

# **Beratung Nr. 2024-20 vom 9. Oktober 2024 über den Rahmen zur Festlegung der technischen Mindestanforderungen an Altersverifizierungssysteme für den Zugang zu bestimmten öffentlichen Online-Kommunikationsdiensten und Video-Sharing-Plattformen, die pornografische Inhalte der Öffentlichkeit zugänglich machen**

NOR: RCAC2428286X

JORF Nr. 0251 vom 22. Oktober 2024

Text Nr. 50

- Anhang

Die Regulierungsbehörde für Audiovisuelle und Digitale Kommunikation  
Gestützt auf die Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft;  
gestützt auf das Gesetz Nr. 2004-575 vom 21. Juni 2004 über das Vertrauen in die digitale Wirtschaft in der geänderten Fassung, insbesondere auf die Artikel 10 und 10-2,  
gestützt auf die der Europäischen Kommission am 15. April 2024 übermittelte Notifizierung Nr. 2024/0208/FR und ihre Bemerkungen vom 15. Juli 2024;  
gestützt auf die Beratung Nr. 2024-067 der Commission nationale de l'informatique et des libertés (französische Datenschutzbehörde) vom 26. September 2024, die eine Stellungnahme zu einem Entwurf des Rahmens der Regulierungsbehörde für audiovisuelle und digitale Kommunikation über Altersüberprüfungssysteme für den Zugang zu bestimmten Diensten, die den Zugang zu pornografischen Inhalten ermöglichen, abgibt;  
unter Hinweis auf die Bemerkungen, die im Rahmen der öffentlichen Konsultation vom 11. April bis 11. Mai 2024 vorgebracht wurden,

Nach eingehender Analyse,  
wird hiermit Folgendes beschlossen:

## **Artikel 1**

Der im Anhang zu diesem Beschluss dargelegte Rahmen wird angenommen.

## **Artikel 2**

Diese Beratung wird im Amtsblatt der Französischen Republik veröffentlicht.

## **Anhang**

## ANHANG

### RAHMEN ZUR FESTLEGUNG DER TECHNISCHEN MINDESTANFORDERUNGEN AN ALTERSVERIFIZIERUNGSSYSTEME FÜR DEN ZUGANG ZU BESTIMMTEN ÖFFENTLICHEN ONLINE-KOMMUNIKATIONSDIENSTEN UND VIDEO-SHARING-PLATTFORMEN, DIE PORNOGRAFISCHE INHALTE DER ÖFFENTLICHKEIT ZUGÄNGLICH MACHEN

#### Inhalt

##### Einleitung

Die Verantwortung von gezielten Diensten, die pornografische Inhalte ausstrahlen

Die Entwicklung der Rolle von ARCOM im Zusammenhang mit dem Gesetz zur Sicherung und Regulierung des digitalen Raums

Die bereits begonnene Arbeit an der Verifizierung des Alters

Präsentation des Rahmens

Unterstützung des Sektors bei der Umsetzung von Altersverifizierungslösungen

Aktualisierung des Rahmens und Stand der Technik

Struktur des Rahmens und Zeitplan für die Umsetzung

Erster Teil: Allgemeine Überlegungen zur Zuverlässigkeit von Altersverifizierungssystemen

Zweiter Abschnitt: Schutz der Privatsphäre

Grundsätze des Schutzes der Privatsphäre

Implementierung eines datenschutzfreundlichen Altersverifizierungssystems standardmäßig und durch Voreinstellungen

Mindestanforderungen an alle Altersverifizierungssysteme

1. Unabhängigkeit des Anbieters des Altersverifizierungssystems in Bezug auf gezielte Dienste, die pornografische Inhalte ausstrahlen

2. Vertraulichkeit gegenüber gezielten Diensten, die pornografische Inhalte ausstrahlen

3. Vertraulichkeit gegenüber Anbietern von Altersnachweisen

4. Vertraulichkeit gegenüber anderen Dritten, die am Altersverifizierungsverfahren beteiligt sind

5. Garantien für die Rechte und Freiheiten von Einzelpersonen durch Altersüberprüfer

Besondere Anforderungen an die Systeme zum Schutz der Privatsphäre unter Beachtung des Grundsatzes der „doppelten Anonymität“

