

Beraadslaging nr. 2024-20 van 9 oktober 2024 over het kader tot vaststelling van de minimale technische vereisten voor leeftijdsverificatiesystemen die zijn opgezet voor toegang tot bepaalde online openbare communicatiediensten en videoplatforms die pornografische inhoud beschikbaar stellen aan het publiek

NOR: RCAC2428286X

JORF nr. 0251 van 22 oktober 2024

Tekst nr. 50

- Bijlage

De regelgevende instantie voor audiovisuele en digitale communicatie

Gezien Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij;

Gezien op Wet nr. 2004-575 van 21 juni 2004, zoals gewijzigd, inzake het vertrouwen in de digitale economie, en met name op de artikelen 10 en 10-2;

Gezien kennisgeving nr. 2024/0208/FR die op 15 april 2024 aan de Europese Commissie is toegezonden en haar opmerkingen van 15 juli 2024;

Gezien beraadslaging nr. 2024-067 van 26 september 2024 van de Commission nationale de l'informatique et des libertés (Franse gegevensbeschermingsautoriteit) houdende een advies over een ontwerpkader van de regelgevende autoriteit voor audiovisuele en digitale communicatie inzake leeftijdsverificatiesystemen die zijn opgezet voor toegang tot bepaalde diensten die toegang bieden tot pornografische inhoud;

Gezien de opmerkingen die zijn gemaakt tijdens de openbare raadpleging van 11 april tot 11 mei 2024;

Na beraadslaging,

Besluit hierbij:

Artikel 1

Het in de bijlage bij dit besluit uiteengezette kader wordt vastgesteld.

Artikel 2

Deze beraadslaging wordt bekendgemaakt in het Publicatieblad van de Franse Republiek.

Bijlage

BIJLAGE

KADER TER BEPALING VAN DE MINIMALE TECHNISCHE VEREISTEN VOOR LEEFTIJDVERIFICATIESYSTEMEN DIE ZIJN OPGEZET VOOR TOEGANG TOT BEPAALDE ONLINE OPENBARE COMMUNICATIEDIENSTEN EN VIDEOPLATFORMS DIE PORNOGRAFISCHE INHOUD BESCHIKBAAR MAKEN VOOR HET PUBLIEK

Inhoud

Inleiding

De verantwoordelijkheid van gerichte diensten die pornografische inhoud uitzenden

De evolutie van de rol van ARCOM in het kader van de wet om de digitale ruimte te beveiligen en te reguleren

Het lopende werk met betrekking tot leeftijdsverificatie

Presentatie van het kader

Ondersteuning van de sector bij de implementatie van oplossingen voor leeftijdsverificatie

Bijwerken van het kader en de stand van de techniek

Structuur van het kader en implementatieschema

Eerste deel: Algemene overwegingen met betrekking tot de betrouwbaarheid van leeftijdsverificatiesystemen

Tweede deel: Bescherming van de persoonlijke levenssfeer

Beginselen ter bescherming van privacy

Implementatie van een privacyvriendelijk leeftijdsverificatiesysteem door standaardinstellingen en door ontwerp

Minimumvereisten voor alle leeftijdsverificatiesystemen

1. Onafhankelijkheid van de aanbieder van het leeftijdsverificatiesysteem met betrekking tot gerichte diensten die pornografische inhoud uitzenden

2. Vertrouwelijkheid ten opzichte van gerichte diensten die pornografische inhoud uitzenden

3. Vertrouwelijkheid ten aanzien van het bewijs van aanbieders van leeftijdsgeneratie

4. Vertrouwelijkheid ten aanzien van andere derden die betrokken zijn bij het leeftijdsverificatieproces

5. Waarborgen van de rechten en vrijheden van personen per leeftijdsverificatie

Specifieke vereisten voor privacybeschermingssystemen met inachtneming van het beginsel van “dubbele anonimiteit”

6. Verbeterde vertrouwelijkheid ten aanzien van gerichte diensten die pornografische inhoud uitzenden

7. Verbeterde vertrouwelijkheid ten aanzien van uitgevers van leeftijdsattributen

8. Verbeterde vertrouwelijkheid ten aanzien van andere derden die betrokken zijn bij het leeftijdsverificatieproces

9. Beschikbaarheid en dekking van de bevolking

Gebruikers informeren over de mate van privacy die verbonden is aan leeftijdsverificatiesystemen

10. Expliciete weergave van het niveau van privacybescherming van de gebruiker

Gewenste doelstellingen en optimale werkwijzen

Derde deel: Afwijkende oplossingen voor bewijs van leeftijd geaccepteerd op tijdelijke basis

Vierde deel: Audit en evaluatie van oplossingen voor leeftijdsverificatie

Evaluatie van de onder reële omstandigheden ingevoerde systemen

Foutpercentages, omzeiling en risico van aanvallen

Onafhankelijkheid van de aanbieder van de audit

Inleiding

De verantwoordelijkheid van gerichte diensten die pornografische inhoud uitzenden

1. Met de democratisering van mobiele apparaten die toegang bieden tot het internet voor kinderen, stijgt de blootstelling van minderjarigen aan pornografische inhoud op het internet snel.

Volgens een studie die door de Audiovisuele en Digitale Communicatie Regelgevende Autoriteit (Arcom) op basis van door Médiamétrie verstrekte gegevens is uitgevoerd, bezoeken 2,3 miljoen minderjarigen pornografische sites maandelijks, waarbij dit aantal de afgelopen jaren snel is toegenomen en verband houdt met de democratisering van mobiele apparaten onder kinderen. Het aantal minderjarigen dat sites voor “volwassen” bezoekt, is binnen 5 jaar tijd met 9 punten gestegen, van 19 % eind 2017 naar 28 % eind 2022. Elke maand in 2022 bezocht meer dan de helft van de jongens van 12 jaar en ouder dergelijke sites, een cijfer dat oploopt tot tweederde van de jongens van 16 en 17 jaar. Gemiddeld bestaat 12 % van het publiek van sites voor volwassenen uit minderjarigen (1).

Sinds het begin van de jaren 2000 (2) blijkt uit onderzoek naar de gevolgen van vroege blootstelling aan pornografie dat het blootstellen van de jongste kinderen aan pornografische inhoud ernstige gevolgen kan hebben voor hun mentale ontwikkeling en het beeld dat ze vormen van seksualiteit en relaties tussen individuen, ten koste van hun persoonlijke ontwikkeling en meer gelijkheid in genderverhoudingen (3).

