https://doi.org/10.22364/juzk.77.38

DROŠĪBAS JĒDZIENS UN IETEKME UZ DATU AIZSARDZĪBAS TIESĪBU ATTĪSTĪBU

SECURITY NOTION AND IMPACT ON THE DEVELOPMENT OF DATA PROTECTION LAW

Irēna Ņesterova, *Dr. iur*.
Latvijas Universitātes Juridiskās fakultātes
Juridiskās zinātnes institūta pētniece

Summary

The objective of the paper is to evaluate the notion of security and its implications on the development of data protection law. It examines the concepts of security, cybersecurity and information security, and how these concepts are related to data protection. The paper argues that the new EU data protection rules tie security and data protection together even closer in two ways. Firstly, it demonstrates how the General Data Protection Regulation (the GDPR) introduces risk-based approach, which is generally applied in security field, as an essential element also in data protection field. Secondly, it examines the personal data breach notification requirements introduced by the GDPR.

Atslēgvārdi: cilvēktiesības, datu aizsardzība, drošība, privātums, Vispārīgā datu aizsardzības regula

Keywords: human rights, data protection, security, privacy, GDPR

Ievads[1]

Personas datu aizsardzība nav īstenojama bez datu drošības. Vispārīgā datu aizsardzības regula[2] (turpmāk – Regula) paredz datu drošību kā vienu no pamatprasībām, kas jānodrošina ikvienam uzņēmumam, iestādei un organizācijai, kas apstrādā Eiropas Savienībā (turpmāk – ES) esošu datu subjektu personas datus. Raksta mērķis ir analizēt drošības jēdzienu un tā ietekmi uz datu aizsardzības tiesību attīstību. Tajā izvērtēti drošības, kiberdrošības un informācijas drošības jēdzieni, kā arī atklāts, kā šie jēdzieni ir saistīti ar datu aizsardzību. Rakstā pamatots, kā jaunais ES datu aizsardzības regulējums vēl vairāk sasaista drošību un datu aizsardzību divos veidos. Pirmkārt, tajā apskatīts, kā Regula ievieš uz risku balstītu

[1] Darbs izstrādāts ERAF specifiskā atbalsta mērķa 1.1.1.2. pasākuma "Pēcdoktorantūras pētniecības atbalsts" projekta 1.1.1.2./VIAA1/1/16/001 pētniecības pieteikuma Nr.1.1.1.2./VIAA/1/16/196 "Taisnīgs līdzsvars starp privātumu un drošību kibertelpā: stingru datu aizsardzības standartu izveide Eiropā" ietvaros.

[2] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula). Pieņemta 04.27.2016. [20.03.2019. red.].

pieeju, kas ir pazīstama un tiek piemērota informācijas drošības jomā, kā būtisku elementu arī datu aizsardzības jomā. Otrkārt, autore darbā analizē personas datu aizsardzības pārkāpumu paziņošanas pienākums, kuru Regula ievieš kā jaunu prasību.

1. Drošības jēdziens

Drošība tiek definēta kā stāvoklis, kad nepastāv briesmas vai draudi.[3] Drošība vienmēr ir saistīta ar kādu risku, ar tā pareizu novērtēšanu un atbilstošu pasākumu izvēlēšanos, lai šo risku samazinātu vai novērstu. Drošība ir nevis gala stāvoklis, bet process, lai saglabātu risku pieņemamā stāvoklī.[4]