6. Verbesserte Vertraulichkeit gegenüber gezielten Diensten, die pornografische Inhalte ausstrahlen

7. Verbesserte Vertraulichkeit gegenüber Emittenten von Altersattributen

8. Verbesserte Vertraulichkeit gegenüber anderen Dritten, die am

Altersverifizierungsverfahren beteiligt sind

9. Verfügbarkeit und Abdeckung der Bevölkerung

Information der Nutzer über das Datenschutzniveau im Zusammenhang mit Altersverifizierungssystemen

10. Explizite Anzeige des Schutzniveaus des Datenschutzes der Nutzer

Wünschenswerte Ziele und bewährte Verfahren

Dritter Abschnitt: Abwertende, beweisgenerierende Lösungen, die vorübergehend akzeptiert werden

Vierter Abschnitt: Prüfung und Bewertung von Altersverifizierungslösungen

Bewertung der unter realen Bedingungen eingerichteten Systeme

Fehlerquoten, Umgehung und Angriffsrisiken

Unabhängigkeit des Prüfungsanbieters

## Einleitung

### Die Verantwortung von gezielten Diensten, die pornografische Inhalte ausstrahlen

1. Mit der Demokratisierung mobiler Geräte, die Kindern den Zugang zum Internet ermöglichen, wächst die Zahl der Minderjährigen, die pornografischen Inhalten im Internet ausgesetzt sind, schnell.

Laut einer Studie der Regulierungsbehörde für audiovisuelle und digitale Kommunikation (Arcom) auf der Grundlage von Daten von Médiamétrie besuchen 2,3 Millionen Minderjährige jeden Monat pornografische Websites, wobei diese Zahl in den letzten Jahren rapide zugenommen hat und mit der Demokratisierung mobiler Geräte unter Kindern zusammenhängt. Der Anteil der Minderjährigen, die „Erwachsenenseiten“ besuchen, ist in fünf Jahren um 9 Punkte gestiegen, von 19 % Ende 2017 auf 28 % Ende 2022. Jeden Monat im Jahr 2022 besuchten mehr als die Hälfte der Jungen im Alter von 12 Jahren und älter solche Websites, bei den Jungen im Alter von 16 und 17 Jahren waren es zwei Drittel. Im Durchschnitt sind 12 % der Besucher von Websites für Erwachsene minderjährig (1). Seit den frühen 2000er Jahren (2) zeigen Untersuchungen zu den Folgen einer frühzeitigen Exposition gegenüber Pornografie, dass der Kontakt der Jüngsten mit pornografischen Inhalten schwerwiegende Folgen für ihre geistige Entwicklung und die Vorstellung, die sie sich von Sexualität und zwischenmenschlichen Beziehungen machen, haben kann, zum Nachteil ihrer persönlichen Entwicklung und einer größeren Gleichheit in den Beziehungen zwischen den Geschlechtern. (3)

2. Seit dem 1. März 1994 ist es gemäß Artikel 227-24 des Strafgesetzbuches, das durch das Gesetz Nr. 92-684 vom 22. Juli 1992 eingeführt wurde, verboten, Minderjährige pornografischen Inhalten auszusetzen.

Der Wortlaut dieses Artikels wurde geändert, um nicht nur dessen Anwendungsbereich zu präzisieren, sondern auch, wie er zu beurteilen ist, wenn eine Straftat im Internet aufgezeichnet wird. Im Einklang mit der ständigen Rechtsprechung sieht Artikel 227-24 seit 2020 vor, dass eine bloße Alterserklärung nicht ausreicht, um die Volljährigkeit nachzuweisen (4). Derzeit gilt folgender Wortlaut:

, Die Herstellung, die Beförderung, die Verbreitung auf jeglichem Wege und ungeachtet des Mediums einer Nachricht, die gewalttätig, terroristisch, pornografisch ist, einschließlich pornografischer Bilder, die ein oder mehrere Tiere zeigen, oder die geeignet ist, die Menschenwürde ernsthaft zu verletzen oder Minderjährige dazu zu bewegen, an Spielen teilzunehmen, die sie physisch gefährden, oder der Handel mit einer solchen Nachricht, wird mit drei Jahren Freiheitsstrafe und einer Geldstrafe von 75 000 EUR bestraft, wenn die Nachricht von einem Minderjährigen gesehen oder wahrgenommen werden kann.

, Werden die in diesem Artikel vorgesehenen Straftaten durch Druck- oder audiovisuelle Medien oder durch öffentliche Online-Kommunikation begangen, so sind hinsichtlich der Ermittlung der Verantwortlichen die besonderen Bestimmungen der für diese Bereiche geltenden Gesetze anzuwenden.