2. Sinds 1 maart 1994 is het krachtens artikel 227-24 van de Strafwet, ingevoerd bij wet nr. 92-684 van 22 juli 1992, verboden minderjarigen bloot te stellen aan pornografische inhoud. De formulering van dit artikel is gewijzigd om niet alleen het toepassingsgebied ervan te verduidelijken, maar ook hoe het dient te worden beoordeeld wanneer er een strafbaar feit op het internet wordt geregistreerd. In overeenstemming met de vaste rechtspraak bepaalt artikel 227-24 sinds 2020 dat een loutere leeftijdsverklaring niet volstaat om de leeftijd van meerderjarigheid aan te tonen (4). De huidige formulering luidt als volgt:

“ De vervaardiging, het vervoer, de verspreiding op welke wijze dan ook en ongeacht het medium van een boodschap van gewelddadige, aanzetten tot terrorisme, pornografische aard, met inbegrip van pornografische beelden waarbij één of meer dieren betrokken zijn, of die de menselijke waardigheid ernstig kunnen schaden of minderjarigen ertoe aanzetten om deel te nemen aan spelletjes die hen fysiek in gevaar brengen, of de handel in een dergelijke boodschap, worden bestraft met een gevangenisstraf van 3 jaar en een boete van 75.000 EUR wanneer de boodschap waarschijnlijk door een minderjarige wordt gezien of waargenomen.

“ Wanneer de in dit artikel bedoelde strafbare feiten door de schrijvende of audiovisuele pers of door middel van online openbare communicatie worden voorgelegd, zijn de bijzondere bepalingen van de wetgeving betreffende deze aangelegenheden van toepassing met betrekking tot de vaststelling van de verantwoordelijke personen.

“ De in dit artikel bedoelde strafbare feiten worden ook gevormd indien de toegang van een minderjarige tot de in het eerste lid bedoelde boodschappen voortvloeit uit een loutere verklaring van de minderjarige dat hij of zij ten minste 18 jaar oud is.”

De wetgever heeft bij wet nr. 2020-936 van 30 juli 2020 ter bescherming van slachtoffers van huiselijk geweld, een speciale procedure ingevoerd, waarbij Arcom betrokken is, tot waarborging van de volledige doeltreffendheid van deze bepalingen betreffende online openbare communicatiediensten die pornografische inhoud op het internet beschikbaar stellen aan het publiek.

Deze wet vertrouwdde de voorzitter van Arcom bijgevolg het voorrecht toe om de uitgever van een site een formele kennisgeving te sturen om te voldoen aan de Strafwet en, als deze kennisgeving niet wordt opgevolgd, om de gewone rechter te vragen aanbieders van internettoegang (IAP's, Internet Access Providers) te gelasten om de toegang tot deze site te verhinderen.

3. Op basis van deze bepalingen heeft de autoriteit 13 aanmaningen uitgevaardigd. Het verwees ook naar de zaak op 8 maart 2022, aan de voorzitter van de Rechtbank van Parijs om de IAP's te gelasten vijf van deze diensten aan de hand van ingebrekestelling te blokkeren. Deze procedure loopt nog op de datum van publicatie van dit kader.

De evolutie van de rol van ARCOM in het kader van de wet om de digitale ruimte te beveiligen en te reguleren

Wet nr. 2024-449 van 21 mei 2024 voor de beveiliging en regulering van de digitale ruimte (SREN) heeft het systeem van de wet van 30 juli 2020 bijgewerkt.

Artikel 10 van wet nr. 2004-575 van 21 juni 2004 inzake vertrouwen in de digitale economie (LCEN) bepaalt dat ARCOM “plaatst en publiceert [...], na raadpleging van de Franse Autoriteit voor Gegevensbescherming, een kader voor de vaststelling van minimale technische vereisten voor leeftijdsverificatiesystemen. Deze vereisten hebben betrekking op de betrouwbaarheid van de leeftijdsverificatie van gebruikers en het respect voor hun privacy.” Het toepassingsgebied van het systeem betreft “pornografische inhoud die onder zijn redactionele verantwoordelijkheid beschikbaar wordt gesteld aan het publiek door een uitgever van een online openbare communicatiedienst, of die wordt verstrekt door een videoplatformdienst in de zin van artikel 2 van wet nr. 86-1067 van 30 september 1986 betreffende de vrijheid van communiceren” (hierna “gerichte diensten die pornografische inhoud uitzenden” of de “gerichte diensten” genoemd). ARCOM mag, in voorkomend geval na advies van de voorzitter van de CNIL, een van deze diensten aan te manen om aan dit kader te voldoen en, indien de inbreuk voortduurt, de dienst na het verkrijgen van het advies van de CNIL, een geldelijke sanctie op te leggen volgens de procedure van artikel 42-7 van wet nr. 86-1067 van 30 september 1986.

De nieuwe bevoegdheden die door de SREN-wet aan ARCOM worden toegekend, zouden een aanvulling vormen op de bevoegdheden die anders worden toegekend aan de rechter, die rechtstreeks kan worden verzocht tot het blokkeren van een site die niet voldoet aan de bepalingen van artikel 227-24 van de Strafwet, op basis van bijvoorbeeld artikel 6-3 van het LCEN, op basis van bijvoorbeeld artikel 6-3 van het LCEN.

Bovendien maakt de bescherming van minderjarigen tegen de toegang tot pornografische inhoud deel uit van een meer algemeen kader voor de bescherming van kinderen, met name het Verdrag van de Verenigde Naties inzake de rechten van het kind van 20 november 1989 en algemene opmerking nr. 25 van 2021 over de rechten van het kind in verband met de digitale omgeving (5), en artikel 24 van het Handvest van de grondrechten van de Europese Unie van 7 december 2000, waarin is bepaald dat “het belang van het kind een eerste overweging dient te zijn”.

Het lopende werk met betrekking tot leeftijdsverificatie

Dit document maakt deel uit van de in de afgelopen jaren door de CNIL verrichte werkzaamheden met betrekking tot leeftijdsverificatie om de bescherming van minderjarigen en respect voor privacy met elkaar te verzoenen.

