

9. oktoobri 2024. aasta avalik arutelu nr 2024-20 raamistiku kohta, milles sätestatakse minimaalsed tehnilised nõuded vanusekontrollisüsteemidele, mis on loodud juurdepääsuks teatavatele internetipõhiste avalikele sideteenustele ja videojagamisplatvormidele, mis teevad pornograafilise sisu üldsusele kättesaadavaks

NOR: RCAC2428286X

JORF nr 0251, 22. oktoober 2024. a.. a.

Tekst nr 50

- Lisa

Audiovisuaal- ja digikommunikatsiooni reguleeriv asutus
võttes arvesse Euroopa Parlamendi ja nõukogu 9. septembri 2015. aasta direktiivi
(EL) 2015/1535, millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste
eeskirjadest teatamise kord,
võttes arvesse 21. juuni 2004. aasta seadust nr 2004-575, muudetud kujul, usalduse kohta
digitaalmajanduses, eriti selle artikleid 10 ja 10-2,
võttes arvesse 15. aprillil 2024 Euroopa Komisjonile saadetud teatist nr 2024/0208/FR ja selle
15. juuli 2024 tähelepanekuid,
võttes arvesse Prantsusmaa andmekaitseasutuse (Commission nationale de l'informatique et
des libertés) 26. septembri 2024. aasta avalikku arutelu nr 2024-067, milles esitatakse
arvamus audiovisuaal- ja digikommunikatsiooni reguleeriva asutuse raamistiku eelnõu kohta,
mis käsitleb vanusekontrollisüsteeme, mis on loodud juurdepääsuks teatavatele teenustele,
mis võimaldavad juurdepääsu pornograafilisele sisule,
võttes arvesse 11. aprillist kuni 11. maini 2024 toimunud avaliku konsultatsiooni käigus
esitatud märkusi,

olles asja kaalunud,
otsustab käesolevaga järgmist:

Artikkel 1

Võetakse vastu käesoleva otsuse lisas sätestatud raamistik.

Artikkel 2

Käesolev avalik arutelu avaldatakse Prantsuse Vabariigi Teatajas.

Lisa

LISA

RAAMISTIK, MILLEGA MÄÄRATAKSE KINDLAKS MINIMAALSED TEHNILISED NÕUDED VANUSEKONTROLLISÜSTEEMIDELE, MIS ON LOODUD JUURDEPÄÄSUKS TEATAVATELE INTERNETIPÕHISTELE AVALIKELE SIDETEENUSTELE JA VIDEOJAGAMISPLATVORMIDELE, MIS TEEVAD PORNOGRAAFILISE SISU ÜLDSUSELE KÄTTESAADAVAKS

Sisukord

Sissejuhatus

Pornograafilist sisu edastavate suunatud teenuste vastutus

ARCOMi rolli areng seaduse kontekstis, et tagada ja reguleerida digitaalset ruumi

Töö, mis on vanuse tõendamisel juba käimas

Raamistiku tutvustus

Sektori toetamine vanusekontrolli lahenduste rakendamisel

Raamistiku ajakohastamine ja tehnika tase

Raamistiku struktuur ja rakendamise ajakava

Esimene osa: Üldised kaalutlused vanusekontrollisüsteemide usaldusväärsuse kohta

Teine osa: Eraelu puutumatuse kaitse

Eraelu puutumatuse kaitse põhimõtted

Eraelu puutumatust toetava vanusekontrollisüsteemi rakendamine vaikimisi ja kavandatult

Kõikide vanusekontrollisüsteemide miinimumnõuded

1. Vanusekontrollisüsteemi pakkuja sõltumatus suunatud teenuste edastatavast pornograafilisest sisust

2. Pornograafilist sisu edastavate suunatud teenuste konfidentsiaalsus

3. Konfidentsiaalsus vanuse tõendamise teenuseosutajate suhtes

4. Konfidentsiaalsus mis tahes kolmanda isiku suhtes, kes osaleb vanuse kontrollimise protsessis

5. Vanusetõendajate meetmed üksikisikute õiguste ja vabaduste kaitseks

Erinõuded eraelu puutumatuse kaitse süsteemidele, mis järgivad topeltanonüümsuse põhimõtet

6. Konfidentsiaalsus suunatud teenuste suhtes, mis edastavad pornograafilist sisu

7. Suurem konfidentsiaalsus vanusetunnuste väljaandjate suhtes

8. Tõhusam konfidentsiaalsus mis tahes kolmanda isiku suhtes, kes osaleb vanuse kontrollimise protsessis

9. Kättesaadavus ja elanikkonna hõlmatus

Kasutajate teavitamine vanusekontrollisüsteemidega seotud eraelu puutumatuse tasemest

10. Kasutaja privaatsuse kaitse taseme selgesõnaline kuvamine

Soovitud eesmärgid ja parimad tavad

Kolmas osa: Erandlikud tõendeid tekitavad lahendused, mida aktsepteeritakse ajutiselt

Neljas osa: Vanusekontrollilahenduste auditeerimine ja hindamine

Tegelikes tingimustes kasutusele võetud süsteemide hindamine

Veamäärad, kõrvalehoidmine ja ründeoht

Audiitori sõltumatus

Sissejuhatus

Pornograafilist sisu edastavate suunatud teenuste vastutus

1. Laste internetile juurdepääsu võimaldavate mobiilseadmete demokratiseerimisega kasvab kiiresti alaealiste kokkupuude pornograafilise sisuga internetis.

Audiovisuaal- ja digikommunikatsiooni reguleeriva asutuse (Arcom) poolt Médiamétrie esitatud andmete põhjal läbi viidud uuringu kohaselt külastab pornograafilisi saite igal kuul 2,3 miljonit alaealist, kusjuures see arv on viimastel aastatel kiiresti kasvanud ja seotud mobiilseadmete demokratiseerimisega laste seas. Täisealistele mõeldud saite külastavate alaealiste osakaal on viie aastaga suurenenud 9 protsendipunkti võrra, 19 %-lt 2017. aasta lõpus 28 %-le 2022. aasta lõpus. 2022. aastal külastasid selliseid saite igal kuul enam kui pooled 12-aastastest ja vanematest poistest ning see näitaja tõuseb 16- ja 17-aastaste poiste puhul kahe kolmandikuni. Keskmiselt 12 % täiskasvanutele suunatud veebisaitide vaatajaskonnast moodustavad alaealised (1).

