



Audiovisuaalvaldkonda ja
digikommunikatsiooni reguleeriv
asutus

Avalik konsultatsioon eelnõu
raamistiku kohta, milles
sätestatakse minimaalsed
tehnilised nõuded vanuse
kontrollimise süsteemidele, mis
on loodud juurdepääsuks
teatavatele internetipõhistele
avalikele sideteenustele ja
videojagamisplatvormidele, mis
teevad pornograafilise sisu
üldsusele kättesaadavaks

Aprill 2024

Sisukord

Sisukord.....	3
Sissejuhatus.....	5
Pornograafilist sisu edastavate suunatud teenuste vastutus	5
Arcomi rolli areng seaduseelnõu kontekstis, et tagada ja reguleerida digitaalset ruumi	6
Töö, mis on vanuse tõendamisel juba käimas	6
Raamistiku tutvustus.....	8
Sektori toetamine vanusekontrolli lahenduste rakendamisel	8
Raamistiku ajakohastamine ja tehnika tase	8
Raamistiku struktuur ja rakendamise ajakava	8
Esimene osa: vanusekontrollimissüsteemide usaldusväärsus.....	10
Alaealiste vaikimisi kaitse	10
• Kriteerium nr 1: vanusekontrolli rangus.....	10
Usaldusväärsuse kriteeriumid	10
• Kriteerium nr 2: lahenduse tõhusus.....	10
• Kriteerium nr 3: kõrvalehoidmise võimaluste piiramine.....	11
• Kriteerium nr 4: vanuse kontrollimine igal teeninduskonsultatsioonil.....	11
• Kriteerium nr 5: kasutajakonto kasutamise raamistik.....	12
• Kriteerium nr 6: mittediskrimineerimine.....	12
Teine osa: eraelu puutumatuse kaitse.....	13
Eraelu puutumatuse kaitse põhimõtted	13
Eraelu puutumatust toetava vanusekontrollisüsteemi rakendamine vaikimisi ja kavandatult	13
Kõikide vanusekontrollisüsteemide miinimumnõuded	14
• Kriteerium nr 7: vanusekontrollisüsteemi pakkuja sõltumatus suunatud teenuste edastatavast pornograafilisest sisust.....	14
• Kriteerium nr 8: konfidentsiaalsus suunatud teenuste suhtes, mis edastavad pornograafilist sisu.....	14
• Kriteerium nr 9: konfidentsiaalsus seoses vanuse tõendajatega.....	14
• Kriteerium nr 10: konfidentsiaalsus mis tahes kolmanda isiku suhtes, kes osaleb vanuse kontrollimise protsessis.....	15
• Kriteerium nr 11: isikute õiguste ja vabaduste kaitse vanusetõendajate poolt	15
Erinõuded eraelu puutumatuse kaitse süsteemidele, mis järgivad topeltanonüümsuse põhimõtet	16
• Kriteerium nr 12: konfidentsiaalsus suunatud teenuste suhtes, mis edastavad pornograafilist sisu.....	16

• Kriteerium nr 13: suurem konfidentsiaalsus vanusetõendite väljastajate juures	16
• Kriteerium nr 14: konfidentsiaalsus mis tahes kolmanda isiku suhtes, kes osaleb vanuse kontrollimise protsessis.....	16
• Kriteerium nr 15: kättesaadavus ja elanikkonna hõlmatus.....	16
Kasutajate teavitamine vanusekontrollisüsteemidega seotud eraelu puutumatuse tasemest	17
• Kriteerium nr 16: kasutaja eraelu puutumatuse kaitse taseme selgesõnaline kuvamine.....	17
Soovitud eesmärgid ja parimad tavad	17
Kolmas osa: alternatiivsed tõenduspõhised lahendused, mida aktsepteeritakse ajutiselt.....	19
Neljas osa: vanusekontrolli lahenduste auditeerimine ja hindamine.....	20
Tegelikes tingimustes kasutusele võetud süsteemide hindamine	20
Veamäärad, kõrvalehoidmine ja ründeoht	20
Audiitori sõltumatus	20

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 alaealised¹.