De CNIL bracht in juni 2021 voor het eerst een advies uit over het ontwerpbesluit voor de tenuitvoerlegging van de wet van 2020 inzake uitvoeringsvoorschriften ter bescherming van minderjarigen tegen toegang tot online openbare communicatiediensten die pornografische inhoud uitzenden (6). Om te voorkomen dat de seksuele geaardheid van mensen – echt of verondersteld – wordt afgeleid uit de bekeken inhoud en rechtstreeks aan hun identiteit wordt gekoppeld, adviseerde de CNIL aan de hand van dit standpunt om vertrouwde derden in te schakelen en deed verschillende aanbevelingen (7), met inbegrip van een gedeelte over leeftijdsverificatie. Deze publicaties werden ondersteund door een mededeling die in juli 2022 werd gepubliceerd, getiteld “Online leeftijdsverificatie: een evenwicht vinden tussen het beschermen van minderjarigen en het respecteren van privacy” (8) en de introductie van een demonstratiemodel van een leeftijdsverificatiemechanisme dat de privacy van gebruikers respecteert (9), in samenwerking met PEReN en Olivier Blazy, professor aan de École Polytechnique.

De CNIL heeft reeds de gelegenheid gehad om eraan te herinneren dat “In tegenstelling tot wat er soms gezegd wordt, de AVG (10) niet onverenigbaar is met leeftijdsverificatie voor de toegang tot pornografische sites, die bij wet is geregeld.” (11)

Net als de CNIL heeft ARCOM ook advies uitgebracht over het ontwerpbesluit tot uitvoering van artikel 23 van de wet van 30 juli 2020 (12).

Het is in deze context dat Arcom en CNIL, met de steun van PEReN, begin 2023 begonnen met gezamenlijke technische uitwisselingen met deelnemers aan leeftijdsverificatie. Deze discussies werden verrijkt door de feedback die Arcom kreeg van een aantal zijn buitenlandse tegenhangers, die ook worden geconfronteerd met de uitdagingen van de bescherming van minderjarigen en privacy bij het beheren van de toegang tot pornografische inhoud.

Dit kader is vastgesteld na een openbare raadpleging van 11 april tot en met 13 mei en de kennisgeving ervan aan de Europese Commissie op 15 april uit hoofde van Richtlijn 2015/1535 van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij, en beraadslaging nr. 2024-067 van de CNIL van 26 september 2024 met een advies over het ontwerp-kader.

Presentatie van het kader

Ondersteuning van de sector bij de implementatie van oplossingen voor leeftijdsverificatie

In overeenstemming met de bepalingen van de wet specificeert het kader de verwachte technische voorschriften.

Het doel van dit kader is niet om technische oplossingen te certificeren.

Het blijft de gerichte diensten die pornografische inhoud uitzenden, vrijstaan om hun eigen oplossingen voor de bescherming van minderjarigen te kiezen, mits zij voldoen aan de technische vereisten van het kader.

Het ontbreken van een leeftijdsverificatiesysteem, evenals leeftijdsverificatiesystemen die onbetrouwbaar zijn of een lager niveau van privacybescherming bieden dan dit kader vereist, komen niet in aanmerking.

Bijwerken van het kader en de stand van de techniek

Het kader kan worden herzien en bijgewerkt om rekening te houden met de stand van de techniek. De SREN-wet bepaalt in dit verband dat het “kader zo nodig onder dezelfde voorwaarden wordt bijgewerkt”.

Het is in feite wenselijk dat de sector oplossingen voor leeftijdsverificatie hanteert die overeenstemmen met de stand van de techniek en de Europese en internationale normen (in het bijzonder Europese normen die op korte termijn verschijnen), en die verenigbaar zijn met de praktijken van de industrie, met name wat de bestaande technische protocollen betreft.

Vanuit die gedachte hebben de Franse autoriteiten in antwoord op een verzoek om informatie van de Europese Commissie in het kader van de kennisgevingsprocedure van Richtlijn 2015/1535 van 9 september 2015 betreffende een procedure voor de verstrekking van informatie op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (gecodificeerde tekst) het volgende aangegeven:

“ Wat de toekomst betreft, verbinden zij zich ertoe hun interne rechtskader geheel of gedeeltelijk te herzien wanneer een voldoende nauwkeurige rechtsgrondslag op EU-niveau het mogelijk zal maken een doeltreffend systeem voor leeftijdsverificatie op te leggen aan alle of sommige platforms waarop toegang tot pornografische inhoud betrekking heeft.

“ In deze omstandigheden zien zij het [kader] als een overgangso oplossing, in afwachting van een doeltreffende Europese oplossing.”

Structuur van het kader en implementatieschema

Het eerste deel van het kader beschrijft de algemene overwegingen over de betrouwbaarheid van wettelijke leeftijdsverificatiesystemen. Naast de noodzaak om de bescherming van minderjarigen standaard te waarborgen, d.w.z. zelfs vóórdat toegang tot de dienst wordt verkregen, is het noodzakelijk om de voorwaarden voor de doeltreffendheid van online leeftijdsverificatiesystemen opnieuw te bekijken en het omzeilen ervan te voorkomen.

Het tweede deel behandelt in het bijzonder de bescherming van privacy door leeftijdsverificatiesystemen die worden ingezet om de toegang tot pornografische inhoud te beheren. Sites kunnen leeftijdsverificatiesystemen met verschillende privacybeschermingsniveau aanbieden, op voorwaarde dat gebruikers worden geïnformeerd over het niveau dat aan elk systeem is gekoppeld.

In dit verband voorziet het kader in minimumdoelstellingen voor alle leeftijdsverificatiesystemen, evenals versterkte specifieke doelstellingen voor de meest privacyvriendelijke systemen die bekend staan als “dubbele anonimiteit”. Er dient ten minste één leeftijdsverificatiesysteem aan gebruikers te worden aangeboden, dat voldoet aan de privacybeschermingsnormen voor “dubbele anonimiteit”.

Dit tweede deel omvat ook optimale werkwijzen op het gebied van gegevensbescherming, die wenselijk worden geacht.

Bovendien kunnen de gerichte diensten die pornografische inhoud uitzenden, op tijdelijke basis oplossingen kunnen implementeren voor het genereren van bewijs van leeftijd, op basis van de verstrekking van een bankpas, in afwijking van de voorwaarden van het eerste en het tweede deel, maar met strikte inachtneming van bepaalde cumulatieve voorwaarden die zijn vastgesteld in het derde deel van dit document.

Tot slot stelt het vierde en laatste deel de belangrijkste beginselen vast die als leidraad kunnen dienen voor het feit dat de diensten die van plan zijn pornografische inhoud uit te zenden, verplicht zijn tot het uitvoeren van een audit van hun leeftijdsverificatiesystemen. In

het bijzonder worden het doel van dergelijke audits, de voorwaarden op grond waarvan ze worden uitgevoerd en de vereisten die van toepassing zijn op externe accountants, gespecificeerd.