Alates 2000. aastate algusest (2) näitavad pornograafiaga varajase kokkupuute tagajärgede uurimise tulemused, et kõige nooremate laste kokkupuutel pornograafilise sisuga võivad olla tõsised tagajärjed nende vaimsele arengule ja pildile, mille nad kujundavad seksuaalsusest ja inimestevahelistest suhetest, mis kahjustab nende isiklikku arengut ja suuremat võrdõiguslikkust sugudevahelistes suhetes (3).

2. Alates 1. märtsist 1994 on 22. juuli 1992. aasta seadusega nr 92–684 kehtestatud karistusseadustiku artikli 227-24 sätete kohaselt keelatud lasta alaealistel pornograafilise sisuga kokku puutuda.

Kõnealuse artikli sõnastust on muudetud, et selgitada mitte ainult selle kohaldamisala, vaid ka seda, kuidas seda tuleb hinnata, kui õigusrikkumine internetis registreeritakse. Kooskõlas väljakujunenud kohtupraktikaga on alates 2020. aastast artiklis 227-24 sätestatud, et üksnes vanuse deklareerimisest ei piisa täisealiseks saamise tõendamiseks (4). Praegu kehtiv sõnastus on järgmine.

„Vägivaldse, terrorismile õhutava, pornograafilise iseloomuga sõnumi, sealhulgas ühe või mitme loomaga seotud pornograafilise kujutise, sealhulgas inimväärikust tõsiselt kahjustavate või neid füüsiliselt ohustavate mängude või sellise sõnumi tootmise, transpordi, mis tahes viisil levitamise ja sõltumata andmekandja liigist, karistatakse kolmeaastase vangistuse ja 75 000 euro suuruse rahatrahviga, kui tõenäoliselt näeb või tajub sõnumit alaealine.

„Kui käesolevas artiklis sätestatud õigusrikkumised esitatakse trüki- või audiovisuaalajakirjanduses või internetis üldsusele edastamise teel, kohaldatakse neid küsimusi reguleerivate õigusaktide erisätteid vastutavate isikute kindlaksmääramise suhtes.

„Käesolevas artiklis sätestatud õigusrikkumised on käsitatavad ka juhul, kui alaealise juurdepääs esimeses lõigus osutatud sõnumitele tuleneb üksnes alaealise kinnitusest, et ta on vähemalt 18-aastane.“

Seadusandja kehtestas 30. juuli 2020. aasta seadusega nr 2020-936 koduvägivalla ohvrite kaitsmiseks Arcomi hõlmava erimenetluse, mille eesmärk on tagada nende sätete täielik tõhusus internetipõhiste avalike kommunikatsiooniteenuste kohta, millega tehakse pornograafiline sisu internetis üldsusele kättesaadavaks.

Seega anti selle seadusega Arcomi presidendile õigus saata veebisaidi avaldajale ametlik teade karistusseadustiku järgimiseks ja kui seda teadet ei täideta, paluda kohtunikul anda Interneti-ühenduse pakkujale (IAP) korraldus takistada juurdepääsu sellele saidile.

3. Nende sätete alusel väljastas amet 13 ametlikku teadet. See edastas küsimuse ka 8. märtsil 2022 Pariisi kohtu esimehele, et kohustada IAPsid ametliku korraldusega blokeerima viis neist teenustest. See menetlus on käesoleva raamistiku avaldamise kuupäeval veel pooleli.

ARCOMi rolli areng seaduse kontekstis, et tagada ja reguleerida digitaalset ruumi

21. mai 2024. aasta seadusega nr 2024-449 digiruumi turvalisuse ja reguleerimise kohta (SREN) ajakohastati 30. juuli 2020. aasta seadusega kehtestatud süsteemi.

21. juuni 2004. aasta seaduse nr 2004-575 (usalduse kohta digitaalmajanduses) (LCEN) artiklis 10 on sätestatud, et ARCOM „loob ja avaldab [...], olles konsulteerinud Prantsusmaa andmekaitseasutusega, vanusekontrollisüsteemide suhtes kohaldatavate tehniliste miinimumnõuete kindlaksmääramise raamistikku. Need nõuded käsitlevad kasutajate vanuse tõendamise usaldusväärsust ja nende privaatsuse austamist.“ Süsteemi kohaldamisalaks on „pornograafiline sisu, mille on üldsusele kättesaadavaks teinud üldkasutatava sideteenuse osutaja oma toimetust vastutusele või mida pakub videojagamispaltvormi teenus 30. septembri 1986. aasta seaduse nr 86–1067 (kommunikatsioonivabaduse kohta) artikli 2 tähenduses“ (edaspidi „suunatud teenused pornograafilise sisu edastamisel“ või „suunatud teenused“). ARCOM võib vajaduse korral pärast CNILi presidendi arvamuse saamist esitada ühele neist teenistustest ametliku teatise kohustuse kohta seda raamistikku järgida ja rikkumise jätkumise korral määrata sellele pärast CNILilt arvamuse saamist rahalise karistuse 30. septembri 1986. aasta seaduse nr 86-1067 artiklis 42-7 sätestatud korras.

SRENi seadusega ARCOMile antud uued volitused täiendaksid kohtunikule muidu antud volitusi, kellelt võib otse paluda blokeerida veebisait, mis ei vasta karistusseadustiku artikli 227-24 sätetele, näiteks LCENi artikli 6-3 alusel.

Lisaks on alaealiste kaitse pornograafilisele sisule juurdepääsu eest osa laste kaitset reguleerivast üldisemast raamistikust, eelkõige ÜRO 20. novembri 1989. aasta lapse õiguste konventsioonist ja selle 2021. aasta üldisest märkusest nr 25 lapse õiguste kohta seoses digitaalse keskkonnaga (5) ning 7. detsembri 2000. aasta Euroopa Liidu põhiõiguste harta artiklist 24, milles on sätestatud, et „esikohale tuleb seada lapse parimad huvid“.

Töö, mis on vanuse tõendamisel juba käimas

Käesolev dokument on osa CNILi viimastel aastatel tehtud tööst vanuse kontrollimise lahendustega alaealiste kaitse ja eraelu puutumatuse austamise ühildamiseks.

