýsingar eru birtar opinberlega, án samþykkis, á vefsíðum á netinu.

Með tilkomu samfélagsmiðla, eins og facebook, er málið hins vegar ekki lengur jafneinfalt og í máli Bodil Lindqvist. Mörkin milli heimilis og opinbers vettvangs eru mun óljósari en áður og sömuleiðis mörkin milli upplýsinga sem einstaklingar setja fram í markaðs- og atvinnuskyni og þeirra sem ekki eru settar fram í þeim tilgangi. Á

[183] C-101/01 *Lindqvist* (n. 59).

facebook og fleiri síðum auglýsa einstaklingar heimilisvarning, eins og fatnað, hjól, húsgögn og heimilisframleiðslu til sölu, ýmist á sérstökum sölusíðum, eins og facebook eða bland.is, eða á sínum persónulegu heimasíðum á samskiptamiðlum. Þar geta einstaklingar einnig birt efni þannig að það sé ýmist aðgengilegt öllum („opinbert“) eða breytt notendastillingum þannig að efnið sé einungis aðgengilegt tilteknum hópum einstaklinga („vinum“ eða „vinum vina“).

Ekki er fullkomlega ljóst af reglugerðardrögum framkvæmdastjórnar ESB hvort og hvernig notkun samfélagsmiðla fellur undir heimilishaldsundantekninguna í d-lið 2. mgr. 2. gr. Takmarkaða vísbendingu er að finna í 15. lið inngangsorða reglugerðardraganna en þar segir:

> Reglugerð þessi skal ekki taka til vinnslu persónuupplýsinga sem framkvæmd er af hálfu einstaklings sé vinnslan hluti af starfsemi sem er einungis í þágu hans sjálfs eða heimilis, eins og samskipti með heimilisföng og varðveisla heimilisfanga, og fer ekki fram í nokkrum hagnaðartilgangi og tengist þar af leiðandi ekki atvinnu- eða markaðsstarfsemi. Undantekningin tekur jafnframt ekki til ábyrgðaraðila eða vinnsluaðila sem útvega þær aðferðir sem notaðar eru til að vinna persónuupplýsingar fyrir starfsemi sem eingöngu fer fram í þágu einstaklings eða heimilishalds hans.[184]

Ekki er tekið fram hvort heimilishaldsundantekningin gildi um vinnslu persónuupplýsinga sem framkvæmd er af hálfu einstaklinga á samfélagsmiðlum eða hvort einstaklingurinn sem birtir efni á netinu teljist í slíkum tilfellum ábyrgðaraðili, sbr. Lindqvist málið. Fræðimaðurinn David Lindsay telur að orðalagið *„og fer ekki fram í nokkrum hagnaðartilgangi og tengist þar af leiðandi ekki atvinnu- eða markaðsstarfsemi“* bendi til þess að undantekningin eigi ekki við þegar athafnir einstaklings á samfélagsmiðlum hafa markaðslegan tilgang, eins og sala einkamuna á facebook.[185] Af framangreindum orðum er þó ljóst að undantekningunni er ekki ætlað að eiga við um fyrirtækin sem reka samskiptamiðlana sjálfa.

Enn á þó eftir að skera úr um það hvort notkun samfélagsmiðla flokkist undir að vera einungis í þágu einstaklingsins sem þá notar og heimilis hans.

Í þessu sambandi má vísa til álits 29. gr. starfshóps ESB frá árinu 2009 þar sem fjallað var um samfélagsmiðla á netinu út frá heimilishaldsundantekningunni. Starfshópurinn komst að þeirri niðurstöðu að þótt heimilishaldsundantekningin ætti almennt við um einstaka notendur samfélagsmiðla þá ætti hún ekki við í eftirtöldum kringumstæðum:

---

[184] Reglugerðardrög framkvæmdastjórnarinnar (n. 6), 15. liður inngangsorða.
[185] David Lindsay (n. 85) 66%.

1. Þegar einstaklingur birtir efni í þágu fyrirtækis eða stofnunar - eða notar samfélagsmiðla til að koma pólitískum skoðunum á framfæri eða auglýsa góðgerðarstarfsemi.
2. Þegar aðgangur að notendaupplýsingum („prófíl“) er ekki bara opinn vinum notandans, heldur opinber. Sé notandi með óvenju marga vini á vinalista, þ.e. með snertiflöt við óvenju marga þriðju aðila, gæti það einnig þýtt að undantekningin ætti ekki við.[186]

Segja má að niðurstaða 29. gr. starfshópsins um að sumar athafnir einstakra notenda samfélagsmiðla rúmist ekki innan heimilishaldsundantekningarinnar sé í samræmi við þá niðurstöðu Evrópudómstólsins í Lindqvist-málinu sem fyrr var reifuð.

4.8.1 Albrecht-skýrslan um heimilishaldsundantekninguna

Í Albrecht-skýrslu Evrópuþingsins er fjallað um það hvenær athafnir einstaklinga eru annað hvort of „markaðslegar“ eða of „opinberar“ til að heimilishaldsundantekningin geti átt við. Í skýrslunni er lagt til að um þetta verði fjallað í inngangsorðum frekar en í reglugerðinni sjálfri.[187] Þá er í skýrslunni lagt til að 15. gr. inngangsorðanna verði endurrituð með eftirfarandi hætti:

> Undantekningin skal ekki eiga við þegar vinnsla persónuupplýsinga fer fram í atvinnulegum eða markaðslegum tilgangi. Taka skal tillit til eðlis persónuupplýsinganna sem unnið er með og hvort aðgangur að þeim er bundinn við tiltekinn eða ótakmarkaðan hóp einstaklinga við mat á því hvort undantekningin eigi við um vinnslu upplýsinganna.[188]

Í útskýringum er breytingin skýrð svo að vinnsla persónuupplýsinga, sem framkvæmd er af hálfu einstaklings í þágu hans sjálfs eða heimilishalds, geti stundum farið fram í þeim tilgangi að hagnast (til dæmis þegar einkamunir séu seldir öðrum einstaklingum) en ættu engu að síður að falla utan gildissviðs reglugerðarinnar, svo lengi sem ekki sé um atvinnu- eða markaðsstarfsemi að ræða.[189]

[186] „Opinion 5/2009 on online social networking“ (Article 29 Data Protection Working Party, 12. júní 2009) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf> skoðað 2. apríl 2014.
[187] Albrect-skýrslan frá 2012 (n. 168); nr. 8, 79; David Lindsay (n. 85) 66%.
[188] Sama heimild.
[189] Sama heimild.

Niðurstaða Evrópuþingsins 12. mars sl. var sú að einfalda orðalag d-liðar 2. mgr. 2. gr. og taka setningarhlutann um atvinnu- og markaðsstarfsemi út:

d-liður 2. mgr. 2. gr. reglugerðar-draga framkvæmdastjórnar ESB, 25. janúar 2012[190]	**d-liður 2. mgr. 2. gr. eftir breytingar Evrópuþingsins 12. mars 2014**[191]
(d) af hálfu einstaklings **án nokkurs hagnaðartilgangs** sé vinnslan hluti af eigin starfsemi sem eingöngu er í þágu hans sjálfs eða athafna sem teljast til heimilishalds	(d) af hálfu einstaklings sé vinnslan hluti af starfsemi sem eingöngu er í þágu hans sjálfs eða athafna sem teljast til heimilishalds. **Þessi undantekning gildir einnig um birtingu persónuupplýsinga þar sem gera má ráð fyrir að einungis takmarkaður hópur hafi aðgang að upplýsingunum.**

Breytingar Evrópuþingsins renna stoðum undir túlkun 29. gr. starfshópsins um að fjöldi vina og friðhelgisstillingar á samfélagsmiðlum skipti máli hvað umfang heimilishaldsundantekningarinnar varðar. Einnig benda þær til að einstaklingar geti fallið undir undantekninguna, þótt þeir noti samfélagsmiðla í hagnaðartilgangi, eins og til að selja heimilismuni og fatnað, svo lengi sem salan fer ekki fram í atvinnuskyni.

4.9 Ábyrgðaraðilar: Hverjum ber að eyða upplýsingunum?

Í ákvæðum 25. og 26. gr. laga pul. kemur fram að kröfum um leiðréttingu, afmáun, aðgangstakmarkanir eða tilkynningar til þriðju aðila um framangreint, skuli beina til ábyrgðaraðila en í frumvarpi til laganna segir að þegar ágreiningur verður milli hins skráða og ábyrgðaraðila um hvort grundvöllur sé fyrir eyðingu upplýsinga eða banni við notkun þeirra sé það hlutverk Persónuverndar að skera úr þeim ágreiningi.

Þegar og ef fyrir liggur að einstaklingur eigi rétt til afmáunar tiltekinna persónuupplýsinga af netinu liggur beinast við að spyrja: Hverjum ber að afmá þessar upplýsingar? Það er að segja: Hver er ábyrgðaraðili, lögum samkvæmt?

Í sumum tilfellum liggur þetta ljóst fyrir. Í öðrum tilfellum ekki. Til dæmis er ekki skýrt hvort einstaklingur telst vera ábyrgðaraðili þegar hann setur efni inn á facebook síðu sína eða hvort hann fellur undir heimilishaldsundantekninguna, sbr. umfjöllun hér að framan. Ekki er heldur ljóst hvaða reglur gilda um einstaklinga sem birta efni á vefsíðum þriðju aðila. Þá hefur verið deilt um hvort Google fyrirtækið telst vera ábyrgðaraðili gagnvart þeim upplýsingum sem finna má með aðstoð leitarvéla þess. Um niðurstöðu Evrópudómstólnum í áðurnefndu prófmáli Google Spain og Google Inc.

[190] Reglugerðardrög framkvæmdastjórnarinnar (n. 6), d-liður 2. mgr. 2. gr.
[191] European Parliament (n. 167), d-liður 2. mgr. 2. gr.

gegn spænsku Persónuverndarstofunni og Mario Costeja González, er fjallað í kafla 4.9.1 hér á eftir.

Hugtakið ábyrgðaraðili er skilgreint í 4. tl. 1. mgr. 2. gr. pul: *Sá aðili sem ákveður tilgang vinnslu persónuupplýsinga, þann búnað sem notaður er, aðferð við vinnsluna og aðra ráðstöfun upplýsinganna.*

Í reglugerðardrögum framkvæmdastjórnarinnar er skilgreining sama hugtaks í 5. mgr. 4. gr. nánast samhljóða sams konar skilgreiningu í tilskipun 95/46/EB:

> Einstaklingur eða lögpersóna, opinbert yfirvald, stofnun eða annar aðili sem ákveður, einn og sér eða í samvinnu við aðra, markmið, skilyrði og aðferðir við vinnslu persónuupplýsinga. Ef markmið, skilyrði og aðferðir við vinnsluna eru ákveðin í lögum bandalagsins eða lögum aðildarríkja þess er heimilt að tilgreina ábyrgðaraðila eða tilteknar viðmiðanir um útnefningu hans í lögum bandalagsins eða aðildarríkis þess.[192]

Gerður er greinarmunur á hugtökunum ábyrgðaraðili og vinnsluaðili í lögunum, líkt og rakið var í skilgreiningum á hugtökum í 2. kafla. Í áliti 29. gr. starfshópsins frá 2010 kom fram að í nútímavefumhverfi, til dæmis á samfélagsmiðlum, geti verið erfitt að greina á milli hlutverks ábyrgðaraðila og vinnsluaðila.[193]

Í öðru áliti 29. gr. starfshópsins, frá 2009, ályktaði hópurinn eftirfarandi:

- Eigendur samfélagsmiðla, sem bjóða einstaklingum vettvang á netinu til að birta upplýsingar og skiptast á upplýsingum við aðra notendur, eru ábyrgðaraðilar, þar sem þeir ákveða tilgang og aðferðir við vinnslu slíkra upplýsinga; og
- Notendur sem hlaða inn persónuupplýsingum um þriðju aðila á samfélagsmiðlum eru líka ábyrgðaraðilar, að því gefnu að þeir falli ekki undir „heimilishaldsundantekninguna“.[194]

Konarski o.fl. hafa auk þess bent á þá flóknu stöðu sem upp getur komið þegar einstaklingar birta efni, persónuupplýsingar þar með taldar, á vefsíðum sem tilheyra þriðju aðilum. Þótt ályktað verði að slíkir notendur skuli teljast ábyrgðaraðilar þá liggi ekki fyrir hvernig þeir einstaklingar ættu að framfylgja þeim lagaskyldum sem ábyrgðaraðilum eru lagðar á herðar, meðal annars um eyðingu gagna.[195]

---

[192] Reglugerðardrög framkvæmdastjórnarinnar (n. 6), 5. mgr. 4. gr.
[193] David Lindsay (n. 85), 67%; „Opinion 1/2010 on the concepts of „controller“ and „processor““ (Article 29 Data Protection Working Party, 16. febrúar 2010) 2. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> skoðað 29. apríl 2014.
[194] David Lindsay (n. 85), 67%; „Opinion 5/2009 on online social networking“ (Article 29 Data Protection Working Party, 12. júní 2009) 5-6 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf> skoðað 2. apríl 2014.
[195] X. Konarski o.fl. (n. 118).