Drošība ir plašs jēdziens. Var izšķirt nacionālo jeb valsts drošību, sabiedrības drošību, kā arī cilvēku jeb personisko drošību. Dažādos vēstures posmos ir bijusi sadursme starp šiem drošības jēdzieniem. Tā sauktā tradicionālā drošības paradigma par prioritāru atzīst nacionālo un valsts drošību, kurā drošība tiek uzskatīta par valsts spēju aizsargāt sevi pret ārējiem draudiem. Personiskā drošības paradigma par drošības galveno aizsargājamo objektu izvirza nevis valsti, bet indivīdu. Liela daļa Apvienoto Nāciju Organizācijas (turpmāk – ANO) drošības stratēģiju, kā arī Eiropas stratēģija sociālās aizsardzības jomā ir balstīta uz personisko drošības doktrīnu. Sociālās drošības paradigma izvirza sabiedrību par centrālo drošības draudu objektu, risinot tādas problēmas kā globālā nabadzība un attīstības trūkums, kas tika īpaši akcentētas tūkstošgades mijā. Tomēr minētā pieeja beidzās pēc sekojošiem teroristu uzbrukumiem, jo īpaši pēc 11. septembra terorakta un starptautisko teroristu grupu pieauguma. To rezultātā notika atgriešanās pie "sākotnējās" drošības izpratnes, kuras galvenais mērķis ir aizsargāt publisko sfēru, kas ļauj piemērot slepenus un nepārredzamus drošības un uzraudzības pasākumus, tos attaisnojot ar tā sauktajiem "ārkārtas" apstākļiem.[5] Līdzās minētajiem trim drošības veidiem atkarībā no konkrētā apdraudējuma veida var tikt izdalītas arī tādas drošības jomas kā, piemēram, ekonomiskā, militārā, veselības, vides un politiskā drošība.[6]

Skatoties no tiesību viedokļa, tiesības uz drošību ir patstāvīgas cilvēktiesības, kas noteiktas starptautiskos cilvēktiesību dokumentos, paredzot valsts pozitīvo pienākumu aizsargā šīs tiesības, piemēram, Eiropas Padomes 1950. gada Eiropas Cilvēktiesību un pamatbrīvību konvencijas[7] (turpmāk – ECTK) 5. pantā, ANO 1966. gada Starptautiskā pakta par pilsoniskajām un politiskajām tiesībām 9. pantā.[8]

---

[3] English Oxford Dictionary. Security. Pieejams: https://en.oxforddictionaries.com/definition/security [aplūkots 20.03.2019.].

[4] Sk.: Handbook on Security of Personal Data Protection. ENISA, 2017. Pieejams: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing [aplūkots 20.03.2019.].

[5] Ethics of Security and Surveillance Technologies. European Commission, 2014, pp. 64–66. Pieejams: https://publications.europa.eu/en/publication-detail/-/publication/6f1b3ce0-2810-4926-b185-54fc3225c969 [aplūkots 20.03.2019.].

[6] Sīkāk sk.: Raab Ch D. Privacy as a Security Value. In: Jon Bing: En Hyllest A Tribute, Norway: Gyldendal Norsk Forlag AS. 2014. Pieejams: https://ssrn.com/abstract=3057433 [aplūkots 21.03.2019.].

[7] Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija. Pieņemta 04.11.1950. [20.03.2019. red.].

[8] Starptautiskais pakts par pilsoņu un politiskajām tiesībām. Pieņemts 16.12.1966. [21.03.2019. red.].

Viena no drošības sastāvdaļām ir kiberdrošība. Tai sāka pievērst uzmanību līdz ar aizvien plašāku interneta izmantošanu, kas radīja jaunus riskus un apdraudējumus. Kiberdrošība attiecas uz drošību kibertelpā un interneta vidē.

Kiberdrošību var aplūkot plašākā un šaurākā nozīmē. Plašākā nozīmē kiberdrošība ietver dažādus draudus kibertelpā, kā arī pasākumus, lai tos novērstu, kas skar vairākas jomas – tehnoloģijas, tiesības, cilvēktiesības, ekonomiku, psiholoģiju, socioloģiju, politiku, diplomātiju, militāro jomu.[9] Gan pasaules, gan Eiropas, gan nacionālā līmenī ir pieņemti daudzi tiesību akti, kā arī veikti pasākumi un iniciatīvas kiberdrošības jomā, jo īpaši attiecībā uz kibernoziegumu apkarošanu, no kuriem viens no nozīmīgākajiem ir Eiropas Padomes Konvencija par kibernoziegumiem.[10]