CNIL esitas esimest korda arvamuse 2021. aasta juunis 2020. aasta seaduse rakenduseeskirjade rakendamise kohta, et kaitsta alaealisi juurdepääsu eest pornograafilist sisu edastavatele internetipõhistele avalikele sideteenustele (6). Selleks et vältida inimeste tegeliku või oletatava seksuaalse sättumuse tuletamist nende identiteediga otseselt seotud sisust, soovitas CNIL selles teates kasutada usaldusväärseid kolmandaid pooli ja andis mitmeid soovitusi (7), mis sisaldasid ka vanuse kontrollimist käsitlevat osa. Neid väljaandeid toetas 2022. aasta juulis avaldatud teatis pealkirjaga „Online age verification: striking a balance between protecting minors and respecting privacy“ („Veebis vanuse kontrollimine: tasakaalu leidmine alaealiste kaitsmise ja eraelu puutumatuse austamise vahel“) (8) ning kasutajate eraelu puutumatust austava vanusekontrolli mehhanismi tutvustuse käivitamine (9) koostöös PEReNi ja École Polytechnique'i professoriga. CNILil on juba olnud võimalus meenutada, et „Vastupidiselt sellele, mida mõnikord öeldakse, ei ole IKÜM (10) vastuolus seaduses sätestatud pornograafilistele saitidele juurdepääsu vanuse kontrollimisega.“ (11)

Sarnaselt CNILiga esitas ARCOM arvamuse ka 30. juuli 2020. aasta seaduse artikli 23 rakendamise määruse eelnõu kohta (12).

Just selles kontekstis hakkasid Arcom ja CNIL PEReNi toetusel 2023. aasta alguses ühist tehnilist teabevahetust vanusekontrolli osapooltega. Neid arutelusid rikastas Arcomi tagasiside, mis saadi mõnelt selle välispartnerilt, kes seisavad pornograafilisele sisule

juurdepääsu kontrollimisel samuti silmitsi probleemidega, mis on seotud alaealiste ja eraelu puutumatuse kaitsmisega.

Raamistik võeti vastu pärast 11. aprillist kuni 13. maini avatud avalikku konsultatsiooni ja sellest 15. aprillil Euroopa Komisjonile teatamist vastavalt Euroopa Parlamendi ja nõukogu 9. septembri 2015. aasta direktiivile (EL) 2015/1535, millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord, ning CNILi 26. septembri 2024. aasta arutelu nr 2024-067, mille käigus esitati arvamus raamistiku eelnõu kohta.

Raamistiku tutvustus

Sektori toetamine vanusekontrolli lahenduste rakendamisel

Vastavalt seaduse sätetele määratakse raamistikus kindlaks eeldatavad tehnilised nõuded.

Selle raamistiku eesmärk ei ole tehniliste lahenduste kinnitamine.

Pornograafilist sisu edastavatele suunatud teenustele jääb vabadus valida alaealiste kaitseks oma lahendusi, tingimusel et need vastavad raamistiku tehnilistele nõuetele.

Vanusekontrollisüsteemi puudumine ja vanusekontrollisüsteemid, mis pole usaldusväärsed või mille eraelu puutumatuse kaitse on väiksem kui käesoleva raamistikuga kehtestatud nõuded, ei ole vastuvõetavad.

Raamistiku ajakohastamine ja tehnika tase

Raamistikku võib läbi vaadata ja ajakohastada, et võtta arvesse tehnika taset. SRENi seaduses sätestatakse, et „raamistikku ajakohastatakse vastavalt vajadusele samadel tingimustel“.

On tõepoolest soovitatav, et sektor võtaks vastu vanusekontrolli lahendused, mis vastavad tehnika tasemele ning Euroopa ja rahvusvahelistele standarditele (eelkõige mis tahes Euroopa standardid, mis tekivad lühikeses perspektiivis) ning oleksid kooskõlas tööstusharu tavade, eelkõige seoses olemasolevate tehniliste protokollidega.

Just selles vaimus märkisid Prantsuse ametiasutused vastuseks Euroopa Komisjoni teabenõudele 9. septembri 2015. aasta direktiivis 2015/1535, millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord (kodifitseeritud tekst), ette nähtud teatamismenetluse raames, et:

„Tulevikku silmas pidades kohustuvad nad täielikult või osaliselt läbi vaatama oma siseriikliku õigusraamistiku, kui piisavalt täpne õiguslik alus ELi tasandil võimaldab kehtestada tõhusa vanusekontrollisüsteemi kõigi või mõnede pornograafilisele sisule juurdepääsuga seotud platvormide suhtes.

„Neil asjaoludel näevad nad [raamistikku] üleminekulahendusena, kuni leitakse tõhus üleeuroopaline lahendus.“

Raamistiku struktuur ja rakendamise ajakava

Raamistiku esimene osa käsitleb vanusekontrollisüsteemide usaldusväärsuse üldisi kaalutlusi. Lisaks vajadusele tagada vaikumisi alaealiste kaitse, st isegi enne teenuse

kasutamist, on vaja meenutada veebipõhiste vanusekontrollisüsteemide tõhususe tingimusi, vältides samal ajal nendest kõrvalehoidmist.

Teine osa tegeleb konkreetsetl eraelu puutumatuse kaitsega vanuse kontrollimise süsteemide puhul, mida kasutatakse pornograafilisele sisule juurdepääsu kontrollimiseks. Saidid võivad pakkuda vanusekontrollisüsteeme, millel on erinevad eraelu puutumatuse kaitse tasemed, tingimusel et kasutajaid teavitatakse iga süsteemiga seotud tasemest.

Sellega seoses kehtestatakse raamistikus kõikidele vanusekontrollisüsteemidele miinimumkriteeriumid lisaks tugevdatud erieesmärkidele eraelu puutumatust soodustavate süsteemide puhul, mida nimetatakse „kahekordseks anonüümsuseks“. Kasutajatele tuleb pakkuda vähemalt ühte vanusekontrollisüsteemi, mis vastab „kahekordse anonüümsusega“ eraelu puutumatuse kaitse standarditele.

Teine osa hõlmab ka parimaid tavasid andmekaitse valdkonnas, mida peetakse soovitatavaks.

Peale selle on pornograafilist sisu edastavatel suunatud teenustel võimalik erandina esimeses ja teises osas sätestatud tingimustest rakendada ajutisi lahendusi vanuse tõestamiseks, mis põhinevad vanuse tõendamisel pangakaarti esitades, kuid need peavad rangelt järgima teatud kumulatiivseid tingimusi käesoleva dokumendi kolmandas osas.