Lindsay telur niðurstöðu 29. gr. starfshópsins, sem sneri að tilskipun 95/46/EB, einnig eiga við um reglugerðardrög framkvæmdastjórnarinnar. Af því leiði að falli einstaklingar, sem eru notendur samfélagsmiðla, ekki undir heimilishaldsundantekninguna verði litið á þá og samfélagsmiðilinn sem sameiginlega ábyrgðaraðila. Um skiptingu ábyrgðar milli slíkra aðila er fjallað í 24. gr. reglugerðardraganna, þar sem segir að um skiptingu ábyrgðar fari þá eftir samkomulagi. Sem þýðir í raun, samkvæmt Lindsay, að þar sem heimilishaldsundantekningin eigi ekki við, þurfi samfélagsmiðillinn og notandinn að gera samning um skiptingu ábyrgðar á því að upplýsingum verði eytt. Þegar heimilishaldsundantekningin eigi hins vegar við beri samfélagsmiðillinn einn ábyrgð á því að ákvæðum 17. gr. sé framfylgt.[196]

4.9.1 Mál C-131/12 Google Spain SL og Google Inc. gegn spænsku Persónuverndarstofunni og Mario Costeja González

Þann 13. maí síðastliðinn birti Evrópudómstóllinn niðurstöðu sína í prófmáli, sem minnst var á fyrr í þessari ritgerð, *Google Spain*-málinu[197] en þar var deilt um hvort almennur réttur til að gleymast væri fyrir hendi í núgildandi tilskipun 95/46/EB.

Málavextir voru þeir að Spánverjinn Mario Costeja González vildi láta eyða af netinu upplýsingum um fjárnám sem gert var hjá honum fyrir mörgum árum. Fjárnámstilkynningin hafði birst á pappír í blaðinu La Vanguardia árið 1998. Eftir að La Vanguardia skannaði blaðasafn sitt yfir á stafrænt form og birti það á netinu urðu þessar upplýsingar aftur aðgengilegar í gegnum netleitarvélar. González hafði samband við blaðið í nóvember 2009 og benti á að þegar nafn hans og eftirnafn væri slegið inn í leitarvél Google á netinu birtist hlekkur á þessar síður blaðsins. Hann benti jafnframt á að fjárnámsmálinu hefði lokið fyrir mörgum árum og hefði enga þýðingu lengur. Hann bað um að upplýsingarnar yrðu fjarlægðar en blaðið taldi ekki unnt að verða við þeirri beiðni.[198]

Í febrúar 2010 hafði González samband við Google á Spáni og fór fram á að hlekkir á þessar tilteknu síður blaðsins yrðu fjarlægðir úr leitarniðurstöðum tengdum nafni sínu. Google á Spáni áframsendi beiðnina til Google Inc. sem er með skráðar höfuðstöðvar í Kaliforníu í Bandaríkjunum, þar sem síðarnefnda fyrirtækið er ábyrgðaraðili. Í kjölfarið lagði González fram kvörtun til Persónuverndarstofu Spánar gegn útgefanda La Vanguardia og Google. Persónuverndarstofan birti ákvörðun sína 30. júlí 2010 þar sem

[196] David Lindsay (n. 85), 67%.
[197] Mál C-131/12 *Google Spain* (n. 115).
[198] Sama heimild, málsgr. 14, 15 og 16.

hún komst að þeirri niðurstöðu að Google á Spáni og Google Inc. bæri að fjarlægja upplýsingarnar úr leitarniðurstöðum og tryggja að aðgangur að þeim yrði ekki opinn framvegis. Persónuverndarstofan taldi útgefandann hins vegar ekki bera ábyrgð í málinu, þar sem birting upplýsinganna í dagblaðinu hefði verið réttlætanleg, á þeim tíma sem þær birtust. Eftir að Google Inc. og Google á Spáni áfrýjuðu málinu til Hæstaréttar Spánar og kröfðust ógildingar á ákvörðun Persónuverndarstofunnar leitaði Hæstiréttur Spánar forúrskurðar Evrópudómstólsins.[199]

Lögsögumaður Evrópudómstólsins hafði birt álit sitt í júní 2013 þar sem fram kom að hann teldi leitarvélafyrirtæki almennt ekki vera ábyrgðaraðila og að Google þyrfti því ekki að eyða upplýsingum af netinu, þótt þær væru þar í óþökk tiltekinna aðila.[200] Evrópudómstóllinn komst að þveröfugri niðurstöðu í maí 2014 og taldi að leitarvélafyrirtækið Google bæri ábyrgð gagnvart þeim persónupplýsingum sem birtust í leitarniðurstöðum og birtar væru af þriðju aðilum á netinu. Samkvæmt niðurstöðu Evrópudómstólsins getur fólk farið fram á að persónuupplýsingar sem því tengjast verði fjarlægðar úr leitarniðurstöðum.[201] Verði eigendur leitarvéla ekki við slíkum beiðnum geta sömu einstaklingar, að tilteknum skilyrðum uppfylltum, lagt málið fyrir viðeigandi eftirlitsstofnun til að fá hlekkjum á upplýsingarnar eytt.[202]

Evrópudómstóllinn fjallaði í fyrsta lagi um það hvort starfsemi leitarvélafyrirtækja teldist söfnun og vinnsla persónuupplýsinga, í skilningi tilskipunar 95/46/EB. Í dómsniðurstöðum sagði að með því að stunda sjálfvirka, viðvarandi og kerfisbundna leit að upplýsingum sem birtar séu á netinu teldist leitarvélafyrirtæki *safna* upplýsingum í skilningi tilskipunar 95/46/EB. Aukinheldur taldi dómstóllinn að þær aðgerðir leitarvélafyrirtækja að flokka vefsíður sem safnað er, heimta persónuupplýsingar, skrá þær, kerfisbinda og geyma á netþjónum sínum, auk þess að miðla þeim og gera þær aðgengilegar notendum í formi leitarniðurstaðna, væru *vinnsla* persónuupplýsinga í skilningi b-liðar 2. gr. tilskipunarinnar. Dómstóllinn sagði að til þessara aðgerða væri sérstaklega og skilyrðislaust vísað í b-lið 2. gr. tilskipunarinnar og þær teldust vinnsla persónuupplýsinga, óháð því að leitarvélafyrirtækið vinnur

[199] Sama heimild, málsgr. 16, 17, 18, 19 og 20.
[200] Mál C-131/12 *Google Spain SL og Google Inc g. Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* [ECR 13. maí 2014], álit N. Jääskinen, mgr. 138, 2. og 3. tölul.
[201] Mál C-131/12 *Google Spain* (n. 115), mgr. 94 og mgr. 100, 3. tölul.
[202] Sama heimild, mgr. 77.

upplýsingarnar án þess að gera greinarmun á persónuupplýsingum og öðrum upplýsingum.[203]

Evrópudómstóllinn ályktaði einnig að leitarvélafyrirtæki teldist *ábyrgðaraðili* gagnvart framangreindri vinnslu persónuupplýsinga, að því tilskildu að fyrirtækið ákveði markmið og aðferðir við vinnsluna.[204] Það væri andstætt skýru orðalagi tilskipunar 95/46/EB, tilgangi hennar og markmiðum, að undanskilja leitarvélafyrirtæki gildissviði hennar, á þeim grundvelli að fyrirtækin hafi ekki vald yfir persónuupplýsingum sem birtar séu á vefsíðum þriðju aðila.[205]

Í öðru lagi fjallaði dómstóllinn um landfræðilegt gildissvið tilskipunarinnar og sagði að a-liður 1. mgr. 4. gr. tilskipunar 95/46/EB tæki til þess þegar leitarvélafyrirtæki setur upp dótturfélag eða útibú í aðildarríki ESB, sem beinir starfsemi sinni að íbúum aðildarríkisins.[206] Þetta þýðir að fyrirtæki utan Evrópu, sem þjónusta aðildarríki EES, verða að hlíta evrópskri löggjöf um vernd persónuupplýsinga. Þau geta ekki borið fyrir sig að netþjónar þeirra séu staðsettir utan Evrópu og að því eigi evrópsk löggjöf ekki við.

Hvað skyldur ábyrgðaraðila varðar taldi Evrópudómstóllinn að b-lið 12. gr. og a-lið 1. mgr. 14. gr. tilskipunar 95/46/EB beri að túlka svo að leitarvélafyrirtæki eigi, að skilyrðum ákvæðanna fullnægðum, að fjarlægja hlekki á vefsíður sem þriðju aðilar hafi birt, þar sem upplýsingar tengdar einstaklingi sé að finna og sem birtist í leitarniðurstöðum þegar notendur skilyrði leitina við nafn þess einstaklings. Dómstóllinn sagði ljóst að slík skylda leitarvélafyrirtækis geti líka verið fyrir hendi þótt nöfn eða aðrar persónuupplýsingar hafi ekki verið fjarlægðar af viðkomandi vefsíðum og jafnvel, eftir atvikum, þótt birting upplýsinganna á vefsíðunum hafi upphaflega verið lögmæt.[207]

Dómstóllinn benti á að með notkun leitarvéla á netinu geti hver sem er flett upp nafni annars einstaklings og fengið skipulegt yfirlit yfir upplýsingar sem þeim einstaklingi tengjast á netinu. Án leitarvéla hafi netnotendur almennt ekki aðgang að slíku safni persónuupplýsinga á einum stað. Þetta geti falið í sér meiri íhlutun í friðhelgi einkalífs en birting upplýsinganna á vefsíðunum sjálfum. Þetta sé auk þess alvarlegra í ljósi þess mikilvæga hlutverks sem netið og leitarvélar gegni í nútímasamfélagi. Slík íhlutun

[203] Sama heimild, mgr. 28.
[204] Sama heimild, mgr. 33.
[205] Sama heimild, mgr. 34.
[206] Sama heimild, mgr. 60.
[207] Sama heimild, mgr. 94 og mgr. 100, 3. tölul.

verði, að mati dómstólsins, ekki réttlætt eingöngu með þeim fjárhagslegu hagsmunum sem leitarvélafyrirtæki hafi af upplýsingavinnslunni.[208]

Þá segir í forúrskurði Evrópudómstólsins að ef einstaklingur leggur fram beiðni um afmáun hlekkja sem vísa á persónuupplýsingar um hann, og talið sé að tilvísun á hlekkina samræmist ekki ákvæðum tilskipunarinnar á þeim tíma, verði að túlka ákvæði b-liðar 12. gr. og a-liðar 1. mgr. 14. gr. tilskipunar 95/46/EB svo að fjarlægja skuli hlekkina af netinu. Í þessu samhengi segir í niðurstöðu Evrópudómstólsins að jafnvel vinnsla sannra og réttra upplýsinga, sem upphaflega hafi verið lögmætt að birta, geti í tímans rás orðið ósamræmanleg ákvæðum tilskipunarinnar, ef upplýsingarnar virðist ófullnægjandi, óviðeigandi, eða ekki lengur viðeigandi, eða óhóflegar, í ljósi þess tilgangs sem vinnslu þeirra var upphaflega ætlaður og í ljósi þess tíma sem liðið hafi.[209] Dómstóllinn segir ennfremur að þegar eigendum leitarvélafyrirtækja berist slíkar beiðnir um afmáun persónuupplýsinga þurfi þeir að kanna hvort einstaklingurinn sem leggur beiðnina fram eigi rétt á því að viðkomandi upplýsingar, sem tengist honum persónulega, verði ekki lengur tengdar við nafn hans með birtingu þeirra í leitarniðurstöðum, þar sem leit er skilyrt við nafn hans.