EERSTE DEEL: ALGEMENE OVERWEGINGEN MET BETREKKING TOT DE BETROUWBAARHEID VAN LEEFTIJDVERIFICATIESYSTEMEN

Het doel van dit kader is om standaard de bescherming van minderjarigen te waarborgen, zodra de eerste pagina van een online communicatiedienst die de uitzending van pornografische inhoud mogelijk maakt, wordt weergegeven.

De bescherming van minderjarigen houdt inderdaad in dat wordt voorkomen dat zij worden blootgesteld aan pornografische inhoud zodra zij toegang hebben tot online openbare communicatiediensten die dergelijke inhoud beschikbaar stellen.

In dit verband bepaalt artikel 1 van de SREN-wet expliciet dat gerichte diensten die pornografische inhoud uitzenden, verplicht zijn een scherm weer te geven dat geen pornografische inhoud bevat “totdat de leeftijd van de gebruiker is geverifieerd”.

Bovendien dienen de gerichte diensten die pornografische inhoud uitzenden er volgens de SREN-wet voor te zorgen dat geen enkele gebruiker toegang heeft tot pornografische inhoud voordat zijn of haar meerderjarigheid is bewezen.

Deze bescherming van minderjarigen kan standaard worden gewaarborgd, bijvoorbeeld door de startpagina van de dienst volledig te vervagen. Uitgevers kunnen ook het pornografische karakter van hun dienst melden. Hiertoe kunnen ze vertrouwen op een mechanisme van eigen verklaring zoals het RTA-label (13) dat op elke pagina van hun sites wordt ingesteld, zodat systemen voor ouderlijk toezicht de minimumleeftijd kunnen achterhalen die is vereist om toegang tot de inhoud op de site te krijgen, door middel van antwoordkoppen (of “kopteksten” [14]).

Om aan de wet te voldoen, dienen leeftijdsverificatiesystemen (in dit geval meerderjarigheid) die zijn ingesteld door de gerichte diensten die pornografische inhoud uitzenden, onderscheid te kunnen maken tussen gebruikers die minderjarig zijn en gebruikers die meerderjarig zijn. Oplossingen zullen zich waarschijnlijk verder ontwikkelen met de verbetering van de technieken en het in de handel brengen van nieuwe leeftijdsverificatiesystemen, inclusief eventuele Europese normen die op korte termijn verschijnen.

Wanneer de technische oplossing van de gerichte diensten die pornografische inhoud uitzenden, wordt gebaseerd op een schatting van de leeftijd van de gebruiker, betekent naleving van de wet dat deze zo dient te worden geconfigureerd dat het risico wordt uitgesloten dat een minderjarige gebruiker als een volwassene wordt beschouwd (“valse positieven”).

Om aan de wet te voldoen, dienen gerichte diensten die pornografische inhoud uitzenden, alles in het werk te stellen, in overeenstemming met de hoge normen in de sector op het gebied van professionele toewijding, om de mogelijkheden van omzeiling van de door hen ingevoerde technische oplossingen te beperken. Leeftijdsverificatiesystemen mogen niet toestaan dat het bewijs van leeftijd met andere mensen wordt gedeeld om het risico op fraude te beperken. Het systeem dient dus robuust te zijn in het licht van de risico's van aanvallen, zoals deepfakes, spoofing, enz.

Bijvoorbeeld met betrekking tot oplossingen op basis van een schatting van de leeftijd door het analyseren van gezichtskenmerken, dienen de gerichte diensten die pornografische inhoud uitzenden, ervoor te zorgen dat de oplossingen een mechanisme voor de herkenning van levende personenopnamen, waarvan de doeltreffendheid in overeenstemming is met de

stand van de techniek. Detectie wordt uitgevoerd door middel van een beeld van voldoende kwaliteit, met uitsluiting van enig omleidingsproces dat door minderjarigen kan worden gebruikt om kunstmatig volwassenen te lijken, met name door het gebruik van foto's, opgenomen video's of maskers. Tot slot, met betrekking tot technische oplossingen voor het genereren van bewijs van leeftijd op basis van de vertegenwoordiging van een fysiek identiteitsdocument, wordt verwacht dat de gerichte diensten die pornografische inhoud uitzenden ervoor zorgen dat de technische oplossingen die zij invoeren het mogelijk maken om te verifiëren: (i) dat het document echt is en dat het niet louter een kopie is; (ii) dat de gebruiker de houder is van het ingevulde identiteitsdocument. Deze verificatie kan met name worden uitgevoerd door middel van een gezichtsherkenning met behulp van een mechanisme voor de detectie van leven, onder de hierboven gespecificeerde voorwaarden. Om te voorkomen dat minderjarigen online worden blootgesteld aan pornografische inhoud, wordt verwacht dat er een leeftijdscontrole wordt uitgevoerd telkens wanneer een dienst wordt geraadpleegd. De onderbreking van deze raadpleging dient dus te leiden tot een nieuwe leeftijdsverificatie als de gebruiker opnieuw toegang wenst te krijgen tot pornografische inhoud. Dit doet geen afbreuk aan de mogelijkheid voor de gebruiker om bewijs van leeftijd te gebruiken dat door hem of haar kan worden hergebruikt of geregenereerd, onder voorbehoud van de aanwezigheid van een tweede verificatiefactor. Dit kan worden gedaan door het gebruik van het herbruikbare bewijs te koppelen aan de terminal van de betrokkene, zoals het geval is met digitale portemonnees.

Bovendien mag het verificatiesysteem niet toestaan dat dit bewijs wordt gedeeld met een andere persoon of dienst. In het geval van een raadplegingsterminal die wordt gedeeld tussen een volwassene en een minderjarige, is het belangrijk te voorkomen dat de geldigheidsduur van de leeftijdsverificatie het mogelijk maakt pornografische inhoud zonder verdere verificatie toegankelijk te maken. Er kan van worden uitgegaan dat de geldigheid van een leeftijdsverificatie daarom dient te worden onderbroken wanneer de gebruiker de dienst verlaat, d.w.z. wanneer de sessie eindigt, wanneer de gebruiker de browser afsluit of wanneer het besturingssysteem in stand-bymodus overgaat en in ieder geval na een periode van een uur van inactiviteit.

Om te voorkomen dat het hergebruik van gebruikersaccounts ertoe leidt dat minderjarigen toegang krijgen tot pornografische inhoud, wordt verwacht dat het bewijs van leeftijd niet kan worden opgeslagen in een gebruikersaccount op de gerichte dienst. In ieder geval volgt uit de wet dat de verplichting tot leeftijdsverificatie geldt voor elke toegang, met of zonder gebruikersaccount.