Neljandas ja viimases osas sätestatakse peamised põhimõtted, mille võivad juhiseks võtta teenused, mille eesmärk on edastada pornograafilist sisu, mis on vajalikud nende vanusekontrollimissüsteemide auditeerimiseks. Eelkõige täpsustatakse nendes nimetatud auditite otstarvet, nende läbi viimise tingimusi ja kolmandatest isikutest audiitorite suhtes kohaldatavaid nõudeid.

ESIMENE OSA: ÜLDISED KAALUTLUSED VANUSEKONTROLLISÜSTEEMIDE USALDUSVÄÄRSUSE KOHTA

Raamistiku eesmärk on tagada vaikimisi alaealiste kaitse niipea, kui kuvatakse pornograafilise sisu edastamist võimaldava veebipõhise sideteenuse esimene lehekülg. Alaealiste kaitse seisnebki selles, et nad ei puutuks pornograafilise sisuga kokku kohe, kui nad avavad avaliku veebipõhise sideteenuse, mis sellist sisu avaldab.

Sellega seoses on SRENi seaduse artiklis 1 sõnaselgelt sätestatud, et pornograafilist sisu edastavad suunatud teenused peavad kuvama ekraani, mis ei sisalda pornograafilist sisu, „kuni kasutaja vanuse kinnitamiseni“.

Lisaks peavad SRENi seaduse kohaselt pornograafilise sisu edastamisega seotud teenused tagama, et ükski kasutaja ei pääse pornograafilisele sisule juurde enne, kui ta on tõendanud oma täisealisust.

Alaealiste kaitse saab vaikimisi tagada näiteks teenuse avalehte täielikult hägustades.

Avaldajad saavad oma teenuse pornograafilisest olemusest ka teavitada. Selleks võivad nad tugineda enese deklareerimise mehhanismile, näiteks RTA märgisele (13), mida kasutatakse saidi kõikidel lehtedel ja mis võimaldab vanemliku kontrolli süsteemidel vastuse päise (või päiste [14]) kaudu teada saada, mis on minimaalne vanus, mis on vajalik saidi sisule juurdepääsuks.

Seaduse järgimiseks peavad pornograafilist sisu edastavate suunatud teenuste kehtestatud vanusekontrollisüsteemid (käesoleval juhul enamik) võimaldama eristada alaealisi ja täiskasvanuid. Tõenäoliselt arenevad lahendused edasi, täiustades tehnikaid ja viies turule uusi vanusekontrollisüsteeme, sealhulgas mis tahes Euroopa standardeid, mis tekivad lühikeses perspektiivis.

Kui pornograafilist sisu edastavate suunatud teenuste kasutusele võetud tehniline lahendus põhineb kasutaja vanuse hindamisel, tähendab seaduse järgimine, et see tuleb konfigurereida nii, et oleks välistatud oht, et alaealist kasutajat peetakse täiskasvanuks („valepositiivsed“). Seaduse järgimiseks peavad pornograafilist sisu edastavad suunatud teenused tegema kõik endast oleneva, järgides tööstusharu ametialase hoolikuse kõrgeid standardeid; et piirata nende kasutatavatest tehnilistest lahendustest kõrvale hoidmise võimalusi.

Vanusekontrollisüsteemid ei tohiks võimaldada vanuse tõendamist teiste inimestega jagada, et vähendada pettuseohtu. Seega peab süsteem olema vastupidav, pidades silmas rünnete ohtu, näiteks süvavõltsimine, teesklus jne.

Näiteks seoses lahendustega, mis põhinevad vanuse hindamisel näoomaduste analüüsimise teel, peavad pornograafilist sisu edastavad suunatud teenused tagama, et lahendused hõlmavad järgmist: elusate inimeste äratundmise mehhanism, mille tõhusus on kooskõlas tehnika tasemega. Tuvastamine toimub piisava kvaliteediga kujutise abil ning see välistab igasuguse kõrvaesumise protsessi, mida alaealised võivad kasutada selleks, et kunstlikult täiskasvanuna näida, eelkõige fotode, salvestatud videote või maskide abil.

Seoses füüsilise isikut tõendava dokumendi esitamisel põhineva vanusetõendamise tehniliste lahendustega peavad pornograafilist sisu edastavad suunatud teenused kontrollima järgmist:

i) dokument on tõene ja mitte koopias; ii) kasutaja on isikut tõendava dokumendi omanik.

Kontrolli võib läbi viia eelkõige näoomaduste tuvastamise abil, mis hõlmab elu tuvastamise mehhanismi, vastavalt ülal nimetatud tingimustele.

Selleks et vältida alaealiste kokkupuudet pornograafilise sisuga internetis, eeldatakse, et vanuse kontrollimine tuleb läbi viia iga kord, kui teenusega seoses konsulteeritakse. Seega peab konsultatsiooni katkestamine käivitama uue vanusekontrolli, kui kasutaja soovib pornograafilist sisu uuesti avada. See ei piira kasutaja võimalust kasutada vanusetõendeid, mida ta saab uuesti kasutada või regenereerida, kui on olemas teine autentimistegur. Seda saab teha, sidudes taaskasutatavate tõendite kasutamise andmesubjekti terminaliga, nagu seda tehakse digitaalsete rahakottide puhul.

Lisaks ei tohi kontrollisüsteem võimaldada seda tõendit jagada teise isiku või talitusega.

Täiskasvanu ja alaealise vahelise konsultatsiooniterminali puhul on oluline vältida seda, et vanusekontrolli kehtivusaeg võimaldaks pornograafilisele sisule juurde pääseda ilma täiendava kontrollita. Vanusekontrolli kehtivus tuleb seetõttu katkestada, kui kasutaja teenusest lahkub, st kui sessioon lõpeb, kui kasutaja lahkub veebilehitsejast või kui operatsioonisüsteem läheb ooteseisundisse ja igal juhul pärast üks tund kestnud tegevusetusest.

Vältimaks seda, et kasutajakontode taaskasutamine sunnib alaealisi pornograafilisele sisule juurde pääsma, eeldatakse, et vanusetõendit ei saa suunatud teenuse kasutajakontole salvestada. Igal juhul tuleneb seadusest, et vanuse kontrollimise kohustus kehtib kõikide juurdepääsude korral nii kasutajakontoga kui ka ilma selleta.