> Þar sem hinn skráði á rétt á því, samkvæmt þeim grundvallarréttindum sem felast í 7. og 8. gr. Réttindaskrárinnar, að fara fram á að viðkomandi upplýsingar verði almenningi ekki lengur aðgengilegar í leitarniðurstöðum, trompa þau réttindi almennt ekki eingöngu fjárhagslega hagsmuni leitarvélafyrirtækisins, heldur einnig þá hagsmuni almennings sem felast í því að hafa aðgang að upplýsingunum, með því að skilyrða netleit við nafn hins skráða. Hins vegar ætti þetta ekki við ef svo virtist af ákveðnum ástæðum, eins og því hlutverki sem hinn skráði gegnir á opinberum vettvangi, að brot á þessum grundvallarréttindum mætti réttlæta með þeim ríku hagsmunum sem almenningur hefur af því að hafa aðgang að slíkum upplýsingum í leitarniðurstöðum.[210]

Verði viðkomandi einstaklingur talinn eiga rétt til afmáunar er það sem sagt álit Evrópudómstólsins að ábyrgðaraðila beri að fjarlægja hlekkina úr leitarniðurstöðum, nema sérstakar ástæður séu fyrir því að gera það ekki, svo sem ef viðkomandi einstaklingur telst vera opinber persóna og áhugi almennings á upplýsingunum er þar af leiðandi meiri en ella.[211]

Þá bendir Evrópudómstóllinn á að einstaklingar geti beint beiðni um afmáun slíkra hlekkja úr leitarniðurstöðum beint til leitarvélafyrirtækja (ábyrgðaraðila), sem verði þá

[208] Sama heimild, mgr. 87 og mgr. 100, 4. tölul.
[209] Sama heimild, mgr. 93 og 94.
[210] Sama heimild, mgr. 100, 4. tölul. Íslensk þýðing höfundar.
[211] Sama heimild, mgr. 97 og mgr. 100, 4. tölul.

að leggja sjálfstætt mat á beiðnina og þann grundvöll sem hún byggist á. Synji leitarvélafyrirtækið beiðninni má leggja málið fyrir til þess bæra eftirlitsstofnun eða dómstól sem metur hvort ástæða sé til að skylda ábyrgðaraðila til að grípa til viðeigandi aðgerða.[212]

Niðurstaða Evrópudómstólsins markar tímamót og er að mati höfundar til marks um aukna áherslu á persónuupplýsingavernd og aukið vægi friðhelgi einkalífs á netinu, í Evrópu. Þess má geta að fræðimaðurinn Christopher Kuner hefur vakið athygli á því að ólíklegt sé að ábyrgðaraðilar geti tekist á hendur ákvarðanir byggðar á flóknum lagaskilgreiningum, þar sem vega þarf og meta jafnvægi milli lagalegra réttinda; réttarins til að gleymast og réttinda eins og tjáningarfrelsis, sbr. 3. mgr. 17. gr. Hið sama gildi um ákvarðanir um hvenær eyða skuli gögnum, sbr. 3. mgr. 17. gr. eða hindra aðgang að þeim, sbr. 4. mgr. 17. gr. Ákvæði 17. gr. verði því líklega erfitt í framkvæmd og geti leitt til „kulnunar“ á netnotkun í aðildarríkjum Evrópusambandsins.[213]

4.10 Takmörkun á ábyrgð milligönguaðila: Lög um rafræn viðskipti nr. 30/2002, sbr. tilskipun 2000/31

Í tilskipun um rafræn viðskipti nr. 2000/31 (e. *E-Commerce Directive*)[214] sem var innleidd með lögum um rafræn viðskipti og aðra rafræna þjónustu nr. 30/2002, er að finna reglur um takmörkun á ábyrgð netþjónustuveitenda sem eru milligönguaðilar (e. internet intermediaries). Milligönguaðilar eru til dæmis þjónustuveitendur sem miðla gögnum um fjarskiptanet eða veita aðgang að fjarskiptaneti og þjónustuveitendur sem hýsa gögn. Fyrirtæki sem reka samfélagsmiðla og leitarvélar eru talin til milligönguaðila.[215] Ákvæði 12.-14. gr. tilskipunarinnar voru innleidd með 12.-14. gr. laga nr. 30/2002.

Í 3. mgr. 2. gr. reglugerðardraga framkvæmdastjórnarinnar kemur fram að ábyrgðarreglur 12.-15. gr. tilskipunar 2000/31 gagnvart milligönguaðilum gildi áfram.

---

[212] Sama heimild, mgr. 77.
[213] Christopher Kuner (n. 87) 6.
[214] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1. Hér eftir tilskipun 2000/31/EB.
[215] OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (Organisation for Economic Co-operation and Development 2011) <www.oecd-ilibrary.org/content/book/9789264115644-en> skoðað 29. apríl 2014.

Þar af leiðandi er ábyrgð slíkra aðila takmörkuð og gildir það einnig um réttinn til afmáunar.[216]

Samkvæmt framangreindum ákvæðum bera milligönguaðilar takmarkaða ábyrgð á því að uppfylla kröfur um að fjarlægja gögn eða hindra aðgang að þeim, að tilteknum skilyrðum uppfylltum. Sem dæmi má nefna að þjónustuveitandi ber takmarkaða ábyrgð vegna hýsingar ólögmæts efnis eða upplýsinga, sbr. 1. mgr. 14. gr. laga nr. 30/2002, hafi hann ekki vitneskju um tilvist þeirra gagna. Að öðrum kosti ber hann takmarkaða ábyrgð ef hann fjarlægir gögnin eða hindrar aðgang að þeim án tafar, eftir að hafa fengið vitneskju um barnaklám, efni varið höfundarréttarlögum, eða vitneskju um lögbann við hýsingu gagna eða dóm um brottfellingu eða hindrun aðgangs að þeim.

Nokkurrar óvissu gætir þó um það hvort ábyrgðartakmarkanir tilskipunar 2000/31 eigi við um brot gegn reglum tilskipunar 95/46/EB, eins og Lindsay bendir á í grein sinni.[217] Í b-lið 5. mgr. 1. gr. tilskipunar 2000/31 segir nefnilega að tilskipunin gildi ekki um álitamál sem varði þjónustu í upplýsingasamfélaginu og fjallað sé um í tilskipun 95/46/EB. Því má með góðum rökum halda því fram að ábyrgðartakmarkanirnar eigi ekki við. Á þessu virðist vera tekið í 3. mgr. 2. gr. reglugerðardraganna, sem að framan greinir. Málið flækist hins vegar með 88. gr. reglugerðardraganna, þar sem segir að allar vísanir til tilskipunar 95/46/EB í öðrum lögum skuli breytt í vísanir til reglugerðar þessarar. Hið sama á þá væntanlega við um b-lið 5. mgr. 1. gr. tilskipunar 2000/31.[218]

Af þessum sökum var í Albrecht skýrslunni lagt til að ákvæði 16. gr. innihéldi eftirfarandi texta: *Með reglugerð þessari eru settar reglur fyrir vinnslu persónuupplýsinga, í tilskipun 2000/31/EB eru skilyrði þess að þjónustuveitandi verið talinn ábyrgur fyrir brotum þriðja aðila á lögunum.*[219]

Evrópuþingið gerði hins vegar engar breytingar á 16. gr. reglugerðardraganna í mars sl. og því fékk þessi tillaga ekki hljómgrunn.

4.11 Hverjir geta farið fram á afmáun persónuupplýsinga á grundvelli réttarins til afmáunar?

Ekki hefur ríkt jafnmikil óvissa um það hverjir geta farið fram á eyðingu persónuupplýsinga og það álitaefni hverjir teljist vera ábyrgðaraðilar. Hinn skráði getur farið fram á að upplýsingum um hann verði eytt, sbr. 2. mgr. 26. gr. pul., sbr. 12. gr.

[216] Christopher Kuner (n. 87) 6.
[217] David Lindsay (n. 85) 67%.
[218] David Lindsay (n. 85), 67%.
[219] Sama heimild; Albrecht-skýrslan frá 2013 (n. 169) 12.

tilskipunar 95/46/EB, sbr. einnig ákvörðun Persónuverndar í máli nr. 2011/73 (Tekjubókhald ríkisins). Í 4. tölul. 28. gr. tilskipunar 95/46/EB segir auk þess að öllum aðilum og samtökum fulltrúa þeirra sé heimilt að leggja fram beiðni til eftirlitsyfirvalds um vernd réttinda þeirra og frelsis í tengslum við vinnslu persónuupplýsinga.

Lögaðilar falla ekki undir persónuverndarlög en fyrirtæki hafa þó látið reyna á réttinn til að gleymast fyrir dómstólum. Um það má vísa til máls spænska fyrirtækisins Alfacs Vacances[220] sem á og rekur tjaldstæðið Los Alfaques við strendur Miðjarðarhafs, skammt frá Barcelona. Fyrirtækið fór í mál við spænska Google og krafðist þess að myndir af illa förnum mannslíkum, eftir gassprengingu á svæðinu á áttunda áratugnum, yrðu fjarlægðar úr leitarniðurstöðum fyrir tjaldstæðið. Eigendur tjaldstæðisins töldu myndirnar skaða viðskiptahagsmuni sína, enda tengdust þeir umræddu slysi ekki neitt. Google Spain bar fyrir sig aðildarskort, þar sem ameríska móðurfyrirtækið Google Inc. væri hinn raunverulegi rekstraraðili leitarvélarinnar. Þar sem dómarinn féllst á þau rök kom ekki til þess að leyst yrði úr efnisatriðum málsins.

Nokkur munur er á gildissviði íslensku persónuupplýsingalaganna og tilskipunar 95/46/EB sem haft getur þýðingu um það álitaefni hver geti krafist afmáunar og leiðréttingar: Íslensk persónuupplýsingalög gilda einnig um persónuupplýsingar látinna einstaklinga, sbr. 1. tölul. 1. mgr. 2. gr. pul., og því vaknar sú spurning hvort aðstandendur látins manns geti farið fram á eyðingu persónuupplýsinga hans.

Svarið má meðal annars lesa út úr áliti Persónuverndar frá 2003 *(Umfjöllun um morðmál í dagblaði)*[221] en þar fjallaði Persónuvernd um grein sem birst hafði í dagblaðinu DV og innihélt upplýsingar um einstakling, sem hafði verið myrtur 14 árum áður. Í greininni voru birtar fullyrðingar um aðdraganda morðsins, sem aðstandendur töldu bæði viðkvæmar persónuupplýsingar, skv. 8. tölul. 1. mgr. 2. gr. og að með birtingu þeirra væri brotið gegn 1. og 4. tölul. 1. mgr. 7. gr. pul. og friðhelgi einkalífs hennar látnu og aðstandenda hennar. Persónuvernd taldi að 73. gr. stjskr. og 10. gr. MSE um tjáningarfrelsi hömluðu því ekki að gerð væri krafa til þess að sýna nærfærni í umfjöllun um látinn einstakling.[222] Ljóst væri að gerð og birting umræddrar blaðagreinar gæti verið sérstaklega sársaukafull fyrir aðstandendur og aðra hlutaðeigandi, en tilefni þess að upplýsingar um látna einstaklinga væru skilgreindar

[220] *Alfacs Vacances S.L. g. Google Spain S.L.* Sentencia Juz. 1.ª Inst. Amposta (núm. 1) 32/2012, de 23 de febrero.