, Die in diesem Artikel vorgesehenen Straftatbestände liegen auch dann vor, wenn der Zugang eines Minderjährigen zu den in Absatz 1 angeführten Nachrichten auf einer bloßen Erklärung des Minderjährigen beruht, mindestens 18 Jahre alt zu sein.

Der Gesetzgeber hat mit dem Gesetz Nr. 2020-936 vom 30. Juli 2020 zum Schutz der Opfer häuslicher Gewalt ein besonderes Verfahren eingeführt, an dem Arcom beteiligt ist, um die volle Wirksamkeit dieser Bestimmungen über öffentliche Online-Kommunikationsdienste, die pornografische Inhalte der Öffentlichkeit im Internet zur Verfügung stellen, zu gewährleisten.

Dieses Gesetz beauftragte den Präsidenten von Arcom daher mit dem Vorrecht, den Veröffentlicher einer Website zur Einhaltung des Strafgesetzbuches aufzufordern und, falls dieser Aufforderung nicht Folge geleistet wird, den ordentlichen Richter zu ersuchen, Internetdiensteanbieter (IAPs) zu bestellen, um den Zugang zu dieser Website zu verhindern. 3. Auf der Grundlage dieser Bestimmungen hat die Behörde 13 Aufforderungen ausgestellt. Ferner übergab sie die Angelegenheit am 8. März 2022 an den Präsidenten des Gerichts erster Instanz von Paris, um die IAPs aufzufordern, fünf dieser Dienste nach Aufforderung zu sperren. Dieses Verfahren ist zum Zeitpunkt der Veröffentlichung dieses Rahmens noch im Gange.

Die Entwicklung der Rolle von ARCOM im Zusammenhang mit dem Gesetz zur Sicherung und Regulierung des digitalen Raums

Das Gesetz Nr. 2024-449 vom 21. Mai 2024 zur Sicherung und Regulierung des digitalen Raums (SREN) sieht vor, das durch das Gesetz vom 30. Juli 2020 geschaffene System zu aktualisieren.

Art. 10 des Gesetzes Nr. 2004-575 vom 21. Juni 2004 über das Vertrauen in die digitale Wirtschaft (LCEN), sieht vor: ARCOM „errichtet und veröffentlicht [...], nach Rücksprache mit der französischen Datenschutzbehörde, einen Rahmen für die Festlegung technischer Mindestanforderungen für Altersverifizierungssysteme. Diese Anforderungen betreffen die Zuverlässigkeit der Altersverifizierung der Benutzer und die Achtung ihrer Privatsphäre.“ Der Anwendungsbereich des Systems betrifft „pornografische Inhalte, die von einem Veröffentlicher von Online-Kommunikationsdiensten unter seiner redaktionellen Verantwortung oder von einem Video-Sharing-Plattformdienst im Sinne von Artikel 2 des Gesetzes Nr. 86-1067 vom 30. September 1986 über die Kommunikationsfreiheit zur Verfügung gestellt werden“ (nachfolgend „gezielte Dienste, die pornografische Inhalte ausstrahlen“ oder „die gezielten Dienste“). ARCOM kann gegebenenfalls nach Einholung der Stellungnahme des Präsidenten der CNIL einen dieser Dienste förmlich auffordern, diesem Rahmen nachzukommen und, falls die Zuwiderhandlung fortbesteht, nach Einholung der Stellungnahme der CNIL eine finanzielle Sanktion gegen ihn nach dem Verfahren des Artikels 42-7 des Gesetzes Nr. 86-1067 vom 30. September 1986 verhängen.

Die neuen Befugnisse, die ARCOM durch das SREN-Gesetz übertragen wurden, würden die Befugnisse ergänzen, die sonst dem Richter übertragen wurden. Dieser kann auf Grundlage von beispielsweise Artikel 6-3 des LCEN direkt aufgefordert werden, eine Website zu sperren, die nicht den Bestimmungen des Artikels 227-24 des Strafgesetzbuches entspricht. Darüber hinaus ist der Schutz Minderjähriger vor dem Zugang zu pornografischen Inhalten Teil eines allgemeineren Rahmens für den Schutz von Kindern, insbesondere des Übereinkommens der Vereinten Nationen über die Rechte des Kindes vom 20. November 1989 und seiner Allgemeinen Bemerkung Nr. 25 von 2021 zu den Rechten des Kindes in Bezug auf das digitale Umfeld (5) sowie von Artikel 24 der Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000, wonach „das Wohl des Kindes eine vorrangige Erwägung“ sein muss.