Alaealiste kaitse ja seaduste järgimise tagamiseks eeldatakse, et pornograafilist sisu edastavate suunatud teenuste pakutavad lahendused on tõhusad kõigi elanikkonnarühmade jaoks ega too seega kaasa teatavate rühmade diskrimineerimist, eelkõige Euroopa Liidu põhiõiguste harta artiklis 21 sätestatud põhjustel. Seega peab vanusekontrolli tehnilise lahenduse tõhusus olema sama, olenemata kasutaja füüsilistest omadustest. Vanuse tõendamise süsteemide puhul, mis põhinevad masinõppel või statistilistel mudelitel, võivad teenuseosutajad näiteks testida oma lahendust mitmesugustes andmebaasides, et tagada selle nõude täitmine. On oluline, et vanusekontrollisüsteemid piiravad diskrimineerivaid eelarvamusi, mis põhjustavad ka vigu, mis võivad seada kahtluse alla nii nende usaldusväärsuse kui ka vastuvõetavuse.

Pornograafilist sisu edastavatel suunatud teenustel palutakse vanusekontrollimissüsteemi tulemuslikkuse hindamisel, aga ka mis tahes auditite puhul lisada mis tahes diskrimineerivad eelarvamused, mis on liigendatud asjakohaste diskrimineerimispõhjuste alusel (vt allpool).

Teine osa: eraelu puutumatuse kaitse

Käesoleva raamistiku eesmärk on tagada ka kasutajate eraelu puutumatuse kaitse vanusekontrollisüsteemide kasutamisel. Need süsteemid võivad kujutada endast suurt ohtu isikuandmete turvalisusele, sest vanuse kontrollimine on sarnane isikusamasuse kontrollimisega ja võib seetõttu nõuda tundlike andmete või isikut tõendavate dokumentide andmete kogumist.

Vanusekontrollisüsteemidega seotud isikud peavad seetõttu pöörama erilist tähelepanu oma kasutajate eraelu puutumatuse kaitsele ja asjaomaste infosüsteemide turvalisusele, mille tagamise eest vastutab CNIL, eelkõige isikuandmete kaitse üldmääruse (IKÜM) järgimisele.

Eraelu puutumatuse kaitse põhimõtted

Praktikas peavad vanusekontrollisüsteemid tervikuna vastama kehtivatele isikuandmete ja eraelu puutumatuse kaitset käsitlevatele õigusaktidele, sealhulgas minimeerimise ja andmekaitse põhimõtetele nii kavandatult kui ka vaikimisi (IKÜM-i artiklid 5 ja 25). Selliste süsteemide pakkujad peavad pöörama erilist tähelepanu järgmistele põhimõtetele:

kogutud andmete täpsus, proportsionaalsus ja minimeerimine;
kokkuvõtlik, läbipaistev, arusaadav ja kergesti kättesaadav kasutajateave;
asjakohased andmete säilitamise tähtajad;
üksikisikute võimalus kasutada oma õigusi, nimelt õigust andmetega tutvuda, esitada vastuväiteid, õigust andmete parandamisele, õigust töötlemise piiramisele, õigust kustutamisele, õigust ülekantavusele;
isikuandmete töötlemiseks kasutatavate infosüsteemide tiptasemel turvalisus.

Eraelu puutumatust toetava vanusekontrollisüsteemi rakendamine vaikimisi ja kavandatult

2022. aastal avaldas CNIL eraelu puutumatust toetava vanusekontrollimehhanismi, mille abil saab edastada identiteeditunnuse (antud juhul vanusetõendi) (15), (16). Eelkõige tagatakse kavandatud mehhanismiga, et pornograafilist sisu edastavate suunatud teenuste, mis on kohustatud kasutajate vanust kontrollima, ja kasutajate vanust kontrollivate kolmandate isikute vahel on kindel eraldus.

Selle mehhanismi, mida sellest ajast alates tuntakse kui kahekordset anonüümsust või topeltkonfidentsiaalsust, on välja töötanud ja seda on katsetanud erinevad avaliku ja erasektori osalejad, kinnitades selle tehnilist teostatavust ja suutlikkust rahuldada vajadust eraelu puutumatuse kaitse järele, mis on omane internetipõhistele vanusekontrollimehhanismidele. See vastab ka digitaalidentiteedi süsteemidele, sealhulgas atribuutide haldamisele üldiselt seatud eesmärkidele. Kuigi käesolevas dokumendis

viidatakse sellele kui „kahekordse anonüümsusele“, ei ole see siiski „anonüümne“ isikuandmete kaitse üldmääruse tähenduses, kuid tagab konfidentsiaalsuse kõrge taseme. Veebipõhised avalikud sideteenused, mis teevad pornograafilise sisu kättesaadavaks, peavad pakkuma oma kasutajatele vähemalt ühte vanusekontrollisüsteemi, mis vastab „kahekordse anonüümsuse“ privaatsusstandarditele, tagades, et seda süsteemi saab kasutada enamik selle kasutajatest.

See nõue jõustub käesoleva raamistiku kolmandas osas sätestatud üleminekuperioodi lõpus, milleks on kuus kuud pärast selle avaldamist, ilma et see piiraks allpool sätestatud miinimumnõuete kohaldamist. Seega peavad vanusekontrollimissüsteemid kuni selle kuupäevani vastama allpool esitatud miinimumnõuetele, et tagada kasutajate isikuandmete kaitse vastuvõetav tase.

Järgmised jaotised täpsustavad:

nõudeid, mida kohaldatakse kõigi käesoleva raamistikuga hõlmatud vanusekontrollisüsteemide suhtes;

eraelu puutumatus soodustavate süsteemide (kahekordse anonüümsuse süsteemide) konkreetseid eesmärke;

läbipaistvuskohustusi, mille eesmärk on teavitada kasutajaid teenuste kaudu pakutavate süsteemidega seotud eraelu puutumatus kaitse tasemest;

ja häid tavaid, mis on esitatud soovitusena, kuid mida ei ole seni nõutud.

Kõikide vanusekontrollisüsteemide miinimumnõuded

Miinimumnõuete kogumit kohaldatakse kõigi käesoleva raamistikuga hõlmatud vanusekontrollisüsteemide suhtes.