Savukārt šaurākā nozīmē kiberdrošība attiecas uz informācijas sistēmu drošību un spēju tās aizsargāt pret kiberuzbrukumiem un kibernoziegumiem. Informācijas drošība ir definēta kā trīs galveno informācijas aspektu saglabāšana kibertelpā: konfidencialitātes, integritātes un pieejamības.[11] Šajā nozīmē tā ietver visus pasākumus, lai aizsargātu sistēmā apstrādāto informāciju no neatļautas piekļuves tai, nozaudēšanas, iznīcināšanas, pārveidošanas.[12]

Pirmais ES mēroga kiberdrošības akts ir 2016. gada maijā pieņemtā tīklu un informācijas sistēmu drošības direktīva jeb tā saucamā NIS direktīva.[13] Nākamais nozīmīgais sasniegums ir Kiberdrošības akts, kas paredz ieviest ES mēroga kiberdrošības sertifikāciju, lai nodrošinātu, ka IKT produkti, pakalpojumi un procesi atbilst drošības standartiem, kā arī stiprināt ES Kiberdrošības aģentūras ENISA pilnvaras.[14]

2. Attiecības starp drošību un datu aizsardzību

Drošība un datu aizsardzība ir gan savstarpēji papildinošas, gan pretējas vērtības. Drošība ir viens no iemesliem, uz kura pamata var ierobežot tiesības uz datu aizsardzību. Tiesības uz datu aizsardzību Eiropā ir patstāvīgas cilvēktiesības, kas līdz ar informācijas sabiedrības un tehnoloģiju attīstību pakāpeniski attīstījās no

[9] Sīkāk sk.: Definition of Cybersecurity – Gaps and overlaps in standardisation. ENISA, 2015. Pieejams: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [aplūkots 20.03.2019.].

[10] Konvencija par kibernoziegumiem. Pieņemta 23.11.2001. [21.03.2019. red.].

[11] Sk.: Guidelines for SMEs on the security of personal data processing. ENISA. 2016. Pieejams: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing [aplūkots 20.03.2019.].

[12] Sk.: ENISA overview of cybersecurity and related terminology. ENISA, 2017. Pieejams: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology [aplūkots 20.03.2019.].

[13] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. Pieņemta 06.07.2016. [21.03.2019. red.].

[14] Eiropas Parlamenta nostāja, pieņemta pirmajā lasījumā 12.03.2019., lai pieņemtu Eiropas Parlamenta un Padomes Regulu (ES) 2019/... par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju un ar ko atceļ Regulu (ES) 526/2013 (Kiberdrošības akts). Pieejams: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0151+0+DOC+XML+V0//LV [aplūkots 20.03.2019.].

tiesībām uz privāto dzīvi.[15] Gan starptautiskajos cilvēktiesību dokumentos, piemēram, ECTK 8. panta otrajā daļā, gan Latvijas Republikas Satversmes[16] 116. pantā valsts drošība un sabiedrības drošība ir noteikta kā pamats, kas ļauj ierobežot cilvēktiesības, tai skaitā tiesības uz datu aizsardzību.

Regulas 23. panta pirmā daļa paredz, ka ar ES vai dalībvalsts tiesību aktiem var piemērot ierobežojumus konkrētiem principiem un datu subjektu tiesībām, kā arī tos var piemērot attiecībā uz ziņošanu datu subjektam par personas datu aizsardzības pārkāpumiem un attiecībā uz dažiem ar to saistītiem pārziņu pienākumiem, ciktāl tas demokrātiskā sabiedrībā ir nepieciešami un samērīgi, lai garantētu svarīgus ES un dalībvalsts vispārējo sabiedrības interešu mērķus, cita starpā valsts drošību, aizsardzību, sabiedrisko drošību, noziedzīgu nodarījumu novēršanu, izmeklēšanu un saukšanu pie atbildības par tiem vai kriminālsodu izpildi, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu.