Alates 2000. aastate algusest² 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 suhetes³.

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 inimväärlikust tõsiselt

¹ Arcom, *Visits to 'adult' sites by minors* (Médiamétrie esitatud andmete põhjal), avaldatud 25. mail 2023: <https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/frequentation-des-sites-adultes-par-les-mineurs>

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-protéger-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?)', *The Conversation*. 28. august 2023: <https://theconversation.com/pornographie-quels-impacts-sur-la-sexualite-adolescente-207142>.

Sellela seoses kutsub Arcom ka vanemaid külastama veebisaiti <https://jeprotegemonenfant.gouv.fr/pornographie/>.

⁴ Kassatsioonikohtu kriminaalkolleegium, 23. veebruar 2000, 99-83.928, <https://www.legifrance.gouv.fr/juri/id/JURITEXT000007070001>.

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 pakkuja (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 onkäesoleva avaliku konsultatsiooni avaldamise kuupäeval veel pooleli.

Arcomi rolli areng seaduseelnõu kontekstis, et tagada ja reguleerida digitaalset ruumi

Parlamendis arutlusel oleva digiruumi turvalisuse ja reguleerimise seaduse eelnõuga (SREN) kavatakse ajakohastada 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, vanusekontrolli süsteemide suhtes kohaldatavate tehniliste miinimumnõuete kindlaksmääramise raamistiku.** Need nõuded käsitlevad kasutajate vanusekontrolli usaldusväärsust ja nende privaatsuse austamist. Süsteemi kohaldamisalaks on „pornograafiline sisu, mille on üldsusele kättesaadavaks teinud üldkasutatava sideteenuse osutaja oma toimetust vastutusele või mida pakub videojagamisplatvormi 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 teenustest ametliku teatise kohustuse kohta seda raamistikku järgida ja rikkumise jätkumise korral määrata sellele pärast CNILTU

arvamuse saamist rahalise karistuse 30. septembri 1986. aasta seaduse nr 86-1067 artiklis 42-7 sätestatud korras. Käesolev avalik konsultatsioon käsitleb kõnealuste sätetega ette nähtud raamistiku eelnõud.

Seaduseelnõuga Arcomile antud uued volitused täiendaksid kohtunikule muidu antud volitusi, kellelt võib otse paluda blokeerida veebisait, mis ei vasta karistusseadustiku artikli 227-24 sätetele.

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 sideteenustele⁵. 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,⁶ 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“) ning kasutajate eraelu puutumatust austava vanusekontrolli mehhanismi tutvustuse käivitamine⁷⁸ koostöös PEReNi ja École Polytechnique'i professoriga.

CNILil on juba olnud võimalus meenutada, et „Vastupidiselt sellele, mida mõnikord öeldakse, ei ole IKÜM⁹ vastuolus seaduses sätestatud pornograafilistele saitidele juurdepääsu vanuse kontrollimisega.“¹⁰

Sarnaselt CNILiga esitas Arcom arvamuse ka 30. juuli 2020. aasta seaduse artikli 23 rakendamise määruse eelnõu kohta¹¹.

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.

⁵ 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>).

⁶ Vt: <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne>

⁷ Vt: <https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie>

⁸ Vt: <https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee>

⁹ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.

¹⁰ Vt CNILi 21. veebruari 2023. aasta pressiteade: <https://www.cnil.fr/fr/controle-de-lage-pour-lacces-aux-sites-pornographiques>

¹¹ CSA, 23. juuni 2021. aasta arvamus nr 2021-11, mis käsitleb dekreed eelnõu meetmete rakendamise kohta alaealiste kaitsmiseks pornograafilist sisu edastavatele saitidele juurdepääsu eest; <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044174211>

Raamistiku tutvustus

Sektori toetamine vanusekontrolli lahenduste rakendamisel

Vastavalt seaduseelnõu sätetele täpsustatakse raamistiku eelnõus: **tehnilised nõuded** nii **usaldusväärsusele** kasutajate vanuse (antud juhul nende täisealisuse) kontrollimisel ja nende **privaatsuse** austamisele.