1. Vanusekontrollisüsteemi pakkuja sõltumatus suunatud teenuste edastatavast pornograafilisest sisust

Vanusekontrollimissüsteemide pakkuja on õiguslikult ja tehniliselt sõltumatu kõigist käesoleva raamistikuga hõlmatud internetipõhistest avalikest sideteenustest ning tagab, et pornograafilist sisu edastavatel suunatud teenustel ei ole mingil juhul juurdepääsu andmetele, mida kasutatakse kasutaja vanuse kontrollimiseks.

2. Pornograafilist sisu edastavate suunatud teenuste konfidentsiaalsus

Isikuandmeid, mis võimaldavad kasutajal kontrollida oma vanust käesoleva raamistikuga hõlmatud sideteenuse abil, ei tohi töödelda sama sideteenus.

Eelkõige ei tohi vanusekontrolli lahenduste rakendamine lubada käesoleva raamistikuga hõlmatud sideteenustel koguda selliste kasutajate identiteeti, vanust, sünniaega ega muid isikuandmeid.

3. Konfidentsiaalsus vanuse tõendamise teenuseosutajate suhtes

Kui vanusekontrollimissüsteem ei võimalda kasutajal saada korduvkasutatavat digitaalset identiteeti või vanusetõendit, ei tohi vanusetõendi looja kasutaja poolt selle atribuudi saamiseks esitatud isikuandmeid säilitada.

Lisaks ei tohiks seda tüüpi süsteem nõuda ametlike isikut tõendavate dokumentide kogumist, kui see ei anna taaskasutatavat vanusetõendit.

See nõue ei piira õiguslike ja regulatiivsete kohustuste täitmist, mida muidu kohaldatakse teatavate vanusetõendi pakkujate suhtes.

4. Konfidentsiaalsus mis tahes kolmanda isiku suhtes, kes osaleb vanuse kontrollimise protsessis

Kui vanuse kontrollimise protsessi on kaasatud kolmandad isikud, kes ei ole vanusetõendite loojad, näiteks tõendite haldamisel või teenuse eest arvete esitamisel; ei tohi need kolmandad isikud salvestada süsteemi kasutajate isikuandmeid, välja arvatud tõendite säilitamiseks kasutaja nõudmisel.

5. Vanusetõendajate meetmed üksikisikute õiguste ja vabaduste kaitseks

Selleks et teha kindlaks, kas kasutajal on talle esitatud tõendite alusel juurdepääs veebipõhisele üldkasutatavale sideteenusele, teeb pornograafilist sisu edastav suunatud teenuse osutaja automatiseeritud otsuse isikuandmete kaitse üldmääruse artikli 22 tähenduses. Teenusele juurdepääsu keelamisega võib see otsus tekitada asjassepuutuvatele isikutele õiguslikke tagajärgi või vähemalt avaldada inimestele sarnasel viisil märkimisväärset mõju.

CNIL leiab, et selline otsus võib põhineda isikuandmete kaitse üldmääruse artikli 22 lõike 2 punktis b sätestatud erandil, kui pornograafilist sisu edastava suunatud teenuse suhtes kehtib karistusseadustiku artikli 227-24 ja SRENi sätete kohane vanuse kontrollimise kohustus. Isikuandmete kaitse üldmääruse artikli 22 lõike 2 punktiga b on ette nähtud asjakohased meetmed andmesubjekti õiguste ja vabaduste ning kaitsvate huvide kaitsmiseks käesolevat automatiseeritud otsust lubavates sätetes.

Eraelu puutumatus kaitse nõuete säilitamiseks, mille eesmärk on piirata teenuste võimet üksikisikuid tuvastada, ei pea selliseid meetmeid kehtestama mitte sihtteenuse osutaja, vaid vanuse kontrollimise tehnilise lahenduse pakkuja, olenemata sellest, kas tegemist on atribuudi pakkuja või tõendi väljaandjaga. Sellised meetmed peaksid võimaldama kasutajatel vea korral vaidlustada oma atribuudi analüüsi tulemus, et saada vanusetõend. Nende õiguskaitsevahendite kasutamiseks peaksid vanusekontrolli lahenduste pakkujad pakkuma kasutajatele võimalust kasutada erinevaid atribuutide pakkujaid või olenevalt lahendustest erinevaid tõendite väljastajaid.

Pornograafilist sisu edastava suunatud teenuse osutaja, nagu ka vanusekontrolli tehniliste lahenduste pakkujad, on siiski kohustatud täitma isikuandmete kaitse üldmäärusega kehtestatud teavitamiskohustusi ja teavitama kasutajaid võimalusest esitada vanusekontrolli lahenduse pakkujale kaebus.

Igal juhul peavad atribuutide pakkujad võimaldama isikutel oma andmeid isikuandmete kaitse üldmääruse artikli 16 alusel parandada.

Erinõuded eraelu puutumatus kaitse süsteemidele, mis järgivad topeltanonüümsuse põhimõtet

Järgmised eesmärgid täiendavad minimaalse aluse eesmäärke, et määrata kindlaks eraelu puutumatus soodustav veebipõhine vanusekontrolli standard.

6. Konfidentsiaalsus suunatud teenuste suhtes, mis edastavad pornograafilist sisu

Lõike 2 nõudeid täiendatakse järgmiste nõuetega.

Vanusekontrollisüsteem, mis kasutab kahekordset anonüümsust, ei tohiks võimaldada käesoleva raamistikuga hõlmatud sideteenustel tunnustada kasutajat, kes on vanusekontrolli käigus saanud andmete põhjal seda süsteemi juba kasutanud.

Vanusekontrollimissüsteemide kasutamine, mille puhul kasutatakse topeltanonüümsust, ei tohiks need teenused teada saada või tuletada vanuse tõendamise allikat või meetodit, mis on seotud kasutaja vanuse kontrollimise protsessiga.

„Kahekordse anonüümsuse“ vanuse kontrollimise süsteem ei tohi võimaldada kõnealustel teenustel tuvastada, et kaks täisealisuse tõendit pärinevad samast vanuse tõendamise allikast.

7. Suurem konfidentsiaalsus vanusetunnuste väljaandjate suhtes

Lõike 3 nõudeid täiendatakse nii, et vanusekontrollisüsteem, milles kasutatakse kahekordset anonüümsust, ei tohi võimaldada tõendit tootvatel pakkujatel teada saada, millise teenuse tarbeks vanuse kontrollimine toimub.