Om de bescherming van minderjarigen en de naleving van de wet te garanderen, wordt verwacht dat de oplossingen die worden gebruikt door de gerichte diensten die pornografische inhoud uitzenden, doeltreffend zijn voor alle bevolkingsgroepen en daarom niet tot gevolg hebben dat bepaalde groepen worden gediscrimineerd, met name op grond van artikel 21 van het Handvest van de grondrechten van de Europese Unie. Bijgevolg zal de doeltreffendheid van de technische oplossing voor leeftijdsverificatie hetzelfde zijn, ongeacht de fysieke kenmerken van de gebruiker. In het geval van bewijs-van-leeftijd-generatiesystemen op basis van machinelere of statistische modellen, kunnen dienstverleners hun oplossing bijvoorbeeld testen op verschillende databanken om ervoor te zorgen dat aan deze vereiste wordt voldaan. Het is van essentieel belang dat leeftijdsverificatiesystemen discriminerende vooroordelen beperken, die ook leiden tot fouten die zowel hun betrouwbaarheid als hun aanvaardbaarheid in twijfel kunnen trekken. Gerichte diensten die pornografische inhoud uitzenden, worden verzocht om bij de beoordeling van de prestaties van hun leeftijdsverificatiesysteem, maar ook in alle audits die zij uitvoeren (zie hieronder), discriminerende vooroordelen op te nemen, uitgesplitst op basis van de relevante gronden voor discriminatie.

TWEEDE DEEL: BESCHERMING VAN PRIVACY

Het doel van dit kader is ook het waarborgen van de bescherming van de privacy van de gebruikers van leeftijdsverificatiesystemen. Deze systemen kunnen grote risico's inhouden voor de beveiliging van persoonsgegevens, aangezien leeftijdsverificatie vergelijkbaar is met identiteitsverificatie en daarom het verzamelen van gevoelige gegevens of identiteitsdocumenten kan vereisen.

Degenen die betrokken zijn bij leeftijdsverificatiesystemen dienen daarom bijzondere aandacht te besteden aan de bescherming van de privacy van hun gebruikers en de beveiliging van de betrokken informatiesystemen, beginselen waarvoor eerbiediging de verantwoordelijkheid van de CNIL is, met name de algemene verordening gegevensbescherming (AVG).

Beginselen ter bescherming van privacy

In de praktijk dienen leeftijdsverificatiesystemen te voldoen aan de bestaande wetgeving inzake de bescherming van persoonsgegevens en privacy, met inbegrip van de beginselen van minimalisering en gegevensbescherming door ontwerp en door standaardinstellingen (artikelen 5 en 25 van de AVG).

Aanbieders van dergelijke systemen dienen bijzondere aandacht te besteden aan de volgende beginselen:

nauwkeurigheid, evenredigheid en minimalisering van de verzamelde gegevens;
beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke gebruikersinformatie;
passende gegevensbewaartermijnen;
de mogelijkheid voor personen om hun rechten uit te oefenen, namelijk het recht van toegang, het recht van bezwaar, het recht op rectificatie, het recht op beperking van de verwerking, het recht op gegevenswissing, het overdraagbaarheidsrecht;
State-of-the-art beveiliging voor informatiesystemen die worden gebruikt voor de verwerking van persoonsgegevens.

Implementatie van een privacyvriendelijk leeftijdsverificatiesysteem door standaardinstellingen en door ontwerp

In 2022 publiceerde de CNIL een privacyvriendelijk mechanisme voor leeftijdsverificatie voor de overdracht van een identificerend attribuut (in dit geval bewijs van leeftijd) (15), (16). Het voorgestelde mechanisme zorgt er met name voor dat er een waterdichte afdichting bestaat tussen de gerichte diensten die pornografische inhoud uitzenden, die verplicht zijn de leeftijd van hun gebruikers te controleren, en derden die leeftijdskenmerken afgeven. Dit mechanisme, dat sindsdien bekend staat als “dubbele anonimiteit” of “dubbele vertrouwelijkheid”, is ontwikkeld en getest door verschillende publieke en particuliere deelnemers, waarmee de technische haalbaarheid ervan en het vermogen ervan om tegemoet te komen aan de behoefte aan privacybescherming die inherent zijn aan online mechanismen

voor leeftijdsverificatie, worden bevestigd. Het komt ook overeen met de doelstellingen die in het algemeen zijn vastgesteld voor digitale identiteitssystemen, met inbegrip van attribootbeheer. Dit mechanisme, dat in dit document “dubbele anonimiteit” wordt genoemd, is evenwel niet “anoniem” in de zin van de AVG, maar garandeert niettemin een hoge mate van vertrouwelijkheid.

Online openbare communicatiediensten die pornografische inhoud beschikbaar stellen, dienen hun gebruikers ten minste één leeftijdsverificatiesysteem aan te bieden dat voldoet aan de privacynormen voor “dubbele anonimiteit”, zodat dit systeem door een grote meerderheid van de gebruikers ervan kan worden gebruikt.

Deze vereiste treedt in werking aan het einde van de overgangsperiode waarin is voorzien in het derde deel van dit kader, dat is vastgesteld op 6 maanden na de publicatie ervan, onverminderd de vastgestelde minimumvereisten hieronder. Tot die datum dienen leeftijdsverificatiesystemen dus te voldoen aan de onderstaande minimumvereisten om een aanvaardbaar niveau van bescherming van de persoonsgegevens van hun gebruikers te waarborgen.

De volgende delen specificeren:

- de vereisten die van toepassing zijn op alle leeftijdsverificatiesystemen die onder dit kader vallen;
- de specifieke doelstellingen voor de meest privacyvriendelijke systemen, bekend als “dubbele anonimiteit”;
- de transparantieverplichtingen die erop gericht zijn gebruikers te informeren over het niveau van privacybescherming dat verbonden is aan de systemen die op de diensten worden aangeboden;
- evenals goede praktijken die zijn omschreven als wenselijk, maar tot op heden niet als vereist.