Drošība ir pamatā speciālajam datu aizsardzības regulējumam, kas paredz atšķirīgas datu aizsardzības prasības. Vienlaicīgi ar Datu aizsardzības regulu tika pieņemta tā saucamā Policijas direktīva,[17] kas paredz īpašus noteikumus attiecībā uz personas datu apstrādi, ko veic tiesībaizsardzības iestādes, lai izmeklētu un atklātu noziedzīgus nodarījumus. Respektējot šo darbību īpašo raksturu, ir pamatoti ierobežot personu tiesības, piemēram, tiesības uz informāciju un piekļuvi datiem.

Lai tiesību ierobežojumi būtu tiesiski, tiem ir jāatbilst cilvēktiesību ierobežošanas kritērijiem un ir jābūt stingri nepieciešamiem un samērīgiem.[18] Tomēr ne visos gadījumos piemērotie pasākumi un tiesību akti, kas pieņemti drošības nolūkos, ir stingri nepieciešami un samērīgi. Vairāki tiesību akti, kas šobrīd tiek izstrādāti ES, ir izpelnījušies plašu kritiku un iebildumus, kā, piemēram, priekšlikums regulai par personas apliecību un citu dokumentu drošības uzlabošanu, kas paredz biometrisko datu apstrādi,[19] pasažieru datu vākšanas sistēma ES, kā arī ārpus ES,[20] priekšlikums regulai, ar ko groza vīzu informācijas sistēmu[21] u. c. Attiecībā uz

---

[15] Eiropas Savienības Pamattiesību harta atšķirībā no citiem agrāk pieņemtajiem starptautiskiem cilvēktiesību dokumentiem ne tikai paredz tiesības uz privātās dzīvi (7. pants), bet arī atsevišķi kā patstāvīgas cilvēktiesības nosaka tiesības uz personas datu aizsardzību (8. pants). Eiropas Savienības Pamattiesību harta. Pieņemta 12.12.2007. [21.03.2019. red.].
Par datu aizsardzības tiesību attīstību sīkāk sk.: Handbook on European data protection law – 2018 edition. FRA, 2018, pp. 18–19. Pieejams: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law [aplūkots 21.03.2019.].

[16] Latvijas Republikas Satversme: LV likums. Pieņemts 15.02.1922. [20.03.2019. red.].

[17] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI. Pieņemta 27.04.2016. [21.03.2019. red.].

[18] Eiropas Savienības Pamattiesību hartas 52. panta pirmā daļa paredz, ka tiesību un brīvību izmantošanas ierobežojumiem ir: • jābūt noteiktiem tiesību aktos; • jārespektē tiesību un brīvību būtība; • jāatbilst vispārējas nozīmes mērķiem, ko atzinusi ES, vai vajadzībai aizsargāt citu personu tiesības un brīvības; • jābūt nepieciešamiem; • jābūt samērīgiem.

[19] Eiropas Datu aizsardzības uzraudzītāja atzinuma kopsavilkums par priekšlikumu regulai par Savienības pilsoņu personas apliecību un citu dokumentu drošības uzlabošanu, 2018. ES OV, 21.09.2018., C 338/12. Pieejams: https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_summary_lv_0.pdf [aplūkots 20.03.2019.].

[20] Fundamental rights report 2018. FRA, p. 159, 166. Pieejams: https://fra.europa.eu/en/publications-and-resources/publications/annual-reports/fundamental-rights-2018 [aplūkots 20.03.2019.].