[221] *Umfjöllun um morðmál í dagblaði:* Álit Persónuverndar, [dagsetningu vantar] 2003.

[222] Persónuvernd benti jafnframt á að þótt fréttamennska væri undanskilin gildissviði laganna, og úrlausn slíkra mála heyrði undir dómstóla, gæti Persónuvernd fjallað um málið á grundvelli 6. tölul. 3. mgr. 37. gr.

sem persónuupplýsingar, sbr. 1. tölul. 1. mgr. 2. gr. pul., væri meðal annars að vernda þá fyrir slíku.[223]

Af ofangreindu má ráða að ekkert virðist því til fyrirstöðu samkvæmt íslenskum lögum, ólíkt tilskipun 95/46/EB, að aðstandendur geti óskað eftir því að upplýsingar um látinn ættingja verði afmáðar, á grundvelli persónuupplýsingalaga.

Í Albrecht-skýrslu Evrópuþingsins bentu nokkrir álitsgjafar á að í reglugerðardrögunum væri ekki tekið á meðferð persónuupplýsinga látinna einstaklinga og lögðu þeir til að rétturinn til afmáunar yrði látinn taka til þeirra með þeim hætti að erfingjar þeirra gætu krafist þess að vinnsla og birting persónuupplýsinga um hina látnu yrði stöðvuð. Töldu álitsgjafarnir mikilvægt að erfingjar látinna einstaklinga ættu þess kost að beita réttinum til að gleymast og til afmáunar í slíkum tilfellum.[224] Þessar tillögur hlutu hins vegar ekki hljómgrunn hjá Evrópuþinginu.

Þá er heimildarákvæði í 25. og 26. gr. persónuverndarlaga þar sem segir að persónuverndarstofnanir geti gripið inn í og bannað notkun upplýsinga eða fyrirskipað eyðingu þeirra. Sams konar heimildir eftirlitsyfirvalda er að finna í 3. tölul. 28. gr. tilskipunar 95/46/EB. Persónuvernd getur bannað notkun upplýsinga sem eiga undir 25. gr. pul. ef eyðing þeirra eða breyting er óheimil skv. öðrum lögum. Þá getur Persónuvernd bannað notkun eða mælt fyrir um eyðingu upplýsinga sem eiga undir 26. gr. pul., bæði í einstökum tilvikum og með setningu almennra reglna. Í 40. gr. pul. er þar að auki ákvæði þess efnis að Persónuvernd geti mælt fyrir um stöðvun vinnslu persónuupplýsinga, þar á meðal söfnunar, skráningar eða miðlunar, mælt fyrir um að persónuupplýsingar verði afmáðar eða skrám eytt, í heild eða að hluta, bannað frekari notkun upplýsinga eða lagt fyrir ábyrgðaraðila að viðhafa ráðstafanir sem tryggja lögmæti vinnslunnar.

Reynt hefur á heimild Persónuverndar til að banna notkun persónuupplýsinga eða fyrirskipa eyðingu þeirra, sbr. 2. mgr. 25. gr., 3. mgr. 26. gr., og 40. gr. pul., í nokkrum málum:

Í *máli nr. 2011/1346 (Eurodac-gagnagrunnur)* fjallaði Persónuvernd um eyðingu upplýsinga úr svokölluðum Eurodac-gagnagrunni, sem hefur að geyma upplýsingar um fingraför hælisleitenda, ólöglegra innflytjenda og þeirra sem handteknir eru í tengslum við ólöglega för yfir landamæri Schengen-svæðisins og ekki er vísað frá. Samkvæmt reglugerð nr. 53/2003, settri með stoð í lögum um útlendinga nr. 96/2002, áttu gögn úr

[223] Álit Persónuverndar (n. 214).
[224] Breytingatillögur LIBE-nefndarinnar (n. 170) nr. 1406-1409.

fingrafaragagnagrunni að eyðast sjálfkrafa tíu árum frá töku fingrafara en önnur gögn fyrr. Ekki hafði verið farið að þessum fyrirmælum. Persónuvernd vísað í 40. gr. pul. og lagði fyrir Ríkislögreglustjóra og Útlendingastofnun að bæta verklag og eyða þeim upplýsingum sem varðveittar væru án heimildar.[225]

Í úrskurði Persónuverndar *í máli 2004/568 frá 18. apríl 2005 (Íslendingabók)* var talið óheimilt að skrá og birta í Íslendingabók upplýsingar um fyrrverandi maka kvartanda, gegn andmælum hans. Í niðurstöðu Persónuverndar var vísað til 7. tl. 1. mgr. 8. gr. og 2. mgr. 26. gr. persónuverndarlaga og bent á að í 2. mgr. 26. gr. segði að ef ákvæði annarra laga stæðu því ekki í vegi geti skráður aðili krafist þess að upplýsingum um hann, skv. 1. mgr., væri eytt eða notkun þeirra bönnuð ef slíkt teldist réttlætanlegt út frá heildstæðu hagsmunamati.[226]

4.12 Núgildandi réttur til afmáunar

Eins og fram hefur komið er rétturinn til að gleymast ekki alveg nýr af nálinni. Ákvæði 17. gr. reglugerðardraga framkvæmdastjórnarinnar byggir að hluta á þeim rétti sem fyrir er í b-lið 12. gr., sbr. d-lið 1. mgr. 6. gr., núgildandi tilskipunar 95/46/EB, sem innleiddur var með 25. gr. pul. Í b-lið 12. gr. tilskipunarinnar er kveðið á um rétt hins skráða til aðgangs að eigin persónuupplýsingum og að aðildarríkin skuli tryggja öllum skráðum aðilum rétt til að krefjast af ábyrgðaraðila:

> b) eftir því sem við á, leiðréttingar, afmáunar eða aðgangstakmarkana á upplýsingum ef vinnsla þeirra uppfyllir ekki ákvæði þessarar tilskipunar, einkum ef þær eru ófullkomnar eða óáreiðanlegar.[227]

Af b-lið 12. gr. má ráða að „gleymska“ í skilningi tilskipunarinnar felur í sér leiðréttingu eða eyðingu persónuupplýsinga og bann við notkun þeirra. Af ákvæðinu má einnig ráða að skilyrði er að vinnsla þeirra uppfylli ekki ákvæði tilskipunarinnar, einkum að upplýsingarnar séu ófullkomnar eða óáreiðanlegar.

Hér á eftir verður gerð grein fyrir innleiðingu ákvæða tilskipunar 95/46/EB um rétt til afmáunar í íslensku persónuverndarlögunum og í löggjöf annarra Norðurlandaþjóða. Umfjölluninni er ætlað að varpa ljósi á það hvað er líkt með ákvæðum um rétt hins skráða til að fá upplýsingum eytt og hvað ólíkt, með áherslu á það hvort rétturinn taki einungis til upplýsinga sem eru rangar eða villandi eða hvort hann taki einnig til upplýsinga sem eru sannar og réttar.

---

[225] Ákvörðun Persónuverndar 17. janúar 2012 í máli nr. 2011/1346.
[226] Úrskurður Persónuverndar 18. apríl 2005 í máli nr. 2004/568.
[227] Tilskipun 95/46/EB (n. 7), b-liður 12. gr.

4.12.1 Ísland

Í 25. gr. pul. er kveðið á um leiðréttingu og eyðingu *rangra og villandi* persónuupplýsinga og er ákvæðið efnislega samhljóða d-lið 1. mgr. 6. gr. tilskipunar 95/46/EB.[228] Á ákvæði 25. gr. pul. reyndi í *máli nr. 2011/1301 (Rangar upplýsingar á vefsíðu)*. Málavextir voru þeir að kona kvartaði til Persónuverndar yfir því að hjúskaparstaða hennar væri rangt skráð á tiltekinni vefsíðu. Þar kæmi fram að hún væri „maki" tiltekins manns, sem væru ævafornar og rangar upplýsingar. Hin ranga skráning kom í veg fyrir að konan gæti skráð sig á stefnumótasíðu á netinu. Eftir að Persónuvernd hafði sent ábyrgðaraðila vefsíðunnar bréf leiðrétti hann upplýsingarnar með því að bæta orðinu „fyrrverandi" framan við orðið „maki" á vefsíðunni. Í svari Persónuverndar var vísað til 25. gr. pul. en á það bent að þar sem ábyrgðaraðili hafi orðið við erindi Persónuverndar væri málinu lokið.[229]

Í skýringum með frumvarpi til laga nr. 77/2000[230] segir að við lögfestingu 26. gr. pul. hafi verið tekið mið af ákvæðum eldri laga, nr. 121/1989, en einnig e-lið 1. mgr. 6. gr. og 1. mgr. 14. gr. tilskipunar 95/46/EB. Ekki er minnst á b-lið 12. gr. tilskipunarinnar í þessu samhengi. Í e-lið 1. mgr. 6. gr. er fjallað um að persónuupplýsingar skuli geymdar í því formi að ekki sé unnt að persónugreina upplýsingar um skráða aðila lengur en þörf er á, miðað við markmiðin með söfnun upplýsinganna eða frekari vinnslu þeirra. Í 1. mgr. 14. gr. er fjallað um andmælarétt skráðra aðila, þ.e. rétt þeirra til að mótmæla vinnslu upplýsinga um þá sjálfa.

Með yfirskrift ákvæðis 26. gr. pul. má segja að gengið sé lengra varðandi rétt til afmáunar en í tilskipun 95/46/EB, þar sem kveðið er á um eyðingu og bann við notkun persónuupplýsinga sem *hvorki eru rangar né villandi*. Ekki er sett skilyrði um að upplýsingarnar séu ófullkomnar eða óáreiðanlegar, líkt og í tilskipun 95/46/EB. Skilyrði 26. gr. pul. fyrir eyðingu og banni við notkun persónuupplýsinga, sbr. 1. mgr., er að ekki sé lengur málefnaleg ástæða til að varðveita upplýsingarnar eða að eyðing og bann teljist réttlætanlegt út frá heildstæðu hagsmunamati, sbr. 2. mgr. 26. gr. Málefnaleg ástæða til varðveislu upplýsinga geti meðal annars byggst á fyrirmælum í lögum eða á því að ábyrgðaraðili vinni enn með upplýsingarnar, í samræmi við upphaflegan tilgang með söfnun þeirra. Þetta er í samræmi við ákvæði 12. gr. tilskipunarinnar um rétt til

[228] Alþt. 1999-2000, A-deild, þskj. 399 – 280. mál., athugasemdir við 25. gr.
[229] Ákvörðun Persónuverndar [dagsetningu vantar] 2012 í máli nr. 2011/1301.
[230] Alþt. 1999-2000, A-deild, þskj. 399 – 280. mál., athugasemdir við 26. gr.

afmáunar „ef vinnsla upplýsinganna uppfyllir ekki ákvæði laga að öðru leyti“. Varðandi hið heildstæða hagsmunamat skal, samkvæmt 2. mgr. 26. gr. laganna, tekið tillit til hagsmuna annarra, almenna persónuverndarhagsmuna, almannahagsmuna og þeirra aðgerða sem þörf er á til að verða við kröfunni.

Því má segja að ákvæði 26. gr. pul. sé efnislega skylt 17. gr. reglugerðardraga framkvæmdastjórnarinnar að því leyti að ekki er sett það skilyrði fyrir eyðingu eða banni við notkun persónuupplýsinga að upplýsingarnar séu rangar, villandi, skráðar án heimildar, ófullkomnar eða óáreiðanlegar.