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.**

Vanusekontrolli süsteemi puudumine ja vanusekontrolli süsteemid, mille usaldusväärsus või 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 eelnõus 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 ning oleksid kooskõlas tööstusharu tavadega, eelkõige seoses olemasolevate tehniliste protokollidega.

Raamistiku struktuur ja rakendamise ajakava

Raamistiku eelnõu esimene osa käsitleb vanusekontrollisüsteemide usaldusväärsust. Lisaks vajadusele tagada vaikumisi alaealiste kaitse, st isegi enne teenuse kasutamist, on vaja täpsustada **veebipõhiste vanusekontrollisüsteemide tõhususe tingimused, vältides samal ajal nendest kõrvalehoidmist.**

Kõik vanuse kontrollimise süsteemid peavad vastama kõigile esimeses osas sätestatud nõuetele.

Teine osa tegeleb konkreetselt 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 raamistiku eelnõus **kõikidele vanusekontrollimissüsteemidele 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 tavaid** 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: vanusekontrollimissüsteemide usaldusväarsus

Raamistiku eesmärk on tagada vaikimisi alaealiste kaitse niipea, kui kuvatakse pornograafilise sisu edastamist võimaldava veebipõhise sideteenuse esimene lehekülg.

Alaealiste vaikimisi kaitse

Alaealiste kaitse seisneb selles, et nad **ei puutuks** pornograafilise sisuga **kokku** kohe, kui nad avavad avaliku veebipõhise sideteenuse, mis sellist sisu avaldab.

Sellel seoses on SRENi eelnõus sätestatud, et pornograafilist sisu edastavad suunatud teenused peavad kuvama ekraani, mis ei sisalda pornograafilist sisu, „**kuni kasutaja vanuse kinnitamiseni**“.

- **Kriteerium nr 1: vanusekontrolli rangus**

Pornograafilise sisu edastamisega seotud teenused peavad tagama, **et ükski kasutaja ei pääse pornograafilisele sisule juurde enne, kui ta on tõendanud oma täisealisust.**

Näited ja rakendamine

Alaealiste kaitse saab vaikimisi tagada näiteks **teenuse avalehte täielikult hõlgustades**.

Avaldajad saavad oma teenuse pornograafilisest olemusest teavitada. Selleks võivad nad tugineda **enese deklareerimise mehhanismile** [näiteks RTA märgisele¹²], mida kasutatakse saidi kõikidel lehtedel ja mis võimaldab vanemliku kontrolli süsteemidel vastuse päise (või päisete¹³) kaudu teada saada, mis on minimaalne vanus, mis on vajalik saidi sisule juurdepääsuks.

Usaldusväarsuse kriteeriumid

Selle standardi täitmiseks peavad vanusekontrollimissüsteemid (antud juhul täisealisuse) **vastama vähemalt järgmistele tehnilistele nõuetele**. Need nõuded tõenäoliselt tehnikate täiustamise ja uute vanusekontrollisüsteemide turule laskmisega muutuvad.

¹² „Ainult täiskasvanutele“.

¹³ Päised on teave, mille veebilehe server tagastab kasutaja veebilehitsejale taotluse esitamise ajal.

- **Kriteerium nr 2: lahenduse tõhusus**

Pornograafilist sisu edastavate suunatud teenuste poolt kasutusele võetud vanuse kontrollimise tehniline lahendus **peab võimaldama kindlalt eristada alaealisi kasutajaid ja täiskasvanuid.**

Näited ja rakendamine

Kui pornograafilist sisu edastavate suunatud teenuste poolt kasutusele võetud tehniline lahendus põhineb kasutaja vanuse hindamisel, tuleb see konfigureerida nii, et oleks välistatud oht, et alaealist kasutajat peetakse täiskasvanuks („valepositiivsed“).