[21] The revised Visa Information System and its fundamental rights implications. FRA Opinion, 2/2018. Pieejams: https://fra.europa.eu/en/opinion/2018/visa-system [aplūkots 20.03.2019.].

dalībvalstu līmenī veiktajiem drošības pasākumiem šobrīd plašas diskusijas ir par videonovērošanas sistēmām, kas izmanto jaunākās sejas atpazīšanas tehnoloģijas, kuras tiek testētas vairākās ES valstīs, piemēram, Apvienotajā Karalistē, Vācijā un Francijā,[22] salīdzinot tās ar Ķīnas digitālo uzraudzības sistēmu.

Drošība un datu aizsardzība ir ne tikai pretējas, bet arī savstarpēji papildinošas vērtības. Personas datu aizsardzība nav īstenojama bez datu drošības nodrošināšanas.

Aplūkojot, kā kiberdrošība šaurākā nozīmē jeb informācijas drošība ir saistīta ar datu aizsardzību, no vienas puses, informācijas drošība ir plašāka, jo tā ietver ne tikai personas datus, tas ir, informāciju, kas attiecas uz identificētu vai identificējamu fizisku personu, bet visu veidu datus. Iestādēm un uzņēmumiem var būt vienlaicīgi saistošas gan Regulā noteiktās drošības prasības, kas attiecas uz personas datu aizsardzību, gan prasības, kas ietvertas citos tiesību aktos, kuri attiecas uz informācijas tehnoloģiju drošību, piemēram, tā sauktās NIS direktīvas prasības.

No otras puses, drošība ir šaurāka par datu aizsardzību, jo datu aizsardzība ietver arī daudzas citas prasības. Regulas 5. pantā drošības princips ir noteikts kā viens no septiņiem datu aizsardzības principiem līdzās tādiem principiem kā likumīgums, godprātība un pārredzamība, nolūka ierobežojumi, datu minimizēšana, precizitāte, glabāšanas ierobežojumi un pārskatatbildība.

Regulējot datu aizsardzības principus, Regulas 5. panta 1. daļas f) punkts nosaka tikai divas no trim drošības prasībām – integritāti un konfidencialitāti, neiekļaujot trešo pazīmi – pieejamību. Tomēr Regulas 32. pants, kas paredz personas datu apstrādes drošības prasības, uzsver nepieciešamību atjaunot personas datu pieejamību, tādējādi ietverot arī šo informācijas drošības aspektu.

Regula paredz drošību kā vienu no pamatprasībām, kas uzlikta datu pārzinim un apstrādātājam. Iepriekš spēkā esošā ES Datu aizsardzības direktīva[23] noteica personas datu drošību kā vienu no pienākumiem datu pārzinim. Regula pastiprina minēto pienākumu pēc būtības, kā arī attiecina to tiešā veidā arī uz datu apstrādātāju.[24]

Atsevišķos gadījumos personas datu drošība var nonākt pretrunā ar datu aizsardzības prasībām. Piemēram, drošības pasākums – sistēmas auditācijas pieraksti, kas ļauj izsekot notikumiem informācijas sistēmā vai lietotāju darbībām un tiek izmantoti, lai atklātu drošības incidentus, – var tikt izmantots arī datu subjektu uzraudzībai vai novērošanai. Reģistrēšana un uzraudzība nebūtu izmantojama kā veids, kā uzraudzīt, izsekot un profilēt lietotājus. Tādējādi, izvēloties atbilstošākos drošības pasākumus, var arī būt nepieciešams nodrošināt līdzsvaru starp drošības un privātuma prasībām.[25]

---

[22] Kharpal A. Facebook's facial recognition technology may not meet strict new EU data rules, a top watchdog says. 19.04.2018. Pieejams: https://www.cnbc.com/2018/04/19/facebooks-facial-recognition-may-not-meet-gdpr-rules.html [aplūkots 20.03.2019.].

[23] Eiropas Parlamenta un Padomes Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. Pieņemta 24.10.1995. [red. spēkā līdz 24.05.2018.].

[24] Sk.: Guidelines for SMEs on the security of personal data processing. ENISA, 2016.