Minimumvereisten voor alle leeftijdsverificatiesystemen

Een minimumset vereisten is van toepassing op alle leeftijdsverificatiesystemen die onder dit kader vallen:

1. Onafhankelijkheid van de aanbieder van het leeftijdsverificatiesysteem met betrekking tot gerichte diensten die pornografische inhoud uitzenden

De aanbieder van leeftijdsverificatiesystemen is juridisch en technisch onafhankelijk van enige onder dit kader vallende online openbare communicatiedienst en zorgt ervoor dat gerichte diensten die pornografische inhoud uitzenden, in geen geval toegang hebben tot de gegevens die worden gebruikt om de leeftijd van de gebruiker te verifiëren.

2. Vertrouwelijkheid ten opzichte van gerichte diensten die pornografische inhoud uitzenden
De persoonsgegevens die de gebruiker in staat stellen zijn leeftijd te verifiëren bij een communicatiedienst die onder dit kader valt, mogen niet worden verwerkt door deze communicatiedienst.

In het bijzonder staat de implementatie van oplossingen voor leeftijdsverificatie de onder dit kader vallende communicatiediensten niet toe de identiteit, leeftijd, geboortedatum of andere persoonsgegevens van dergelijke gebruikers te verzamelen.

3. Vertrouwelijkheid ten aanzien van het bewijs van aanbieders van leeftijdsgeneratie
Wanneer het leeftijdsverificatiesysteem de gebruiker niet in staat stelt een herbruikbare digitale identiteit of bewijs van leeftijd te verkrijgen, mogen de persoonsgegevens die door

de gebruiker worden verstrekt om dit kenmerk te verkrijgen, niet worden bewaard door de aanbieder die het bewijs van leeftijd genereert.

Bovendien mag voor dit type systeem niet worden vereist dat er officiële identiteitsdocumenten worden ingezameld als het geen herbruikbaar bewijs van leeftijd genereert.

Deze eis doet geen afbreuk aan de naleving van wettelijke en reglementaire verplichtingen die anderszins van toepassing zijn op bepaalde aanbieders van bewijs van leeftijd.

4. Vertrouwelijkheid ten aanzien van andere derden die betrokken zijn bij het leeftijdsverificatieproces

Wanneer er andere derden dan aanbieders die bewijs van leeftijd genereren, zijn betrokken bij het leeftijdsverificatieproces, bijvoorbeeld voor het beheer van bewijzen of facturering van de dienst, mogen deze derden geen persoonsgegevens van gebruikers van het systeem opslaan, met uitzondering van de opslag van bewijs op verzoek van de gebruiker.

5. Waarborgen van de rechten en vrijheden van personen per leeftijdsverificatie

Wanneer wordt bepaald of een gebruiker al dan niet toegang heeft tot een online openbare communicatiedienst op basis van bewijsmateriaal dat eraan is voorgelegd, neemt de gerichte dienst die pornografische inhoud uitzendt een geautomatiseerd besluit in de zin van artikel 22 van de AVG. Door de toegang tot een dienst te weigeren, kan dit besluit rechtsgevolgen teweegbrengen voor de betrokkenen of op zijn minst op soortgelijke wijze aanzienlijke gevolgen hebben voor personen.

De CNIL is van mening dat een dergelijk besluit kan worden gebaseerd op de uitzondering van artikel 22, lid 2, onder b), van de AVG, voor zover de gerichte dienst die pornografische inhoud uitzendt, wordt onderworpen aan een leeftijdsverificatieverplichting uit hoofde van artikel 227-24 van de Strafwet en de bepalingen van de SREN-wet. Artikel 22, lid 2, onder b), van de AVG vereist dat er passende maatregelen worden genomen tot bescherming van de rechten en vrijheden en de beschermingsbelangen van de betrokkene in de bepalingen die dit geautomatiseerde besluit toestaan.

Met het oog op de privacybescherming die is gericht op het beperken van het vermogen van diensten om personen te identificeren, mogen dergelijke maatregelen niet worden genomen door de gerichte dienst die pornografische inhoud uitzendt, maar door de aanbieder van de technische oplossing voor leeftijdsverificatie, ongeacht of het de aanbieder van het attribuut dan wel de uitgever van het bewijs betreft. Dergelijke maatregelen dienen gebruikers in staat te stellen om, in geval van een fout, het resultaat van de analyse van hun attribuut aan te vechten om een bewijs van leeftijd te verkrijgen. Voor de uitoefening van deze oplossingen dienen deze aanbieders van leeftijdsverificatieoplossingen gebruikers de mogelijkheid te bieden om verschillende aanbieders van attributen of, afhankelijk van de oplossingen, verschillende uitgevers van bewijsmiddelen te gebruiken.

De gerichte dienst die pornografische inhoud uitzendt, is niettemin, net als aanbieders van technische oplossingen voor leeftijdsverificatie, verplicht om te voldoen aan de door de AVG opgelegde informatieverplichtingen en dient gebruikers te informeren over de mogelijkheid om een klacht in te dienen bij de aanbieder van de leeftijdsverificatieoplossing. In ieder geval dienen aanbieders van attributen personen ook toestaan hun gegevens te rectificeren op grond van artikel 16 van de AVG.

Specifieke vereisten voor privacybeschermingssystemen met inachtneming van het beginsel van “dubbele anonimiteit”

De volgende doelstellingen vormen een aanvulling op de doelstellingen van de minimumbasis om een privacyvriendelijke standaard voor online leeftijdsverificatie vast te stellen.

6. Verbeterde vertrouwelijkheid ten aanzien van gerichte diensten die pornografische inhoud uitzenden

De vereisten in nr. 2 worden aangevuld met het volgende.

Een leeftijdsverificatiesysteem met “dubbele anonimiteit” mag de onder dit kader vallende communicatiediensten niet in staat stellen een gebruiker te herkennen die het systeem reeds heeft gebruikt op basis van de gegevens die door het leeftijdsverificatieproces zijn gegenereerd.

Het gebruik van systemen voor leeftijdsverificatie waarbij gebruik wordt gemaakt van “dubbele anonimiteit” mag deze diensten niet in staat stellen de bron of methode te kennen of af te leiden om een bewijs van leeftijd te verkrijgen dat betrokken is bij het leeftijdsverificatieproces van een gebruiker.

Een systeem voor leeftijdsverificatie met “dubbele anonimiteit” mag niet toelaten dat deze diensten kunnen herkennen dat twee bewijzen van meerderjarigheid afkomstig zijn van dezelfde bron van bewijs van leeftijd.

7. Verbeterde vertrouwelijkheid ten aanzien van uitgevers van leeftijdsattributen

De vereisten in nr. 3 worden aangevuld, zodat een leeftijdsverificatiesysteem dat gebruikmaakt van “dubbele anonimiteit” niet in staat mag zijn om te weten voor welke dienst de leeftijdsverificatie wordt uitgevoerd.