- **Kriteerium nr 3: kõrvalehoidmise võimaluste piiramine**

Pornograafilist sisu edastavad suunatud teenused peavad tegema kõik endast oleneva, järgides tööstusharu ametialase hoolikuse kõrgeid standardeid; et **piirata nende kasutatavatest tehnilistest lahendustest kõrvale hoidmise võimalusi.**

Vanusekontrollimissüsteemid ei tohiks võimaldada vanuse tõendamist teiste inimestega jagada.

Viimasena peab süsteem olema vastupidav, pidades silmas rünnete ohtu, näiteks *süvavõltsimine, võltsimisirünnakud* jne.

Näited ja rakendamine

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 kõrvalesuunamise 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 sihtteenused kontrollima järgmist: i) dokument on tõene ja mitte koopia; ii) kasutaja on isikut tõendava dokumendi omanik. Kontrolli võib läbi viia eelkõige näoomaduste tuvastamise abil, mis hõlmab elu tuvastamise mehhanismi, vastavalt *ülal* nimetatud tingimustele.

- **Kriteerium nr 4: vanuse kontrollimine igal teeninduskonsultatsioonil**

Vanuse kontrollimine tuleb läbi viia iga kord, kui teenusega seoses konsulteeritakse. Konsultatsiooni katkestamine peab käivitama uue vanusekontrolli, kui kasutaja soovib pornograafilist sisu uuesti avada.

Selle kriteeriumi järgimine 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.

Näited ja rakendamine

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 tegevusest.

- **Kriteerium nr 5: kasutajakonto kasutamise raamistik**

Vanusekontrolli lahenduse rakendamine ei tohi nõuda kasutajakonto loomist pornograafilist sisu pakkuva teenuse kasutamiseks.

Lisaks ei saa vanusetõendit teenuse kasutajakontole salvestada.

Igal juhul kehtib vanuse kontrollimise kohustus kõikide juurdepääsude korral nii kasutajakontoga kui ka ilma selleta.

- **Kriteerium nr 6: mittediskrimineerimine**

Pornograafilist sisu edastavate suunatud teenuste pakutavad lahendused ei tohi diskrimineerida teatavaid elanikkonnarühmi, eelkõige Euroopa Liidu põhiõiguste harta artiklis 21 sätestatud alustel. Seega peab vanuse kontrollimise 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 vanusekontrolli süsteemid **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 eelarvamusel, mis on liigendatud asjakohaste diskrimineerimispõhjuste alusel (vt *allpool*).

Teine osa: eraelu puutumatuse kaitse

Käesoleva raamistiku eelnõu eesmärk on tagada ka **kasutajate eraelu puutumatuse kaitse** vanusekontrollimissüsteemide 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 tipptasemel 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).¹⁴ ¹⁵ 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

¹⁴ <https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee>

¹⁵ <https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie>

vanusekontrollimehhanismidele. See vastab ka digitaalidentiteedi süsteemidele, sealhulgas atribuutide haldamisele üldiselt seatud eesmärkidele. Kuigi käesolevas dokumendis viidatakse sellele kui „kahekordsele 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, mis on kehtestatud [...], 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:

- kriteeriumeid, mida kohaldatakse kõigi käesoleva raamistikuga hõlmatud vanusekontrollisüsteemide suhtes;
- eraelu puutumatust soodustavate süsteemide (kahekordse anonüümsuse süsteemide) konkreetseid eesmärke;
- läbipaistvuskohustusi, mille eesmärk on teavitada kasutajaid teenuste kaudu pakutavate süsteemidega seotud eraelu puutumatuse kaitse tasemest;
- ja häid tavaid, mis on esitatud soovitusena, kuid mida ei ole seni nõutud.

Kõikide vanusekontrollisüsteemide miinimumnõuded

Järgmised kriteeriumid kujutavad endast **miinimumnõuete kogumit, mida kohaldatakse kõigi käesoleva raamistiku eelnõuga hõlmatud vanusekontrollisüsteemide suhtes.**

- **Kriteerium nr 7: vanusekontrollisüsteemi pakkuja sõltumatus suunatud teenuste edastatavast pornograafilisest sisust**

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

- **Kriteerium nr 8: konfidentsiaalsus suunatud teenuste suhtes, mis edastavad pornograafilist sisu**

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

Eelkõige ei tohivanusekontrolli lahenduste rakendamine **lubada käesoleva raamistiku eelnõuga hõlmatud sideteenustel koguda selliste kasutajate identiteeti, vanust, sünniaega ega muid isikuandmeid.**

- **Kriteerium nr 9: konfidentsiaalsus seoses vanuse tõendajatega**

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.