[25] Reinforcing trust and security in the area of electronic communications and online services – Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing. ENISA, 2018, p. 33. Pieejams: https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services [aplūkots 20.03.2019.].

3. Kā jaunais ES datu aizsardzības regulējums sasaista drošību un datu aizsardzību?

Jaunais ES datu aizsardzības regulējums vēl vairāk sasaista datu aizsardzību un drošību, pirmkārt, ieviešot uz risku balstītu pieeju, un, otrkārt, ieviešot pārkāpumu paziņošanas pienākumu.

Regula ievieš uz risku balstītu pieeju, kas ir labi pazīstama un tiek piemērota informācijas drošības jomā, kā būtisku elementu arī datu aizsardzības jomā. Regula paredz, ka pārzinim un apstrādātājam ir jānovērtē apstrādei raksturīgais risks un jāīsteno atbilstoši tehniskie un organizatoriskie pasākumi, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam (32.1. p.).[26] Regula nosaka uz risku balstītu pieeju un uzliek pienākumu ikvienam uzņēmumam un organizācijai novērtēt apstrādei raksturīgos riskus un īstenot atbilstošus pasākumus, kas būtu piemēroti, lai šos riskus mazinātu un novērstu, ievērojot: jo augstāks ir risks, jo stingrāki pasākumi jāveic (83. apsvērums).

Pārzinim un apstrādātājam ir pašam jāizvērtē un jānosaka, kādi "atbilstoši pasākumi" ir īstenojami, ņemot vērā tehnikas līmeni (angļu val. – *the state of the art*), īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un smaguma pakāpes risku attiecībā uz fizisku personu tiesībām un brīvībām (Regulas 32. p.). Tātad, izvēloties atbilstošus drošības pasākumus, ir jāņem vērā apstrādes iespējamības un smaguma risks tieši "attiecībā uz fizisku personu tiesībām un brīvībām". Tomēr, kaut arī ekonomiski ir iespējams aprēķināt, cik uzņēmumam var izmaksāt drošības pārkāpums, daudz grūtāk ir novērtēt tā ietekmi uz "personas tiesībām un brīvībām".[27]

Regula paredz ņemt vērā risku, ne tikai izvēloties atbilstošus drošības pasākumus, bet arī izpildot citas Regulas prasības. Regula nosaka vispārīgu pienākumu novērtēt apstrādes darbību risku attiecībā uz datu subjekta tiesībām un brīvībām ikvienā datu apstrādes gadījumā (24.1. p.). Turklāt Regulas 35. pants paredz, ka situācijās, kad apstrāde var radīt augstu risku, pārzinim ir pienākums veikt novērtējumu par ietekmi uz datu aizsardzību, kurā tiek izvērtēta ne tikai apstrādes atbilstība drošības prasībām, bet arī visiem pārējiem Regulā noteiktajiem principiem. Pasākumi, kas var būt nepieciešami, lai risku mazinātu, var būt gan drošības pasākumi, gan arī cita veida pasākumi, piemēram, ievākto datu apjoma un glabāšanas termiņa samazināšana, speciālista nozīmēšana, personu informēšana un piekrišanas saņemšana utt.

Otrs veids, kā Regula savieno datu aizsardzību ar drošību ir, kā vienu no drošības prasībām ieviešot personas datu aizsardzības pārkāpumu paziņošanas pienākumu. Pēc būtības personas datu aizsardzības pārkāpums ir drošības pārkāpums,

[26] Regulas 32. panta 1. punktā ir uzskaitīti drošības pasākumi, kas, cita starpā, var tikt īstenoti: a) personas datu pseidonimizācija un šifrēšana; b) spēja nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību; c) spēja laicīgi atjaunot personas datu pieejamību un piekļuvi gadījumā, ja ir noticis fizisks vai tehnisks negadījums; d) process regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību.