8. Verbeterde vertrouwelijkheid ten aanzien van andere derden die betrokken zijn bij het leeftijdsverificatieproces

De vereisten in nr. 4 worden aangevuld met de volgende vereisten:

Een leeftijdsverificatiesysteem met “dubbele anonimiteit” mag niet toestaan dat andere bij het proces betrokken derden een gebruiker die het systeem al heeft gebruikt, herkennen. Een derde partij die bewijs van leeftijd levert of de geldigheid ervan certificeert, mag bijvoorbeeld niet in staat zijn te weten of hij al bewijs van dezelfde gebruiker heeft verwerkt.

9. Beschikbaarheid en dekking van de bevolking

De communicatiediensten die onder dit kader vallen, dienen ervoor te zorgen dat hun gebruikers ten minste twee verschillende methoden voor het verkrijgen van bewijs van leeftijd hebben door middel van een systeem voor leeftijdsverificatie met “dubbele anonimiteit”. In de praktijk dient een dienstverlener die een dubbele anonimiteitsoplossing aanbiedt, ten minste twee methoden te combineren om een bewijs van leeftijd te verkrijgen (bijv. een oplossing op basis van identiteitsdocumenten en één op basis van leeftijdsschatting).

De communicatiediensten die onder dit kader vallen, dienen ervoor te zorgen dat er een systeem voor leeftijdsverificatie met “dubbele anonimiteit” beschikbaar is voor ten minste 80 % van de volwassen bevolking die in Frankrijk woont.

Voorbeelden en toepassing:

In de praktijk dienen oplossingen met “dubbele anonimiteit” verschillende aanbieders voor het verkrijgen van bewijs van leeftijd aan te bieden (bijv. verschillende aanbieders van internettoegang en/of banken) en voor andere oplossingen, verschillende methoden voor het verkrijgen van bewijs van leeftijd (bijv. analyse van de gezichtskenmerken en het verstrekken van identiteitsdocumenten).

Gebruikers informeren over de mate van privacy die verbonden is aan leeftijdsverificatiesystemen

10. Expliciete weergave van het niveau van privacybescherming van de gebruiker
Elke leeftijdsverificatieoplossing dient expliciet te worden gekoppeld aan het niveau van privacybescherming, zodat oplossingen die voldoen aan de normen voor “dubbele anonimiteit” duidelijk en leesbaar worden weergegeven. In ieder geval mogen andere oplossingen niet worden verward of gepromoot om de gebruiker te misleiden ten gunste van oplossingen die de privacy in mindere mate beschermen.
Wanneer een derde partij die betrokken is bij het leeftijdsverificatieproces op de hoogte is van de dienst waarvoor de leeftijdsverificatie wordt uitgevoerd, dient de gebruiker hierover duidelijk te worden geïnformeerd.
Wat betreft leeftijdsverificatiesystemen die voldoen aan het beginsel van “dubbele anonimiteit”, dient de gebruiker duidelijk te worden geïnformeerd dat deze oplossing waarborgt dat de aanbieder van de leeftijdsverificatie niet weet voor welke dienst deze verificatie wordt uitgevoerd.

Gewenste doelstellingen en optimale werkwijzen

De volgende doelstellingen worden nog niet vereist voor leeftijdsverificatiesystemen om aan dit kader te voldoen, maar vormen een reeks optimale werkwijzen die door leeftijdsverificatieoplossingen dienen te worden nagestreefd.
Mogelijkheid voor gebruikers om zelf op vertrouwelijke wijze bewijs van leeftijd te genereren:

de gebruiker kan ter plaatse bewijzen van leeftijd genereren, zonder de oorspronkelijke uitgevende instelling of een andere derde partij in kennis te stellen van zijn leeftijdskenmerken;
de gebruiker kan via een online dienst bewijs van leeftijd genereren dat kan worden gebruikt zonder enige toegang tot zijn persoonsgegevens.

Vertrouwelijkheid van leeftijdsverificatiesystemen als geheel:

het systeem is gebaseerd op nulkenisbewijs;
het systeem is gebaseerd op versleutelingstechnieken met de meest complexe aanvalswaerstandseigenschappen, zelfs in de toekomst.

DERDE DEEL: ALTERNATIEVE OPLOSSINGEN VOOR BEWIJS VAN LEEFTIJD GEACCEPTEERD OP TIJDELIJKE BASIS

Overeenkomstig artikel 10 van wet nr. 2004-575 van 21 juni 2004 inzake het vertrouwen in de digitale economie dienen de diensten waarop de bepalingen van toepassing zijn, binnen drie maanden na de bekendmaking ervan een leeftijdscontrolesysteem in te voeren dat voldoet aan de technische kenmerken van dit kader. Echter, na afloop van deze 3 maanden, voor een overgangperiode van 3 maanden vanaf de publicatie van dit kader, ontworpen om de diensten die eronder vallen, in staat te stellen een oplossing voor leeftijdsverificatie te

identificeren en implementeren, die voldoet aan alle criteria vastgesteld in het eerste en tweede deel, waarbij oplossingen die gebruik maken van bankpassen geïmplementeerd worden, die geacht worden te voldoen aan de technische kenmerken van het kader, onderverminderd de volgende voorwaarden.

Een oplossing die gebruikmaakt van een bankpas, zou een initiële methode zijn om bepaalde minderjarigen uit te filteren. Deze tijdelijke oplossing wordt gebaseerd op een infrastructuur die al is ingezet en kan worden gemobiliseerd.

Mits aan de onderstaande vereisten wordt voldaan, zou deze oplossing in eerste instantie in staat zijn om de jongste minderjarigen te beschermen. Filtering dient plaats te vinden door middel van sterke authenticatie (d.w.z. twee-factor-authenticatie). Het kan bijvoorbeeld worden gedaan via alleen sterke authenticatie (zonder betaling), of via een betaling (inclusief een bedrag van nul euro) in combinatie met sterke authenticatie.