Á ákvæði 26. gr. pul. reyndi í *máli nr. 2011/73 (Tekjubókhald ríkisins)* þar sem Persónuvernd fjallaði um hvort málefnalegar ástæður teldust vera fyrir hendi til að eyða upplýsingum um gjaldþrot sem starfsmaður tiltekins fyrirtækis hafði gengið í gegnum fyrir mörgum árum. Starfsmaðurinn vann í fyrirtæki þar sem hann hafði aðgang að upplýsingunum og það sama átti við um samstarfsmenn hans. Starfsmaðurinn taldi þessa tengingu við kennitölu sína í tekjubókhaldinu til þess fallna að skaða stöðu sína meðal samstarfsfólks síns og benti á að einkafyrirtækinu CreditInfo hefði verið gert að eyða upplýsingum um gjaldþrotið fjórum árum eftir lok þrotabúsins. Persónuvernd vísaði til 26. gr. pul. um eyðingu og bann við notkun persónuupplýsinga sem hvorki eru rangar né villandi, og benti jafnframt á að ákvæðið væri efnislega skylt 5. tölul. 1. mgr. 7. gr. pul., þar sem segir að ekki eigi að varðveita persónuupplýsingar í því formi að unnt sé að bera kennsl á hinn skráða aðila lengur en þörf krefji miðað við tilgang vinnslu. Þá vísaði Persónuvernd til heimildar í 3. mgr. 26. gr. um að stofnunin geti bannað notkun upplýsinga eða farið fram á eyðingu þeirra en benti á að þar sem ábyrgðaraðilinn hafi ákveðið að verða við beiðni hins skráða um eyðingu, skv. 2. mgr. 26. gr. pul., hafi málið verið látið niður falla.[231]

4.12.2 Noregur

Í 27. gr. norsku persónuverndarlaganna er fjallað um réttinn til að leiðrétta ófullkomnar persónuupplýsingar: *Retting av mangelfulle personopplysninger*. Ákvæðið tekur til persónuupplýsinga sem eru rangar eða ófullkomnar eða persónuupplýsinga sem ekki hefur verið heimilt að vinna.[232]

[231] Ákvörðun Persónuverndar 10. maí 2011 í máli nr. 2011/73.
[232] LOV-2000-04-14-31 Lov om behandling af personopplysninger (personopplysningsloven).

Í 28. grein laganna er fjallað um bann við varðveislu ónauðsynlegra persónuupplýsinga: *Forbud mot å lagre unødvendige personopplysninger*.[233] Ekki er sérstaklega tiltekið að þar sé um að ræða persónuupplýsingar sem hvorki séu rangar né villandi, eins og í íslensku lögunum, en ákvæðið er þó að stórum hluta sambærilegt 26. gr. pul.

Ákvæði 1. mgr. 28. gr. norsku persónuverndarlaganna er sambærilegt 1. mgr. 26. gr. pul. en í norska ákvæðinu segir að ábyrgðaraðili skuli eyða persónuupplýsingum eftir að vinnsla þeirra hefur þjónað tilgangi sínum, nema lagaskylda sé til að varðveita þær. Í 2. mgr. 28. gr. norsku laganna segir að varðveisla persónuupplýsinga geti engu að síður verið heimil í sagnfræðilegum, tölfræðilegum eða vísindalegum tilgangi, vegi almannahagsmunir af varðveislu upplýsinganna þyngra en ókostirnir fyrir einstaklinginn. Þessar undantekningar eru í 2. tölul. 1. mgr. 7. gr. pul. Í 3. mgr. 28. gr. norsku laganna kemur fram að hinn skráði geti krafist þess að upplýsingum, sem eru honum mjög óhagstæðar, verði eytt eða notkun þeirra bönnuð, svo lengi sem það stangist ekki á við önnur lög og sé réttlætanlegt út frá heildstæðu hagsmunamati. Þetta ákvæði virðist einnig eiga við um upplýsingar sem eru réttar en hinn skráði telur vera sér mjög óhagstæðar og er því sambærilegt 2. mgr. 26. gr. pul. Skyldleiki íslenskra og norskra laga kemur ekki á óvart þar sem við undirbúning á lögleiðingu persónuupplýsingatilskipunar ESB í íslenskan rétt var litið sérstaklega til þess hvernig Norðmenn hygðust innleiða tilskipunina í sinn rétt.[234]

4.12.3 Danmörk

Í dönsku persónuverndarlögunum er ekki minnst sérstaklega á eyðingu upplýsinga sem eru sannar og réttar.[235] Í 37. gr. laganna er að finna ákvæði um að ábyrgðaraðili skuli, samkvæmt kröfu hins skráða, leiðrétta eða eyða röngum eða villandi persónuupplýsingum eða sæta banni við notkun slíkra upplýsinga. Hið sama á við um upplýsingar sem unnar hafa verið í andstöðu við lög og reglur. Hið síðarnefnda gæti tekið til réttra upplýsinga en eyðing þeirra er þá bundin því skilyrði að vinnsla þeirra hafi verið í andstöðu við lög. Ábyrgðaraðili skal tilkynna þriðja aðila, sem fengið hefur gögnin í hendur um leiðréttingu, eyðingu eða bann við notkun persónuupplýsinganna, samkvæmt kröfu hins skráða. Þetta á hins vegar ekki við ef slík tilkynningaskylda reynist ómöguleg í framkvæmd eða felur í sér óhóflega fyrirhöfn.

[233] Sama heimild.
[234] Alþt. 1999-2000, A-deild, þskj. 399 – 280. mál., athugasemdir, kafli I.
[235] L 2000-05-31 nr. 429 om behandling af personoplysninger.

4.12.4 Svíþjóð

Ákvæði b- og c-liðar 12. gr. í tilskipun 95/46/EB voru innleidd með ákvæði 37. gr. sænsku persónuverndarlaganna, undir yfirskriftinni „Leiðrétting“.[236] Þar segir í 1. mgr. að ábyrgðaraðili skuli, að kröfu hins skráða, leiðrétta, afmá eða loka aðgengi að persónuupplýsingum sem reynist ónákvæmar eða villandi eða með öðrum hætti unnar í andstöðu við lög eða reglur. Í 2. mgr. 37. gr. segir að ábyrgðaraðili skuli tilkynna þriðja aðila sem fengið hefur gögnin áframsend um hvers konar leiðréttingu, eyðingu eða bann við vinnslu upplýsinga sem komið hafi til framkvæmda, skv. 1. mgr., ef hinn skráði krefjist þess eða ef þannig mætti koma í veg fyrir verulegt tjón eða óþægindi fyrir hinn skráða. Hins vegar skuli þetta ekki eiga við ef slík tilkynning reynist ómöguleg í framkvæmd eða feli í sér óhóflega fyrirhöfn.

4.12.5 Finnland

Í 29. gr. finnsku persónuverndarlaganna er ákvæði undir heitinu „Leiðrétting“ þar sem segir í 1. mgr. að ábyrgðaraðili skuli, að eigin frumkvæði eða að kröfu hins skráða, án tafar, leiðrétta, eyða eða bæta við persónuupplýsingar sem geymdar eru í gagnabanka viðkomandi ábyrgðaraðila og séu rangar, óþarfar, ófullnægjandi eða úreltar hvað varðar tilganginn með vinnslu þeirra.[237] Ábyrgðaraðili skal einnig hindra miðlun slíkra persónuupplýsinga ef það gæti stefnt vernd friðhelgi einkalífs hins skráða í hættu eða öðrum réttindum hans. Í 2. mgr. segir að synji ábyrgðaraðili kröfu hins skráða, um leiðréttingu á villum, skuli skrifleg staðfesting gefin út og ástæður synjunar teknar fram. Í þessum kringumstæðum getur hinn skráði skotið málinu fyrir umboðsmann persónuverndarmála. Í 3. mgr. segir að ábyrgðaraðili skuli tilkynna aðilum sem fengið hafa upplýsingarnar áframsendar um leiðréttingu þeirra og jafnframt þeim sem skráði hinar röngu persónuupplýsingar. Hins vegar fellur tilkynningarskyldan niður ef hún er óframkvæmanleg eða úr hófi fram erfið í framkvæmd.

4.12.6 Ísland gekk lengst

Eins og framangreind umfjöllun sýnir er ákvæði norrænnar löggjafar um eyðingu og bann við notkun persónuupplýsinga, sem hvorki eru rangar né villandi, skýrast í íslenskum persónuverndarlögum. Sambærileg ákvæði er að finna í lögum annarra

[236] Personuppgiftslag 1998:204.
[237] Henkilötietolaki, 22.4. 1999/523.

Norðurlandaþjóða og eru líkindi íslenskra og norskra laga mest. Hvergi er orðalagið þó skýrara en í íslenskum lögum, sbr. yfirskrift 26. gr. pul. Rétturinn í núgildandi tilskipun 95/46/EB er ekki orðaður jafnskýrt hvað þetta varðar.

Gagnstætt þeirri túlkun 26. gr. pul. sem lesa má út úr áliti Persónuverndar í máli nr. 2011/73 og áðurnefndum forúrskurði Evrópudómstólsins í Google Spain málinu, þann 13. maí sl., komst Lögsögumaður Evrópudómstólsins að þeirri niðurstöðu í júní 2013 að rétturinn til að gleymast væri ekki fyrir hendi, samkvæmt tilskipun 95/46/EB, þegar um sannar og réttar upplýsingar væri að ræða. Ekki væri hægt að byggja slíkan rétt á þeirri tilskipun, jafnvel þótt ákvæði hennar væru túlkuð með hliðsjón af Réttindaskrá Evrópusambandsins. [238] Nú hefur Evrópudómstóllinn hins vegar úrskurðað að núgildandi réttur til afmáunar persónuupplýsinga í tilskipun 95/46/EB tekur einnig til upplýsinga sem eru sannar og réttar og geti átt við um upplýsingar sem birst hafi með lögmætum hætti, sbr. niðurstöðu dómstólsins í Google Spain-málinu sem reifað var í kafla 4.9.1.[239]

4.13 Vernd barna

Viviane Reding hefur lagt mikla áherslu á að rétturinn til að gleymast snúist ekki síst um vernd barna, þar sem börn átti sig ekki á þeirri hættu sem því fylgir að birta persónuupplýsingar á netinu, sbr. orð hennar sem vísað var til í upphafi 2. kafla: *Þetta snýst um að myndir af þér á táningsárum verði ekki aðgengilegar á netinu að eilífu*.[240]

Vandamálið blasir við, líka hér á Íslandi. Það má meðal annars sjá á nýlegu dæmi frá aprílmánuði 2014, þar sem fréttir bárust af því að nektarmyndir af barnungum, íslenskum stúlkum hefðu verið birtar á erlendum spjallsíðum. Á síðunni skiptust notendur á myndunum og voru flestar stúlkurnar nafngreindar og greint frá því í hvaða bæjarfélagi þær byggju. Einhverjar myndanna voru um áratugs gamlar.[241]

Konarski og fleiri eru á meðal þeirra sem bent hafa á að vandamál tengd persónuupplýsingum barna hafi aukist með tilkomu samfélagsmiðla og vinsælda þeirra meðal barna og ungmenna. Slík vandamál tengist meðal annars því hvað teljist viðeigandi grundvöllur fyrir vinnslu slíkra persónuupplýsinga, til dæmis álitaefnum

[238] Mál C-131/12 *Google Spain* (n. 115).
[239] Mál C-131/12 *Google Spain* (n. 115).
[240] Reding (n. 8).
[241] Sveinn Arnarsson, „Nektarmyndir af stúlkum á fermingaraldri á spjallsíðu“ (*Vísir*, 15. apríl 2014) <www.visir.is/nektarmyndir-af-stulkum-a-fermingaraldri-a-spjallsidu/article/2014704159975> skoðað 17. apríl 2014.

varðandi samþykki foreldra eða lögráðamanna og skilyrðum laga um upplýsingagjöf. Á þessu sé tekið í hinni nýju reglugerð framkvæmdastjórnar ESB en hins vegar sé útfærslan þar ekki endilega viðunandi.[242]

Í áliti Ráðherranefndar Evrópuráðsins frá 2012 var fjallað um vernd barna á samfélagsmiðlum. Ráðherranefndin benti á að þrátt fyrir mikilvægi tjáningar- og upplýsingafrelsis, þurfi að huga sérstaklega að vernd barna á slíkum miðlum og að þar gegni foreldrar og uppfræðendur lykilhlutverki. Einnig þurfi eigendur samfélagsmiðla að veita skýrar upplýsingar um meðferð persónuupplýsinga og koma upp einföldum leiðum til að tilkynna óviðeigandi og ólöglegt efni. Þá þurfi að leiðbeina börnum um örugg og góð samskipti á netinu, meðal annars til að sporna við einelti og bregðast við kynferðislegu áreiti fullorðinna einstaklinga, sem sigli undir fölsku flaggi á samskiptamiðlum.[243]

Eins og fram hefur komið var lagt til í Albrecht skýrslunni að tilvísanir í sérstaka vernd barna yrðu fjarlægðar úr 17. gr. reglugerðardraganna, á þeim forsendum að með því væri gefið til kynna að vernd fullorðinna sætti takmörkunum. Verndin gildi jafnt um alla. Því lítur út fyrir að áhersla Reding, á sérstaka vernd fyrir börn í 17. gr., nái ekki fram að ganga og sé í raun óþörf, þar sem börn og fullorðnir hafi sama rétt, miðað við núverandi útfærslu 17. gr.