8. Tõhusam konfidentsiaalsus mis tahes kolmanda isiku suhtes, kes osaleb vanuse kontrollimise protsessis

Lõike 4 nõudeid täiendatakse järgmiste nõuetega.

Vanusekontrollimissüsteem, mis kasutab kahekordset anonüümsust, ei tohiks lubada teistel protsessis osalevatel kolmandatel isikutel tuvastada kasutajat, kes on süsteemi juba kasutanud. Näiteks ei tohiks kolmas isik, kes esitab tõendi vanuse kohta või tõendab selle kehtivust, teada saada, kas ta on juba töödelnud samalt kasutajalt saadud tõendeid.

9. Kättesaadavus ja elanikkonna hõlmatus

Käesoleva raamistikuga hõlmatud sideteenused peavad kahekordse anonüümsuse süsteemi abil tagama, et nende kasutajatel on oma vanuse tõendamiseks vähemalt kaks erinevat vanuse tõendamise meetodit. Praktikas peab kahekordse anonüümsuse lahendust pakkuv teenuseosutaja kombineerima vähemalt kaks vanuse tõendamise meetodit (nt isikut tõendavatel dokumentidel põhinev lahendus ja vanuse hindamisel põhinev lahendus).

Käesoleva raamistikuga hõlmatud sideteenused peavad tagama, et kahekordse anonüümsusega vanusekontrollisüsteem on kättesaadav vähemalt 80 %-le Prantsusmaal elavatest täiskasvanud elanikest.

Näited ja rakendamine:

Praktikas peavad kahekordse anonüümsuse lahendused pakkuma mitut vanusetõendaja tõendit (nt erinevad internetiühenduse pakkujad ja/või pangad) ja muude lahenduste puhul vanuse tõestamise erinevat meetodit (nt näoomaduste analüüs ja isikut tõendava dokumendi esitamine).

Kasutajate teavitamine vanusekontrollisüsteemidega seotud eraelu puutumatuse tasemest

10. Kasutaja privaatsuse kaitse taseme selgesõnaline kuvamine

Iga vanuse kontrollimise lahendus peab olema selgelt seotud selle eraelu puutumatuse kaitse tasemega, nii et kahekordse anonüümsuse standarditele vastavad lahendused oleksid selgelt ja loetavalt esitatud. Igal juhul ei tohiks teisi lahendusi segi ajada ega reklaamida, et eksitada kasutajat eraelu puutumatust vähem kaitsvate lahenduste suunas.

Kui vanusekontrollis osalev kolmas isik võib olla teadlik teenusest, mille jaoks vanuse kontrollimine toimub, tuleb kasutajat sellest selgelt teavitada.

Mis puudutab vanusekontrollimissüsteeme, mis vastavad kahekordse anonüümsuse põhimõttele, siis tuleb kasutajat selgelt teavitada, et see lahendus tagab, et vanusekontrolli pakkuja ei tea, millise teenuse tarbeks see kontroll tehakse.

Soovitud eesmärgid ja parimad tavad

Vanusekontrollimissüsteemidelt ei nõuta veel järgmisi eesmäärke, et tagada vastavus käesolevale raamistikule, kuid sõnastatud on parimate tavade kogum, mille poole peaksid vanusekontrollilahendused püüdlema.

Kasutajate võime luua ise konfidentsiaalselt tõendeid oma vanuse kohta:

kasutaja saab koostada tõendi vanuse kohta kohalikult, teavitamata algset väljaandjat või muud kolmandat isikut oma vanuseandmetest;
kasutaja saab esitada vanusetõendi veebiteenuse kaudu, mida saab kasutada ilma juurdepääsuta tema isikuandmetele.

Vanusekontrollisüsteemide kui terviku konfidentsiaalsus:

süsteem põhineb teadmiste puudumise tõendamisel;
süsteem põhineb krüptimistehnikatel, millel on kõige keerukamad rünnakukindluse omadused, isegi tulevikus.

KOLMAS OSA: ALTERNATIIVSED TÕENDUSPÕHISED LAHENDUSED, MIDA AKTSEPTEERITAKSE AJUTISELT

Vastavalt 21. juuni 2004. aasta seaduse nr 2004-575 (usalduse kohta digitaalmajanduse vastu) artiklile 10 peavad teenused, mille suhtes neid sätteid kohaldatakse, rakendama vanusekontrollisüsteemi, mis vastab selle raamistiku tehnilistele omadustele, kolme kuu jooksul alates selle avaldamisest. Nimetatud kolme kuu lõpuks kolmekuulisel üleminekuperioodil alates käesoleva raamistiku avaldamisest, mis on loodud selleks, et teenused, mille suhtes neid kohaldatakse, saaksid kindlaks teha ja rakendada vanusekontrollilahenduse, mis vastab kõigile esimeses ja teises osas sätestatud kriteeriumidele, loetakse lahendused, milles kasutatakse pangakaarte, raamistiku tehnilistele omadustele vastavaks järgmistel tingimustel.

Lahendus pangakaardiga oleks esialgne meetod mõne alaealise välja filtreerimiseks. See ajutine lahendus põhineb taristul, mis on juba kasutusele võetud ja mida on võimalik rakendada.

Eeldusel, et allpool esitatud nõuded on täidetud, võimaldaks see lahendus esialgu kaitsta noorimaid alaealisi. Filtreerimine peab toimuma tugeva autentimise (st kaheastmelise autentimise) teel. Näiteks saab seda teha kas ainult tugeva autentimisega (ilma makseta) või makse kaudu (sealhulgas nulleurose summaga), millega kaasneb tugev autentimine. Nendele kontrollisüsteemidele kehtivad järgmised nõuded.

Neid ei tohi rakendada otse pornograafilist sisu edastavad suunatud teenused, vaid teenusest sõltumatud kolmandad pooled.

Need peavad tagama kontrolli turvalisuse, et vältida sellega seotud andmepüügi ohtu.

Seetõttu on oluline tagada, et makseteave sisestatakse usaldusväärsel saitidel. Sellega seoses oleks soovitatav, et pornograafilist sisu edastavad suunatud teenused ja lahenduste pakkujad käivitaksid kooskõlastatud kampaania, et suurendada teadlikkust andmepüügiriskidest, võttes eelkõige arvesse seda uut tava.