Die bereits begonnene Arbeit an der Verifizierung des Alters

Dieses Dokument ist Teil der in den letzten Jahren von der CNIL über Altersverifizierungslösungen durchgeführten Arbeiten, um den Schutz von Minderjährigen und die Achtung der Privatsphäre in Einklang zu bringen.

Die CNIL hat erstmals im Juni 2021 eine Stellungnahme zum Entwurf eines Dekrets zur Umsetzung des Gesetzes von 2020 über Durchführungsbestimmungen zum Schutz Minderjähriger vor dem Zugang zu öffentlich-rechtlichen Online-Kommunikationsdiensten, die pornografische Inhalte verbreiten (6). Um zu verhindern, dass die sexuelle Orientierung der Menschen – real oder vermutet – aus dem betrachteten Inhalt abgeleitet und direkt mit ihrer Identität verknüpft wird, empfahl die CNIL bereits in dieser Stellungnahme, vertrauenswürdige Dritte einzusetzen, und formulierte mehrere Empfehlungen (7), zu denen auch ein Abschnitt zur Altersverifizierung gehörte. Diese Veröffentlichungen wurden durch eine im Juli 2022 veröffentlichte Mitteilung mit dem Titel „Online-Altersverifizierung: ein Gleichgewicht zwischen dem Schutz von Minderjährigen und der Achtung der Privatsphäre“ (8) und die Einführung eines Demonstrators eines Altersverifizierungsmechanismus, der die Privatsphäre der Nutzer respektiert (9), in Zusammenarbeit mit PEReN und Herrn Olivier Blazy, Professor der École Polytechnique.

Die CNIL hatte bereits Gelegenheit, daran zu erinnern, dass „Im Gegensatz zu dem, was manchmal gesagt wird, die DSGVO (10) nicht mit der gesetzlich vorgesehenen Alterskontrolle für den Zugang zu pornografischen Websites, unvereinbar ist.“ (11)

Wie die CNIL gab auch ARCOM eine Stellungnahme zum Entwurf eines Dekrets zur Umsetzung von Artikel 23 des Gesetzes vom 30. Juli 2020 ab (12).

In diesem Zusammenhang haben Arcom und CNIL, mit Unterstützung von PEReN, einen gemeinsamen technischen Austausch mit Akteuren der Altersverifizierung Anfang 2023 begonnen. Diese Diskussionen wurden bereichert durch das Feedback, das Arcom von einigen ihrer ausländischen Partner erhalten hat, die auch mit den Herausforderungen konfrontiert sind, Minderjährige und Privatsphäre bei der Kontrolle des Zugangs zu pornografischen Inhalten zu schützen.

Dieser Rahmen wurde im Anschluss an eine öffentliche Konsultation, die vom 11. April bis zum 13. Mai lief, und seine Notifizierung an die Europäische Kommission am 15. April gemäß der Richtlinie 2015/1535 vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft und der Beratung Nr. 2024-067 der CNIL vom 26. September 2024 mit einer Stellungnahme zu dem Entwurf des Rahmens angenommen.

## Präsentation des Rahmens

### Unterstützung des Sektors bei der Umsetzung von Altersverifizierungslösungen

Der Rahmen gibt entsprechend den gesetzlichen Vorgaben vor, welche technischen Anforderungen zu erfüllen sind.

Der Zweck dieses Rahmens besteht nicht darin, technische Lösungen zu zertifizieren.

Die gezielten Dienste, die pornografische Inhalte ausstrahlen, können weiterhin ihre eigenen Lösungen zum Schutz von Minderjährigen wählen, sofern sie die technischen Anforderungen des Rahmens erfüllen.

Das Fehlen eines Altersverifizierungssystems sowie Altersverifizierungssysteme, die eine geringere Zuverlässigkeit oder einen geringeren Schutz der Privatsphäre bieten als in diesem Rahmen gefordert, sind nicht zulässig.