[27] Schneier B. Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World. New York, London: W. W. Norton & Company, 2015, p. 166.

kas skar personas datus.[28] Ne katrs informācijas drošības incidents ir personas datu aizsardzības pārkāpums, bet katrs personas datu aizsardzības pārkāpums ir informācijas drošības incidents. Ja tiek ietekmēti personas dati, incidents tiks uzskatīts par personas datu aizsardzības pārkāpumu.

Regula uzliek pienākumu datu pārzinim 72 stundu laikā paziņot par šādiem pārkāpumiem gan uzraudzības iestādei, gan, ja pastāv augsts risks, personām (33., 34. p.). Lai gan šāds pienākums nebija iepriekš paredzēts ES Datu aizsardzības direktīvā, tajā pašā laikā tas nav jaunums ES tiesiskajā regulējumā. Tas ir paredzēts un var pārklāties ar citos ES tiesību aktos paredzēto pārkāpumu paziņošanas pienākumu, piemēram, tā saucamo E-privātuma direktīvu,[29] kas paredz šādu pienākumu attiecībā uz telekomunikāciju pakalpojumu sniedzējiem (4. p.), NIS direktīvu, kas uzliek pienākumu paziņot drošības pārkāpumus pamatpakalpojumu, piemēram, enerģētikas, banku, transporta pakalpojumu sniedzējam, kā arī digitālo pakalpojumu sniedzējiem (16.3. p.).

Regulā noteiktais paziņošanas pienākums un ar to saistītais risku izvērtējums atšķiras no citos tiesību aktos noteiktā paziņošanas pienākuma. Atšķirībā no Regulas, kas uzliek pienākumu paziņot uzraudzības iestādei par jebkāda veida personas datu aizsardzības pārkāpumu, kas "varētu radīt risku fizisku personu tiesībām un brīvībām" (33.1. p.), NIS direktīva uzliek pienākumu paziņot par jebkuru incidentu, kam ir "būtiska ietekme uz tā pakalpojuma sniegšanu" (16.3. p.). Tādējādi Regula paredz novērtēt risku attiecībā uz fizisko personu tiesībām un brīvībām, savukārt NIS direktīva paredz izvērtēt "ietekmi uz pakalpojumu sniegšanas nepārtrauktību".

Drošības pārkāpumi ir vieni no biežākajiem iemesliem nopietniem privātuma un datu aizsardzības pārkāpumiem, kas var radīt būtiskas negatīvas – fiziskas, psiholoģiskas un materiālas – sekas personām. Kopš Regulas piemērošanas sākuma pirmajos astoņos mēnešos ES dalībvalstu uzraudzības iestādes saņēma paziņojumus par vairāk nekā 59 tūkstošiem personas datu aizsardzības pārkāpumu.[30]

Jaunais ES datu aizsardzības regulējums, tai skaitā uz risku balstītā pieeja un pārkāpumu paziņošanas pienākums, ir sākumpunkts attieksmes maiņai pret datu aizsardzību un drošību. Šī attieksmes maiņa ir ieviesta ar pārskatatbildības principu – tas ir jauns princips, kas noteikts Regulā un kas uzliek pienākumu katram uzņēmumam, iestādei un organizācijai veikt atbilstošus pasākumus, lai ne tikai nodrošinātu, bet arī spētu uzskatāmi parādīt jeb pierādīt atbilstību datu aizsardzības prasībām (Regulas 5. p. 2. d.). Atslēgvārds ir atbildība, kam ir jābūt pamatā gan datu izmantošanai un pārvaldībai, gan arī jauno tehnoloģiju, kā mākslīgā intelekta, attīstīšanai un piemērošanai.

---

[28] Regulas 4. panta 12. punkts "personas datu aizsardzības pārkāpumu" definē kā drošības pārkāpumu, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

[29] Eiropas Parlamenta un Padomes Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju). Pieņemta 07.12.2002. [21.03.2019. red.].

[30] DLA Piper GDPR Data Breach Survey: February 2019. Pieejams: https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/ [aplūkots 21.03.2019.].