Tilvísanir í sérstaka vernd barna er þó víða að finna í reglugerðardrögum framkvæmdastjórnarinnar. Í lokaútgáfu þeirra, sem Evrópuþingið samþykkti 4. mars sl., segir, í nýju ákvæði a-liðar 1. mgr. 8. gr., að upplýsingagjöf til barna, foreldra og lögráðamanna, áður en gefið sé samþykki, meðal annars fyrir söfnun og notkun persónuupplýsinga barns, skuli vera með skýru orðalagi, sem hæfi markhópnum. Í 9. gr. inngangsorða reglugerðardraganna segir jafnframt að börn eigi rétt á sérstakri vernd persónuupplýsinga, þar sem þau séu ekki nógu meðvituð um þær hættur, afleiðingar, öryggisatriði og réttindi sem tengist vinnslu persónuupplýsinga. Við þetta ákvæði bætti Evrópuþingið skilyrði um að þegar vinnsla upplýsinga byggist á samþykki og tengist sölu á vörum eða þjónustu, sem beint sé að barni, verði foreldri eða lögráðamaður að veita samþykki, þegar barnið er yngra en 13 ára. Í slíkum tilfellum eigi einnig að nota orðalag sem hæfi aldurshópnum.

---

[242] Xavery Konarski o.fl. (n. 118).

[243] Council of Europe, „Reccommendation CM/Rec (2012)4 of the Committee of Ministers to Member States on the protection of human rights with regard to social networking services“, (4. apríl 2012) 4 <www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CM%20Rec%282012%294_En_Social%20networking%20services.pdf> skoðað 28. apríl 2014.

4.14 Viðurlög

Sektarákvæði er að finna í 5. mgr. 79. gr. reglugerðardraga framkvæmdastjórnarinnar. Þar segir meðal annars að eftirlitsyfirvald skuli mæla fyrir um sektargreiðslu sem nemi allt að 500.000 evrum eða, ef um fyrirtæki er að ræða, allt að 1% af árlegri veltu fyrirtækisins sem greiðist af hverjum þeim sem, viljandi eða sökum vanrækslu, uppfylli ekki réttinn til að gleymast eða til afmáunar.

Í meðförum Evrópuþingsins var viðurlagaákvæði 79. gr. breytt og það stytt og hert með þeim hætti að eftirlitsyfirvald skal beita einum af eftirtöldum viðurlögum þegar einhver uppfyllir ekki þær skyldur sem honum ber að gera, samkvæmt reglugerðinni:

-skriflegri viðvörun ef um fyrsta brot er að ræða eða ef ekki er ásetningur til að bregðast skyldum sínum;

-reglulegri endurskoðun persónuverndarmála;

-sektargreiðslum allt að 100.000.000 evrum eða allt að 5% af árlegri veltu, þegar um fyrirtæki er að ræða.[244]

[244] European Parliament (n. 167).

5 Niðurstöður

Hér að framan hefur verið fjallað um rétt einstaklinga til að afmá persónuupplýsingar af netinu, eins og rétturinn var settur fram í 17. gr. draga framkvæmdastjórnar ESB að reglugerð um vernd persónuupplýsinga og frjálsa miðlun slíkra upplýsinga, frá 25. janúar 2012. Einnig hefur verið fjallað um núgildandi rétt til afmáunar í tilskipun 95/46/EB, lögum nr. 77/2000 og annarri norrænni löggjöf. Ljósi hefur verið varpað á þær endurbætur og réttarsamræmingu sem er fyrir dyrum á þessu réttarsviði innan Evrópusambandsins og helstu nýmæli í reglugerð framkvæmdastjórnarinnar hafa verið skýrð. Einnig hefur verið fjallað um þær breytingartillögur á 17. gr. sem settar voru fram í Albrecht-skýrslunum og gerður samanburður á 17. gr. reglugerðardraganna og þeirri útgáfu 17. gr. sem samþykkt var af Evrópuþinginu, þann 12. mars 2014. Þá voru reifaðar niðurstöður Evrópudómstólsins, frá 13. maí 2014, í prófmáli um réttinn til að gleymast og til afmáunar og ábyrgð leitarvélafyrirtækja á netinu.

Sú rannsóknarspurning sem varpað var fram í inngangi þessarar ritgerðar var þessi: Hvað þýðir rétturinn til að gleymast og til afmáunar, til hvaða miðla tekur hann, hver á réttinn og hver ber ábyrgð á framkvæmd hans? Spurningin er því í raun fjórþætt.

Umfjöllunin sýnir í fyrsta lagi að þýðing réttarins til að gleymast og til afmáunar tengist þeirri hugmyndafræði að eilíft líf upplýsinga sem geymdar eru á netinu stríði gegn eðlislægri tilhneigingu manna til að gleyma. Með réttinum til að gleymast og til afmáunar er leitast við að koma í veg fyrir að atvik fortíðar fái óeðlilega mikið vægi í nútíðinni. Þannig er dregið úr líkum þess að afglöp og mistök í fortíð fylgi fólki um aldur og ævi, eins og stafrænt brennimerki. Réttinum er ætlað að styrkja réttindi hins skráða til persónuupplýsingaverndar og friðhelgi einkalífs, sem varin eru í 8. gr. MSE, sbr. 71. gr. stjskr., og undirstrika að persónuupplýsingar séu eign einstaklingsins en ekki fyrirtækjanna sem safna þeim. Samkvæmt niðurstöðu Evrópudómstólsins frá 13. maí 2014 felur rétturinn til afmáunar í sér heimild til að fá afmáðar persónuupplýsingar sem eru viðkvæmar, ófullnægjandi, óviðeigandi, eða ekki lengur viðeigandi, eða óhóflegar í ljósi þess tilgangs sem vinnslu þeirra var upphaflega ætlaður og í ljósi þess tíma sem liðið hefur. Af niðurstöðu dómstólsins má ráða að rétturinn sætir ekki þeim takmörkunum að upplýsingar séu rangar eða villandi, heldur getur verið um sannar upplýsingar að ræða. Hins vegar gildir hann ekki endilega um allar persónuupplýsingar, til dæmis ekki ef upplýsingarnar varða einstaklinga sem teljast opinberar persónur.

Í öðru lagi hefur verið leitt í ljós að rétturinn til að gleymast og til afmáunar á rætur að rekja til hins franska *droit à l'oubli* en fréttamennska er undanþegin gildissviði hans, ólíkt hinum franska rétti. Auk þess að undanskilja fréttamennsku gildir rétturinn til að gleymast og til afmáunar ekki um upplýsingar sem birtar hafa verið í tengslum við bókmenntir, sagnfræðilegar rannsóknir og fleiri svið. Þá er starfsemi þjóðaröryggisstofnana einnig undanþegin gildissviðinu.

Umfjöllunin sýnir að ekki er gerður greinarmunur á gömlum og nýrri upplýsingum í tilskipun 95/46/EB og 17. gr. reglugerðardraganna. Tími og aldur upplýsinga hefur þannig almennt ekki áhrif á réttinn til að gleymast og til afmáunar og á það einnig við um undanþágur frá gildissviði laganna. Þannig gæti fjölmiðill, sem birtir persónuupplýsingar í fullum rétti, vísað í undanþágu vegna fréttamennsku tíu árum eftir birtingu og enn verið undanskilinn reglum tilskipunarinnar og hinnar væntanlegu reglugerðar. En, eins og niðurstöður Evrópudómstólsins frá 13. maí sl. sýna, getur vinnsla leitarvélarfyrirtækis á sönnum og réttum upplýsingum, sem upphaflega var lögmætt að birta í fjölmiðli, orðið ósamræmanleg ákvæðum tilskipunarinnar í tímans rás. Þannig getur leitarvélarfyrirtækið, sem ábyrgðaraðili, þurft að sæta því að fjarlægja hlekki á gamlar og úreltar upplýsingar, þótt fjölmiðillinn þurfi ekki að fjarlægja sömu upplýsingar úr gagnabanka sínum, þar sem hann er undanþeginn gildissviði tilskipunarinnar.

Spyrja má hvort aldur upplýsinga ætti að að hafa meira vægi þegar teknar eru ákvarðanir um eyðingu persónuupplýsinga. Með hliðsjón af framangreindri ályktun Evrópudómstólsins um aldur upplýsinga getur hugsanlega talist réttlætanlegra að eyða gömlum persónuupplýsingum, sem litla eða enga þýðingu hafa í nútíð, en nýrri upplýsingum. Vakin hefur verið athygli á þeirri hugmynd að draga megi úr vægi gamalla upplýsinga með því að leitarniðurstöður leitarvéla sýni upplýsingar í tímaröð og yngstu leitarniðurstöðurnar birtist efst á síðunni. Sú hugmynd er einföld í framkvæmd, felur ekki í sér ritskoðun upplýsinga og samræmist reglum um meðalhóf. Undir hana er því tekið hér. Einnig hefur verið fjallað um hugmyndir um tímamörk á varðveislu persónuupplýsinga á netinu, „síðasta neysludag“ persónuupplýsinga, sem fela það í sér að upplýsingar eyðist eftir ákveðinn tíma. Þær hugmyndir ganga lengra og verður ekki séð að nauðsyn sé á svo róttækum útþurrkunum upplýsinga. Eðlilegra væri að afmáun upplýsinga fari fram að beiðni þess sem upplýsingarnar má rekja til.

Bent var á að í meðförum Evrópuþingsins hafi undanþágur frá gildissviði verið víkkaðar út. Sjónum var sérstaklega beint að svokallaðri heimilishaldsundantekningu í d-lið 2. mgr. 2. gr. reglugerðardraganna og því álitaefni hvort samfélagsmiðlar eigi að falla undir hana eða ekki. Ekki er fullkomlega ljóst af reglugerðardrögum framkvæmdastjórnar ESB hvort og hvernig notkun samfélagsmiðla fellur undir heimilishaldsundantekninguna. Vísbendingu um flækjustig þess álitaefnis má finna í 15. lið inngangsorða reglugerðardraganna en þar segir að reglugerðin gildi ekki um vinnslu einstaklings á persónuupplýsingum, sé vinnslan hluti af starfsemi sem sé einungis í þágu hans sjálfs eða heimilis og fari ekki fram í nokkrum hagnaðartilgangi og tengist þar af leiðandi ekki atvinnu eða markaðsstarfsemi. Fjallað hefur verið um hvort túlka megi framangreint orðalag svo að heimilishaldsundantekningin eigi almennt við um einstaka notendur samfélagsmiðla, nema í þeim tilfellum þegar þeir birta efni í markaðslegum tilgangi, til dæmis í þágu fyrirtækis eða stofnunar, eða nota samfélagsmiðla til að koma pólitískum skoðunum á framfæri. Þá hefur verið fjallað um þýðingu þess þegar aðgangur að notendaupplýsingum á samfélagsmiðlum er opinber, opinn vinum vina eða eingöngu opinn vinum. Niðurstaðan er sú að séu samfélagsmiðlar notaðir í markaðslegum tilgangi verði þeir að öllum líkindum ekki taldir falla undir heimilishaldsundantekninguna, nema eingöngu sé verið að selja heimilismuni, og aðra persónulega muni, og ekki í atvinnuskyni. Þá geti opinber aðgangur að persónulegum samfélagsmiðlasíðum þýtt að heimilishaldsundantekningin eigi ekki við. Hið sama geti átt við sé aðgangur opinn „vinum vina“ eða sé notandi með óvenju marga vini á vinalista sínum, þar sem slík birting hefði í för með sér snertiflöt við fjölda þriðju aðila. Framangreind túlkun er studd af breytingum Evrópuþingsins á ákvæði d-liðar 2. mgr. 2. gr. reglugerðardraganna, álitsgerð 29. gr. starfshóps ESB og samræmist að hluta niðurstöðu Evrópudómstólsins í máli Bodil Lindqvist.