Need peavad võimaldama kontrollida vähemalt kaardi olemasolu ja kehtivust, mis välistab kaardi numbri vastavuse lihtsa kontrollimise.

Need peavad rakendama makseteenuseid käsitlevas Euroopa direktiivis (EL) 2015/2366 (teine makseteenuste direktiiv) sätestatud tugevat autentimist, tuginedes näiteks 3-D Secure protokollile. Teises kehtivas versioonis tuleb tagada, et teenuse kasutaja on kaardi omanik kaheastmelise autentimise abil.

Neljas osa: vanusekontrolli lahenduste auditeerimine ja hindamine

SRENi seaduses on sätestatud, et „Audiovisuaal- ja digikommunikatsiooni reguleeriv asutus võib nõuda avaldajatelt ja teenuseosutajatelt [...] auditit vanusekontrollisüsteemide kohta, mida nad rakendavad, et tõendada nende süsteemide vastavust raamistikuga kindlaks määratud tehnilistele nõuetele. Raamistikus määratakse kindlaks auditi läbiviimise ja avalikustamise kord, mis on usaldatud tõendatud kogemustega sõltumatule asutusele.“ Järgmiste jaotiste eesmärk on selgitada peamisi põhimõtteid, millest pornograafilist sisu edastavad suunatud teenused võiksid sellise auditi tegemisel juhinduda.

Tegelikes tingimustes kasutusele võetud süsteemide hindamine

Selleks et tagada alaealiste kaitse kõrge tase, hindab Arcom iga juhtumi puhul eraldi vanuse kontrollimise tehnilisi lahendusi, kui need on kasutusele võetud avaldajate poolt, st in concreto. Kuna pornograafilist sisu edastavad suunatud teenused saavad teatavaid lahendusi konfigurioneerida, on vaja teha hindamine tegelikes kasutustingimustes. Pornograafilist sisu edastavad suunatud teenused peavad tagama kehtestatud lahenduste süstemaatilise vastavuse raamistiku nõuetele, kohandades vajaduse korral oma tegevuspõhimõtteid ja parameetreid.

Veamäärad, kõrvalehoidmine ja ründeoht

Tehnilise auditi käigus hinnatakse üldiselt, kas vanusekontrollilahendus vastab tervikuna kõikidele seaduses ja selles raamistikus sätestatud kriteeriumidele. Sellega seoses hinnatakse eelkõige järgmist:

tehnilise lahenduse võime eristada alaealisi kasutajaid;
diskrimineeriva kallutatuse puudumine;
vastuseis võimalikele meetmetest kõrvalehoidmisele (nt süvavõltsingutele) ja ründeohule (17).

Audiitori sõltumatus

Selleks et mitte kahjustada auditi usaldusväärsust, peaks audiitoril olema tõendatud teadmised ja kogemused ning ta peaks olema sõltumatu nii vanusekontrollilahendusi pakkuvatest ettevõtetest kui ka pornograafilist sisu edastavatest suunatud teenustest, mis kasutavad nimetatud tehnilist lahendust (või lahendusi).

Arcom võib selle raamistiku hilisemas versioonis täpsustada, millistel tingimustel tuleb auditeid läbi viia ja üldsusele kättesaadavaks teha.

Praeguse seisuga ja kuni ARCOMilt täiendava selgituse saamiseni julgustatakse ettevõtteid tegema oma vanusekontrollisüsteemide tehnilisi auditeid esialgu kuue kuu jooksul pärast käesoleva raamistiku avaldamist ja seejärel vähemalt kord aastas.

Samuti julgustatakse pornograafilist sisu edastavaid suunatud teenuseid läbipaistvuse huvides, eriti seoses kasutajatega, avaldama oma auditiaruannet oma internetipõhise kasutajaliidese kergesti juurdepääsetaval lehel kergesti mõistetavas vormingus.

- (1) Arcom, Visits to 'adult' sites by minors (Médiamétrie esitatud andmete põhjal), avaldatud 25. mail 2023;
- (2) Arzano, C. Rozier, Alice au pays du porno (Alice pornomaal): Ados : leurs nouveaux imaginaires sexuels (Teismelised: nende uued seksuaalsed kujutlused) Ramsay, 2005.
- (3) Vt: <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Quelles-solutions-pour-protoger-votre-enfant-des-images-a-caractere-pornographique-sur-internet>; ja B. Smaniotto (psühhopaatoloogia ja kliinilise psühholoogia teadlane), Pornography: what impact on adolescent sexuality? (Pornograafia: milline on mõju noorukite seksuaalsusele?)', Vestlus, 28. august 2023: <https://theconversation.com/pornographie-quels-impacts-sur-la-sexualite-adolescente-207142>.
- (4) Kassatsioonikohtu kriminaalkolleegium, 23. veebruar 2000, 99-83.928,
- (5) <https://www.ohchr.org/fr/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>
- (6) CNIL, 3. juuni 2021. aasta arutelu nr 2021-069 arvamuse kohta, mis käsitleb määruse eelnõu, mis käsitleb rakendusmeetmeid alaealiste kaitsmiseks pornograafilist sisu edastavatele saitidele juurdepääsu eest (vt: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044183781>).
- (7) Vt: <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne>
- (8) Vt:
- (9) Vt: <https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee>
- (10) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.
- (11) Vt CNILi 21. veebruari 2023. aasta pressiteade: <https://www.cnil.fr/fr/controle-de-lage-pour-laces-aux-sites-pornographiques>
- (12) CSA, 23. juuni 2021. aasta aramus nr 2021-11, mis käsitleb dekree eelnõu meetmete rakendamise kohta alaealiste kaitsmiseks pornograafilist sisu edastavatele saitidele juurdepääsu eest;
- (13) Ainult täiskasvanutele“.
- (14) Päised on teave, mille veebilehe server tagastab kasutaja veebilehitsejale taotluse esitamise ajal.
- (15) <https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee>
- (16) <https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie>
- (17) Vanusekontrollilahenduse ründamise ohu hindamisel tuleb kindlaks teha, kas süsteemi võidakse tõenäoliselt kuritarvitada pettuse eesmärgil.

Koostatud 9. oktoobril 2024.

Audiovisuaalset ja digitaalset kommunikatsiooni reguleeriv asutus:
Esimees,

R.-O. Maistre