- **Kriteerium nr 10: 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.**

- **Kriteerium nr 11: isikute õiguste ja vabaduste kaitse vanusetõendajate poolt**

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 märkimisväärt mõju.

CNIL leiab, et selline otsus võib põhineda isikuandmete kaitse üldmääruse artikli 22 lõike 2 punktis b sätestatud erandil, kui pornograafilise sisu suunatud teenuse suhtes kehtib karistusseadustiku artikli 227-24 ja viimasena ka PjL 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.

Pornograafilise sisu suunatud teenuse osutaja on siiski kohustatud täitma isikuandmete kaitse üldmäärusega kehtestatud teavitamiskohustusi ja peab teavitama kasutajaid võimalusest esitada vanuse kontrollimise lahenduse pakkujale kaebus.

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

Erinõuded eraelu puutumatuse kaitse süsteemidele, mis järgivad topeltanonüümsuse põhimõtet

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

- **Kriteerium nr 12: konfidentsiaalsus suunatud teenuste suhtes, mis edastavad pornograafilist sisu**

Kriteeriumi nr 8 nõudeid täiendatakse järgmiste nõuetega.

Vanusekontrollimissüsteem, mis kasutab topeltanonüümsust, ei tohiks võimaldada käesoleva raamistiku eelnõuga hõlmatud sideteenustel tunnustada kasutajat, kes on vanusekontrolli käigus saadud 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.

- **Kriteerium nr 13: suurem konfidentsiaalsus vanusetõendite väljastajate juures**

Kriteeriumi nr 9 nõudeid täiendatakse nii, et vanusekontrollimissüsteem, milles kasutatakse topeltanonüümsust, ei tohi võimaldada tõendit tootvatel pakkujatel teada saada, millise teenuse tarbeks vanuse kontrollimine toimub.

- **Kriteerium nr 14: konfidentsiaalsus mis tahes kolmanda isiku suhtes, kes osaleb vanuse kontrollimise protsessis**

Kriteeriumi nr 10 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.

- **Kriteerium nr 15: 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 anonüümsuse süsteem on kättesaadav vähemalt **[80 %]** 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

- **Kriteerium nr 16: kasutaja eraelu puutumatuse 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 tõendus põhised lahendused, mida aktsepteeritakse ajutiselt

[Kuuekuulisel] ülemineku perioodil alates käesoleva raamistiku avaldamisest, mis on loodud selleks, et teenused, mille suhtes neid kohaldatakse, saaksid kindlaks teha ja rakendada vanuse kontrollimise lahenduse, 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 võib toimuda kas 0 euro suuruse maksena või lihtsa autentimise teel (ilma makseta).

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 usaldusväärsetel 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.

Selle ülemineku perioodi lõpus selgitatakse tingimusi, mille korral võidakse jätkuvalt aktsepteerida vanuse kontrollimist pangakaardiga.

Neljas osa: vanusekontrolli lahenduste auditeerimine ja hindamine

SRENi eelnõus on sätestatud, et „Audiovisuaal- ja digitaalside 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 konfigureerida, 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 **kõikidele 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 ründeohule¹⁶.

¹⁶ Vanusekontrollilahenduse ründamise ohu hindamisel tuleb kindlaks teha, kas süsteemi võidakse tõenäoliselt kuritarvitada pettuse eesmärgil.

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 Arcomi täiendava selgituse saamiseni julgustatakse ettevõtteid tegema oma vanusekontrollimissüsteemide tehnilisi auditeid esialgu [...] 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 auditaruannet oma internetipõhise kasutajaliidese kergesti juurdepääsetaval lehel kergesti mõistetavas vormingus**.