Fjallað var um breytingar Evrópuþingsins á d-lið 2. mgr. 2. gr. og hvernig þær renna stoðum undir þá túlkun að fjöldi vina og friðhelgisstillingar á samfélagsmiðlum skipti máli, hvað umfang heimilishaldsundantekningarinnar varðar. Einnig að breytingar þingsins bendi til að einstaklingar geti fallið undir heimilishaldsundantekninguna, þótt þeir noti samfélagsmiðla í hagnaðartilgangi, eins og til að selja heimilismuni og fatnað, svo lengi sem salan fer ekki fram í atvinnuskyni og takmarkaður hópur hefur aðgang að upplýsingunum.

Í þriðja lagi hefur verið sýnt fram á að rétturinn til afmáunar tekur til einstaklinga en ekki lögaðila. Bent hefur verið á að samkvæmt íslenskum persónuverndarlögum taki

rétturinn til persónuupplýsinga um látna jafnt sem lifandi einstaklinga en að hið sama eigi ekki við um gildissvið tilskipunar 95/46/EB eða reglugerðardraga framkvæmdastjórnarinnar. Fjallað var um að varfærið orðalag í 17. gr. reglugerðardraganna hafi vakið upp þá spurningu hvort um raunverulegt nýmæli sé að ræða eða einungis gamalt vín á nýjum belgjum. Niðurstaðan er sú að 17. gr. reglugerðardraganna felur í sér aukinn rétt fyrir hinn skráða, sér í lagi vegna samspils þess ákvæðis við 19. gr. sömu reglugerðardraga, um andmælarétt. Núgildandi andmælaréttur sætir þeim takmörkunum að hinn skráði þarf að hafa lögmætar og knýjandi ástæður til að andmæla vinnslu upplýsinga um sjálfan sig. Í 19. gr. reglugerðardraganna snýst sönnunarbyrðin við með þeim hætti að ábyrgðaraðilinn ber sönnunarbyrðina af því að lögmætar og knýjandi ástæður séu fyrir vinnslunni. Andmælaréttur 19. gr. gildir auk þess þegar vinnsla er nauðsynleg til að vernda mikilvæga hagsmuni hins skráða og tengist réttinum til afmáunar í 17. gr. með þeim hætti að beri andmæli hins skráða árangur virkjar það rétt 17. gr. til að fá persónuupplýsingum eytt.

Í fjórða lagi var farið var yfir það hverjir geti talist ábyrgðaraðilar og í því samhengi var fjallað sérstaklega um samfélagsmiðla, leitarvélar og einstaklinga sem birta efni um aðra einstaklinga á vefsíðum sínum. Bent var á þá erfiðu stöðu sem upp getur komið þegar notendur birta persónuupplýsingar á vefsíðum sem tilheyra þriðju aðilum. Slíkir aðilar hljóti að teljast ábyrgðaraðilar en séu þó ekki í aðstöðu til að afmá upplýsingarnar og uppfylla lagaskyldur sínar sem slíkir.

Ályktað var að ætlun framkvæmdastjórnar ESB hafi verið að rétturinn í 17. gr. tæki meðal annars til samfélagsmiðla og leitarvéla. Með breytingum Evrópuþingsins í mars 2014 hafi verið dregið úr þeim væntingum, þar sem þær þóttu óraunhæfar í ljósi tæknilegrar uppbyggingar netsins. En með forúrskurðinum 13. maí 2014, um ábyrgð leitarvélafyrirtækisins Google, hafi Evrópudómstóllinn aftur kynt undir slíkum væntingum og slegið því föstu að fyrirtæki sem reka leitarvélar á netinu teljist ábyrgðaraðilar.

Niðurstaða þessa hluta er sú að eigendur samfélagsmiðla teljast ábyrgðaraðilar, þar sem þeir ákveða tilgang og vinnslu slíkra upplýsinga. Hins vegar er ekki fullkomlega skýrt hvort einstaklingur telst vera ábyrgðaraðili þegar hann setur efni inn á facebook síðu sína eða hvort hann telst falla undir svokallaða heimilishaldsundantekningu.

Hvað ábyrgð leitarvélafyrirtækja varðar var vísað til forúrskurðar Evrópudómstólsins frá 13. maí sl. Niðurstaða hans var sú að Google teldist ábyrgðaraðili þeirra vefsíðna

sem fyrirtækið vinnur með, í skilningi tilskipunar 95/46/EB, þar sem Google safnar upplýsingum, flokkar þær vefsíður sem safnað er, heimtir upplýsingar, skráir, þær, kerfisbindur og geymir á netþjónum sínum, auk þess að gera upplýsingarnar aðgengilegar notendum í formi leitarniðurstaðna. Sá sem birtir persónuupplýsingar á netinu ber því ekki eingöngu ábyrgð á því að afmá þær, sé þess krafist af til þess bærum einstaklingi, heldur líka leitarvélin sem finnur þær og vinnur með þær. Bent hefur verið á að slíkar kröfur til leitarvélafyrirtækja geti leitt til íhlutunar í tjáningar- og upplýsingafrelsi.

Eins og umfjöllunin hefur leitt í ljós ríkir óvissa um mikilvæg álitaefni, meðal annars um gildissvið hinnar nýju reglugerðar, sér í lagi um það hvort réttur 17. gr. til afmáunar gildir um persónuupplýsingar á samfélagsmiðlum og þá með hvaða hætti. Ekki er tekið fyllilega á þessum álitaefnum í reglugerðardrögunum. Ekki verður þó séð hvernig rétturinn til afmáunar getur falið í sér raunverulegan rétt til að fá persónuupplýsingum eytt varanlega af netinu, nema að rétturinn verði talinn ná til samfélagsmiðla og leitarvéla, eins og Google og sambærilegra hjálpartækja, sem hjálpa notendum að finna upplýsingar. Þessi sjónarmið endurspeglast í dómi Evrópudómstólsins frá 13. maí sl. Þegar persónuupplýsingar eru eitt sinn komnar á netið er of auðvelt að deila þeim áfram út í hið óendanlega og varla gerlegt að eltast við ábyrgðaraðila hverrar einustu vefsíðu sem birt hefur afrit af þeim. Þá vaknar hins vegar sú spurning hvort að með því að gera leitarvélafyrirtæki ábyrg fyrir því að eyða efni sem notendur vilja að falli í „gleymsku“ sé brotið á tjáningarfrelsi.

Svo virðist sem setja eigi í hendur eigenda samfélagsmiðla og leitarvélafyrirtækja að ákveða hvort eyða eigi upplýsingum af netinu, að kröfu einstaklinganna sem þær varða. Til dæmis þurfi eigandi samfélagsmiðils að vega og meta hvort notandi falli undir heimilishaldsundantekninguna, þegar hann hleður inn persónuupplýsingum um þriðju aðila. Falli hann ekki undir þá undantekningu teljast notandinn og eigandi samfélagsmiðilsins sameiginlegir ábyrgðaraðilar, sbr. 24. gr. reglugerðardraganna, og þurfa að semja um skiptingu ábyrgðar á því að eyða upplýsingunum. Teljist notandinn falla undir undantekninguna virðist eigandi samfélagsmiðilsins bera ábyrgð á að fjarlægja efnið, nema varðveislu þess megi réttlæta með rétti til tjáningarfrelsis.

Þetta kallar á flókið hagsmunamat; það er mat á réttinum til afmáunar og friðhelgi einkalífs annars vegar og tjáningarfrelsi þeirra sem birta og/eða endurbirta efni á samfélagsmiðlum hins vegar. Þar sem slíkt mat fer mikið til eftir aðstæðum hverju

sinni, og dómafordæmi eru lítil sem engin, gerir þetta fyrirkomulag miklar kröfur til ábyrgðaraðila, sem óvíst er hvort þeir geti staðið undir.

Sú lausn að gera fyrirtæki sem reka netleitarvélar og samfélagsmiðla ábyrg fyrir því að eyða efni af netinu getur haft í för með sér allsherjarritskoðun á netinu; að fyrirtækin eyði fleiri upplýsingum en nauðsynlegt er, til að forðast sektargreiðslur, en slíkt fyrirkomulag hlýtur að teljast andstætt viðteknum gildum í lýðræðislegu samfélagi.

Einnig var fjallað um takmarkanir á ábyrgð milligönguaðila í tilskipun 2000/31, sbr. lög um rafræn viðskipti nr. 30/2002. Fram kom að ábyrgðarreglur gagnvart þjónustuveitendum, eins og samfélagsmiðlum og leitarvélum, verði áfram að finna á tveimur stöðum; í hinni nýju reglugerð um vernd persónuupplýsinga og frjálsa miðlun slíkra upplýsinga og einnig í tilskipun 2000/31 um rafræn viðskipti en hún gildir meðal annars um símaforrit (e. applications) og kortlagningu persónuupplýsinga (e. profiling). Verður það að teljast galli og að betur færi á því að allar ábyrgðarreglur væru á einum stað, það er í hinni nýju persónuupplýsingareglugerð.

Hluti vandans við birtingu og vinnslu persónuupplýsinga á netinu er hugsanlega sá að almenningur er ekki nógu meðvitaður um réttindi sín og þær hættur sem því kann að fylgja að deila myndum og öðrum persónuupplýsingum á netinu. Þetta á sér í lagi við um börn. Þann vanda mætti að einhverju leyti fyrirbyggja með því að auka fræðslu um netnotkun, með áherslu á fræðslu barna, ungmenna og forráðamanna þeirra.

Á það skal bent að á síðustu árum hafa orðið gríðarlegar framfarir í upplýsingatækni, sem fært hafa almenningi stórkostleg tækifæri til upplýsingaöflunar og margvísleg hlunnindi í hendur. Gegn því að deila persónuupplýsingum á netinu fær almenningur ókeypis þjónustu, á borð við tölvupóst, samfélagsmiðla og myndhýsingarforrit. Ef starfsumhverfi þjónustuveitenda á netinu verður stráð boðum og bönnum með hertri löggjöf og hærri sektargreiðslum er ekki útilokað að ábyrgðaraðilar verði á endanum tilneyddir að innheimta gjald fyrir þessa þjónustu. Ekki er víst að þorri almennings sé tilbúinn að greiða fyrir hana.

Þótt endalok einkalífs séu að öllum líkindum ekki runnin upp er vinnsla einkafyrirtækja á persónuupplýsingum almennings þó augljóslega komin á grátt svæði, hvað friðhelgi einkalífs varðar. Veruleikinn er sá að nethegðun; samskipti, verslun og netleit notenda er kortlögð og tölvupóstar skannaðir. Auk þess eru upplýsingar um löngu liðna atburði varðveittar í tölvuskýjum, í músarsmellsfjarlægð.

Af túlkun Evrópudómstólsins 13. maí sl. á núgildandi rétti til afmáunar, í tilskipun 95/46/EB, er ljóst að persónuverndarlöggjöf Evrópusambandsins felur í sér skilvirkan

rétt til að hindra aðgang að persónuupplýsingum eða fá þeim varanlega eytt af netinu. Rétturinn til afmáunar er styrktur í 17. gr. reglugerðardraga framkvæmdastjórnarinnar. Hann felur í sér tæknilegar, lagalegar og pólitískar áskoranir sem varða hagsmuni og grundvallarréttindi almennings í nútímasamfélagi. Hann markar nýja stefnu og ákveðin tímamót og er ætlað að svara breyttri heimsmynd á sviði upplýsingatækni. Rétturinn er þó ekki fullkomlega skýr og mörgum spurningum er enn ósvarað. Hvort netnotendur öðlast öruggt skjól í faðmi regluverks Evrópusambandsins er því ennþá of snemmt að fullyrða.