Deze verificatiesystemen:

mogen niet rechtstreeks worden geïmplementeerd door de gerichte diensten die pornografische inhoud uitzenden, maar door derden die onafhankelijk zijn van de dienst; dienen de beveiliging van de verificatie te waarborgen om de risico's van phishing die eraan verbonden zijn, te voorkomen. Het is daarom belangrijk ervoor te zorgen dat betalingsinformatie op vertrouwde sites wordt ingevoerd. In dit verband zou het raadzaam zijn voor de gerichte diensten die pornografische inhoud uitzenden en aanbieders van oplossingen om een gecoördineerde campagne te starten om het bewustzijn van phishingrisico's te vergroten, met name rekening houdend met deze nieuwe praktijk; zijn op zijn minst in staat het bestaan en de geldigheid van de kaart te controleren, hetgeen een eenvoudige verificatie van de consistentie van het kaartnummer uitsluit; implementeren de sterke verificatie als bedoeld in de Europese Richtlijn (EU) 2015/2366 betreffende betalingsdiensten (bekend als "PSD2"), bijvoorbeeld door te vertrouwen op het 3D veilige protocol in de tweede versie die van kracht is, om ervoor te zorgen dat de servicegebruiker de kaarthouder is door middel van tweefactorauthenticatie.

VIERDE DEEL: AUDIT EN EVALUATIE VAN LEEFTIJDVERIFICATIEOPLOSSINGEN

De SREN-wet bepaalt dat "De regelgevende instantie voor audiovisuele en digitale communicatie uitgevers en dienstverleners kan verplichten [...] om een audit uit te voeren van de leeftijdsverificatiesystemen die zij implementeren om te bevestigen dat deze systemen voldoen aan de in het kader vastgestelde technische vereisten. Het kader specificeert de procedures voor het uitvoeren en bekendmaken van deze audit, die wordt toevertrouwd aan een onafhankelijk orgaan met bewezen ervaring."

Het doel van de volgende artikelen is een verduidelijking te bieden van de belangrijkste beginselen die als leidraad kunnen dienen voor het feit dat de gerichte diensten die pornografische inhoud uitzenden, verplicht zijn om een dergelijke audit uit te voeren.

Evaluatie van de onder reële omstandigheden ingevoerde systemen

Om een hoog beschermingsniveau voor minderjarigen te waarborgen, evalueert Arcom de technische oplossingen voor leeftijdsverificatie van geval tot geval, zodra ze door de uitgevers zijn geïmplementeerd, d.w.z. in concreto. Aangezien bepaalde oplossingen kunnen

worden geconfigureerd door de gerichte diensten die pornografische inhoud uitzenden zelf, is het noodzakelijk een beoordeling uit te voeren onder feitelijke bedrijfsomstandigheden. Gerichte diensten die pornografische inhoud uitzenden, dienen ervoor te zorgen dat de ingevoerde oplossingen systematisch kunnen voldoen aan de vereisten van het kader door, in voorkomend geval, hun werkingsbeginselen en -parameters aan te passen.

Foutpercentages, omzeiling en risico van aanvallen

De technische audit richt zich in het algemeen op het beoordelen van de vraag of de leeftijdsverificatieoplossing voldoet aan de wet en aan dit kader in zijn geheel. In dit verband wordt in het bijzonder het volgende beoordeeld:

het vermogen van de technische oplossing om minderjarige gebruikers te onderscheiden; het ontbreken van discriminerende vooroordelen;
- de weerstand tegen mogelijke omzeilingspraktijken (zoals deepfakes) en de risico's van een aanval (17).

Onafhankelijkheid van de aanbieder van de audit

Om de geloofwaardigheid van de audit niet te ondermijnen, dient de auditor over bewezen deskundigheid en ervaring te beschikken en onafhankelijk te zijn van zowel bedrijven die oplossingen voor leeftijdsverificatie aanbieden als de gerichte diensten die pornografische inhoud uitzenden, die gebruikmaken van de genoemde technische oplossing(en).

Arcom kan in een latere versie van dit kader aangeven onder welke voorwaarden audits dienen te worden uitgevoerd en ter beschikking van het publiek dienen te worden gesteld. In afwachting van verdere verduidelijking van ARCOM worden bedrijven aangemoedigd om technische audits uit te voeren van hun leeftijdsverificatiesystemen, in eerste instantie binnen 6 maanden na publicatie van dit kader en vervolgens ten minste elk jaar.

Gerichte diensten die pornografische inhoud uitzenden, worden ook aangemoedigd om hun auditverslag te publiceren op een gemakkelijk toegankelijke pagina van hun online interface en in een gemakkelijk te begrijpen indeling omwille van de transparantie, met name ten aanzien van de gebruikers.

- (1) Arcom, Bezoeken van sites voor “volwassen” door minderjarigen (op basis van door Médiamétrie verstrekte gegevens) gepubliceerd op 25 mei 2023;
- (2) Mr. Arzano, C. Rozier, Alice au pays du porno (Alice in Pornoland): Ados: leurs nouveaux imaginaires sexuels (Tieners: hun nieuwe seksuele verbeelding) Ramsay, 2005.
- (3) Zie: <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Quelles-solutions-pour-protoger-votre-enfant-des-images-a-caractere-pornographique-sur-internet>; en B. Smaniotto (Onderzoeker in psychopathologie en klinische psychologie), "Pornografie: welke impact op de seksualiteit van adolescenten? ", The Conversation, 28 augustus 2023: <https://theconversation.com/pornographie-quels-impacts-sur-la-sexualite-adolescente-207142>.
- (4) Hof van Cassatie, Kamer voor Strafzaken, 23 februari 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, Beraadslaging nr. 2021-069 van 3 juni 2021 betreffende een advies over een ontwerpbesluit betreffende uitvoeringsvoorschriften inzake maatregelen om minderjarigen te beschermen tegen toegang tot sites die pornografische inhoud uitzenden (zie: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044183781>).
- (7) Zie: <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne>
- (8) Zie:
- (9) Zie: <https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee>
- (10) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
- (11) Zie het persbericht van CNIL van 21 februari 2023: <https://www.cnil.fr/fr/controle-de-lage-pour-lacces-aux-sites-pornographiques>
- (12) CSA, Advies nr. 2021-11 van 23 juni 2021 over het ontwerpbesluit betreffende uitvoeringsvoorschriften inzake maatregelen om minderjarigen te beschermen tegen toegang tot sites die pornografische inhoud uitzenden,
- (13) Beperkt tot volwassenen”.
- (14) De kopteksten zijn gegevens die door de server van de website naar de browser van de gebruiker worden teruggestuurd op het moment van een verzoek.
- (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) De beoordeling van het risico op een aanval op een oplossing voor leeftijdsverificatie is om te bepalen of het systeem waarschijnlijk zal worden misbruikt voor frauduleuze doeleinden.

Gedaan op 9 oktober 2024.

Voor de regelgevende instantie voor audiovisuele en digitale communicatie:

De voorzitter,

R.-O. Maistre