Kopsavilkums

1. Drošība vienmēr ir saistīta ar risku, ar tā pareizu novērtēšanu un atbilstošu pasākumu izvēlēšanos, lai šo risku samazinātu vai novērstu. Drošība ir plašs jēdziens, kas ietver valsts drošību, sabiedrības drošību, personisko drošību un citus drošības veidus. Kiberdrošība ir drošības sastāvdaļa, kas plašākā nozīmē ietver dažādus draudus kibertelpā un pasākumus, lai tos novērstu, un kas skar dažādas jomas – tehnoloģijas, tiesības, ekonomiku, socioloģiju, politiku, diplomātiju, militāro jomu u. c., savukārt šaurākā nozīmē tā attiecas uz informācijas sistēmu drošību un spēju tās aizsargāt pret kiberuzbrukumiem un kibernoziegumiem.
2. Drošība un datu aizsardzība ir gan savstarpēji papildinošas, gan pretējas vērtības. Drošība ir viens no iemesliem, uz kura pamata var ierobežot tiesības uz datu aizsardzību. Tā ir pamatā speciālajam datu aizsardzības regulējumam, kas paredz atšķirīgas datu aizsardzības prasības. Tomēr ES un nacionālajā līmenī veiktie pasākumi un pieņemtie tiesību akti, kas paredz plašu personas datu apstrādi un nodošanu drošības nolūkos, ne vienmēr ir stingri nepieciešami un samērīgi, piemēram, pašlaik plašas diskusijas ir par videonovērošanas sistēmām, kas izmanto sejas atpazīšanas tehnoloģijas.
3. Personas datu aizsardzība viennozīmīgi nav īstenojama bez datu drošības nodrošināšanas. No vienas puses, kiberdrošība šaurākā nozīmē jeb informācijas drošība ir plašāka, jo tā ietver ne tikai personas datus, bet visu veidu datus. No otras puses, drošība ir šaurāks jēdziens par datu aizsardzību, jo datu aizsardzība ietver daudzas citas prasības un drošības princips ir tikai viens no septiņiem Regulā noteiktajiem datu aizsardzības principiem. Tajā pašā laikā atsevišķi drošības pasākumi, piemēram, auditācijas pieraksti un uzraudzība, var nonākt pretrunā ar datu aizsardzības prasībām, tāpēc, izvēloties atbilstošākos drošības pasākumus, var būt nepieciešams nodrošināt līdzsvaru starp drošības un datu aizsardzības prasībām.
4. Jaunais ES datu aizsardzības regulējums vēl vairāk sasaista datu aizsardzību un drošību, pirmām kārtām ieviešot uz risku balstītu pieeju, kas ir labi pazīstama un tiek piemērota informācijas drošības jomā, kā būtisku elementu arī datu aizsardzības jomā. Regula paredz ņemt vērā risku, ne tikai izvēloties atbilstošus drošības pasākumus, bet ikvienā datu apstrādes gadījumā, turklāt situācijās, kad apstrāde var radīt augstu risku, pārzinim ir pienākums veikt novērtējumu par ietekmi uz datu aizsardzību. Otrs veids, kā Regula sasaista datu aizsardzību un drošību, ir ieviešot personas datu aizsardzības pārkāpumu paziņošanas pienākumu. Citi ES tiesību akti, piemēram, NIS direktīva, nosakot pārkāpumu paziņošanas pienākumu, paredz būtiski atšķirīgu pieeju attiecībā uz risku izvērtēšanu.
5. Jaunais ES datu aizsardzības regulējums ir sākumpunkts attieksmes maiņai pret datu aizsardzību un drošību. Šī attieksmes maiņa ir ieviesta ar pārskatatbildības principu, kas ir jauns princips, kurš noteikts Regulā. Atbildība ir pamatā gan datu izmantošanai un pārvaldībai, gan arī jauno tehnoloģiju, kā mākslīgā intelekta, attīstīšanai un piemērošanai.