Heimildaskrá

——„Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses" (*European Union*, 25. janúar 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> skoðað 10. mars 2014

——„Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union" (4. nóvember 2010) COM (2010) 609 <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf> skoðað 29. apríl 2014

——„Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU" (27. nóvember 2013) COM (2013) 847 <http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf> skoðað 29. apríl 2014

——„Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" (*European Parliament*, 12. mars 2014) <www.europarl.europa.eu/oeil/popups/summary.do?id=1342337&t=d&l=en> skoðað 20. apríl 2014

——„EDPS: Active supervision effective in keeping EU bodies on track for data protection" (*European Union*, 27. janúar 2014) <http://europa.eu/rapid/press-release_EDPS-14-3_en.htm> skoðað 29. apríl 2014

——„LIBE Committee vote backs new EU data protection rules“ (*European Union*, 22. október 2013) <http://europa.eu/rapid/press-release_MEMO-13-923_en.htm> skoðað 19. mars 2014

——„Opinion 4/2007 on the concept of personal data“ (Article 29 Data Protection Working Party, 20. júní 2007) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> skoðað 14. mars 2014

——„Opinion 5/2009 on online social networking“ (Article 29 Data Protection Working Party, 12. júní 2009) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf> skoðað 29. apríl 2014

——„Opinion 1/2010 on the concepts of „controller“ and „processor““ (Article 29 Data Protection Working Party, 16. febrúar 2010) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> skoðað 29. apríl 2014

——„Progress on EU data protection reform now irreversible following European Parliament vote“ (*European Union*, 12. mars 2014) <http://europa.eu/rapid/press-release_MEMO-14-186_en.htm> skoðað 29. apríl 2014

——„SPIEGEL Exclusive: NSA Spies on International Bank Transactions“ *Spiegel Online* (15. september 2013) <http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html> skoðað 10. mars 2014

——„Tölvu- og netnotkun mest á Íslandi af öllum Evrópulöndum“ (*Hagstofa Íslands*, 27. janúar 2014) <http://hagstofa.is/Pages/95?NewsID=10778> skoðað 3. febrúar 2014

——„Umsögn um drög framkvæmdastjórnar ESB að reglugerð um vernd persónuupplýsinga og frjálsa miðlun slíkra upplýsinga“ (*Persónuvernd*, maí 2013) <www.personuvernd.is/efst-a-baugi/Umsagnir/2013/greinar/nr/1645> skoðað 6. mars 2014

——„US NSA: stop mass surveillance now or face consequences, MEPs say“ (*European Parliament*, 12. mars 2014) <www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203> skoðað 21. apríl 2014

Albrecht, Jan Philipp, „Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ (European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 17. desember 2012) <www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf> skoðað 2. apríl 2014

Albrecht, Jan Philipp, „Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ (European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 16. janúar 2013) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Data%20Protection%20Reform/13-01-16_Albrecht_draft_report.pdf> skoðað 2. apríl 2014

Albrecht, Jan Philipp, „Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ Amendments tabled in committee.
(European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 6. mars 2013)
<www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE506.147> skoðað 20. apríl 2014

Ambrose, M. L., „It's about time: Privacy, information life cycles and the right to be forgotten“ (2013) 16 (2) Stanford Technology Law Review 101

Amrose, Meg Leta og Ausloos, Jef, „The Right to be Forgotten Across the Pond“ (2013) 3 Journal of Information Policy 1

Björg Thorarensen, *Stjórnskipunarréttur: mannréttindi* (Bókaútgáfan Codex 2008)

Björg Thorarensen og Sigrún Jóhannesdóttir, „Nýjar ógnir og ný úrræði í persónuvernd“ *Fréttablaðið* (17. október 2012)

Bygrave, L. A., *Data protection law: approaching its rationale, logic, and limits* (Kindle útg., Kluwer Law International 2002)

Comi, L., „Opinion on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ (European Parliament, Internal Market and Consumer Protection, 28. janúar 2013) 2012/0011(COD) <www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE496.497&secondRef=02> skoðað 29. apríl 2014

Commission, „Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data“ COM (2012) 11 final

——, „Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data“ COM (2012)10 final

——, „Data Protection“ (október 2013) <http://ec.europa.eu/commission_2010-2014/reding/pdf/news/20131022-libe-data-protection_en.pdf> skoðað 29. apríl 2014

Council of Europe, „Reccommendation CM/Rec(2012) 4 of the Committee of Ministers to Member States on the protection of human rights with regard to social networking services“ (4. apríl 2012) <www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CM%20Rec%282012%294_En_Social%20networking%20services.pdf> skoðað 28. apríl 2014

——, „Recommendation R(86)1 of the Committee of Ministers to Member States on the Protection of Personal Data used for Social Security Purposes“ (23. janúar 1986) <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1894447&SecMode=1&DocId=688622&Usage=2> skoðað 12. apríl 2014

European Data Protection Supervisor, „Stellungnahme des Europäischen Datenschutzbeauftragten zum Datenschutzreformpaket“ (Brussel 7. mars 2012), mgr. 66-67, 149 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf> skoðað 2. apríl 2014

European Parliament, Committe on Civil Liberties, Justice and Home Affairs (Skýrsluhöfundur: Albrecht, J. P.), „Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“ (Brussel, 16. janúar 2012) (COM(2012)0011 - C7-0025/2012-2012/0011(COD)) <www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf> skoðað 29. apríl 2014

European Union Agency for fundamental rights og Council of Europe, *Handbook on European Data Protection Law* (Publications Office of the European Union, Lúxemborg 2014) <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law_en.pdf> skoðað 26. febrúar 2014

Fleischer, P., „Book Burning, updated for the Digital Age“ <http://peterfleischer.blogspot.com/2012/11/book-burning-updated-for-digital-age.html> skoðað 29. apríl 2014

Froomkin, A. Michael, „The Death of Privacy?“ (2000) 52 *Stanford Law Review* 1461

General Secretariat of the Council, „Conclusions“ (European Council október 2013) EUCO 169/13 <www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf> skoðað 19. mars 2014

Goni, U., „Can a Soccer Star Block Google Searches?“ (*TIME*, nóvember 2008) <http://content.time.com/time/world/article/0,8599,1859329,00.html> skoðað 29. apríl 2014

Herdís Þorgeirsdóttir, „Þröng skýring á fjölmiðlafrelsi og vafasamt eftirlit opinberrar stofnunar?“ *mbl.is* (Reykjavík, júlí 2005) <www.mbl.is/greinasafn/grein/1029789/> skoðað 8. maí 2014

House of Commons Justice Committee, „The Committee's Opinion on the European Union Data Protection Framework Proposals,“ (2012) House of Commons Paper 572-I

Kelly, Seán, „Opinion of the Committe on Industry, Research and Energy for the Committe on Civil Liberties, Justice and Home Affairs“ (European Parliament, Committee on Industry, Research and Energy, 26. febrúar 2013) nr. 162 <www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+COMPARL+PE-496.562+02+DOC+PDF+V0//EN&language=EN> skoðað 3. apríl 2014

Kirby, M. D., „Transborder Data Flows and the „Basic Rules“ of Data Privacy“ (1980) 16 Stanford Journal of International Law 58

Konarski, X. o.fl., *Reforming the Data Protection Package.* (European Parliament 2012)

Kuner, Christopher o.fl., „The Proposed EU Data Protection Regulation Two Years Later“ [2014] *Bloomberg BNA, Privacy and Security Law Report* <www.wsgr.com/eudataregulation/pdf/kuner-010614.pdf> skoðað 16. apríl 2014

Kuner, Christopher, *European data protection law: corporate compliance and regulation* (2. útg., Oxford University Press 2007)

——, „The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law“ [2012] *Bloomberg BNA Privacy and Security Law Report* <http://ico.org.uk/news/events/~/media/documents/future_of_dp_in_europe_2012/ico_event_future_of_dp_in_europe_2012_Chris_Kuner_article.ashx> skoðað 29. apríl 2014

Kuschewsky, M., „The right to be forgotten - the Fog Finally Lifts“ (2012) 12 Privacy & Data Protection 10

Lindsay, David, „The Right to be forgotten in European Data Protection Law“. Witzleb, N. (ritstj.), *Emerging challenges in privacy law: comparative perspectives* (Kindle útg., Cambridge University Press 2014)

Markesinis, B. o.fl., „Concerns and Ideas about the Developing English Law of Privacy (and How Knowledge of Foreign Law Might Be of Help)“ (2004) 52 American Journal of Comparative Law 133

Maxwell, W.J., „Data Privacy: the European Comission Pushes for Total Harmonisation“ (2012) 18 (6) Computer and Telecommunications Law Review

Mayer-Schönberger, Viktor, *Delete the Virtue of Forgetting in the Digital Age* (Princeton University Press 2009)

——, „The Right to be Forgotten - Events - IIEA - The Institute of International and European Affairs“ (Dublin, Ireland, október 2011) <www.iiea.com/events/the-right-to-be-forgotten?gclid=CIrbrKChkr0CFeXLtAodgHUAHg> skoðað 29. apríl 2014

OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [1980] C(80) 58/FINAL, uppfærðar 11. júlí 2013, sbr. C(2013) 79

OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (Organisation for Economic Co-operation and Development 2011) <www.oecd-ilibrary.org/content/book/9789264115644-en> skoðað 29. apríl 2014

Pastukhov, O., „The Right to Oblivion: What's in a Name?“ (2013) 19 Computer and Telecommunications Law Review 13

Páll Hreinsson, *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála* (Lagastofnun Háskóla Íslands 2007)

Páll Sigurðsson, *Fjölmiðlaréttur: meginþættir réttarumhverfis fjölmiðlanna* (Háskólaútgáfan 1997)

Páll Þórhallsson, „Andlitslyfting Evrópusambandsins“ (*mbl.is*, 11. febrúar 2001) <www.mbl.is/greinasafn/grein/588574/> skoðað 29. apríl 2014

Reding, Viviane, „The Upcoming Data Protection Reform for the European Union“ (2011) 1 (1) International Data Privacy Law 3

——, „Justice Council: We need a simple solution for citizens and business on data protection“ (*European Union*, desember 2013) <http://europa.eu/rapid/press-release_SPEECH-13-1029_en.htm> skoðað 29. apríl 2014

——, „A data protection compact for Europe“ (*European Union*, 28. janúar 2014) <http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm> skoðað 16. apríl 2014

Schechner, Sam, „Online Privacy Could Spark U.S.-EU Trade Rift“ (*The Wall Street Journal*) <http://online.wsj.com/news/articles/SB10001424052702304361604579291041878017398> skoðað 10. mars 2014

Schwartz, J., „Two German Killers Demanding Anonymity Sue Wikipedia's Parent“ *The New York Times* (13. nóvember 2009) <www.nytimes.com/2009/11/13/us/13wiki.html> skoðað 14. apríl 2014

Sigurður Líndal og Skúli Magnússon, *Réttarkerfi Evrópusambandsins og Evrópska efnahagssvæðisins: megindrættir* (Hið íslenska bókmenntafélag 2011)

Schmid Petersen, F., „The press as public watch dogs and the privacy of public figures“ [2004] International Law Office

Sveinn Arnarsson, „Nektarmyndir af stúlkum á fermingaraldri á spjallsíðu“ (*Vísir*, 15. apríl 2014) <www.visir.is/nektarmyndir-af-stulkum-a-fermingaraldri-a-spjallsidu/article/2014704159975> skoðað 17. apríl 2014

Thierer, A., „Europe's „Right to Be Forgotten“: Privacy as Internet Censorship“ (*The Technology Liberation Front*, 23. janúar 2012) <http://techliberation.com/2012/01/23/europes-right-to-be-forgotten-privacy-as-internet-censorship/> skoðað 29. apríl 2014

Verbiest, T. o.fl., „Study on the Liability of Internet Intermediaries“ <http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf> skoðað 29. apríl 2014