## Aktualisierung des Rahmens und Stand der Technik

Der Rahmen kann überprüft und aktualisiert werden, um dem Stand der Technik Rechnung zu tragen. Das SREN-Gesetz schreibt in diesem Zusammenhang vor, dass „der Rahmen wird erforderlichenfalls unter denselben Bedingungen aktualisiert.“

Es ist in der Tat wünschenswert, dass der Sektor Altersverifizierungslösungen annimmt, die dem Stand der Technik und den europäischen und internationalen Normen entsprechen (insbesondere etwaige kurzfristig entstehende europäische Normen) und mit den Branchenpraktiken, insbesondere in Bezug auf bestehende technische Protokolle, vereinbar sind.

In diesem Sinne haben die französischen Behörden auf ein Auskunftsersuchen der Europäischen Kommission im Rahmen des in der Richtlinie 2015/1535 vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (kodifizierter Text) vorgesehenen Notifizierungsverfahrens ausgeführt, dass:

, Für die Zukunft verpflichten sie sich, ihren internen Rechtsrahmen ganz oder teilweise zu überarbeiten, wenn eine hinreichend genaue Rechtsgrundlage auf EU-Ebene es ermöglicht, allen oder einigen der vom Zugang zu pornografischen Inhalten betroffenen Plattformen ein wirksames Altersverifizierungssystem vorzuschreiben.

, Unter diesen Umständen sehen sie den [Rahmen] als Übergangslösung an, bis eine wirksame europäische Lösung gefunden ist.“

## Struktur des Rahmens und Zeitplan für die Umsetzung

Der erste Teil des Rahmens betrifft allgemeine Überlegungen zur Zuverlässigkeit gesetzlicher Altersverifizierungssysteme. Neben der Notwendigkeit, den Schutz Minderjähriger standardmäßig zu gewährleisten, d. h. auch vor dem Zugriff auf den Dienst, ist es notwendig, an die Bedingungen für die Wirksamkeit von Online-Altersverifizierungssystemen zu erinnern und gleichzeitig deren Umgehung zu verhindern. Der zweite Teil befasst sich speziell mit dem Schutz der Privatsphäre durch Altersverifizierungssysteme, die eingesetzt werden, um den Zugang zu pornografischen Inhalten zu kontrollieren. Websites können Altersverifizierungssysteme mit unterschiedlichem Datenschutzniveau anbieten, vorbehaltlich der Unterrichtung der Nutzer über das mit jedem System verbundene Niveau.

In diesem Zusammenhang werden mit dem Rahmen Mindestziele für alle Altersverifizierungssysteme sowie verstärkte spezifische Ziele für die datenschutzfreundlichsten Systeme festgelegt, die als „doppelte Anonymität“ bezeichnet werden. Den Nutzern muss mindestens ein Altersverifizierungssystem angeboten werden, das den Datenschutzstandards der doppelten Anonymität entspricht.

Dieser zweite Teil beinhaltet auch bewährte Verfahren im Bereich des Datenschutzes, die als wünschenswert erachtet werden.

Darüber hinaus werden die gezielten Dienste, die pornografische Inhalte ausstrahlen, in der Lage sein, auf vorübergehender Basis Lösungen zur Generierung von Altersnachweisen auf Basis der Bereitstellung einer Bankkarte einzusetzen, abweichend von den Bedingungen des ersten und zweiten Teils, jedoch unter strikter Einhaltung der bestimmten kumulativen Bedingungen im dritten Teil dieses Dokuments.

Schließlich legt der vierte und letzte Teil die wichtigsten Grundsätze fest, an denen sich die Dienste, die für die Ausstrahlung pornografischer Inhalte bestimmt sind, orientieren können, wenn sie eine Prüfung ihrer Altersverifizierungssysteme durchführen müssen. Insbesondere

werden der Verwendungszweck bei solchen Prüfungen, die Bedingungen, unter denen sie durchgeführt werden und die Anforderungen anwendbar auf Drittprüfer spezifiziert.

## **ERSTER TEIL: ALLGEMEINE ÜBERLEGUNGEN ZUR ZUVERLÄSSIGKEIT VON ALTERSVERIFIZIERUNGSSYSTEMEN**

Zweck dieses Rahmens ist es, standardmäßig den Schutz Minderjähriger zu gewährleisten, sobald die erste Seite eines Online-Kommunikationsdienstes, der die Ausstrahlung pornografischer Inhalte ermöglicht, angezeigt wird.

Der Schutz von Minderjährigen besteht nämlich darin, zu verhindern, dass sie pornografischen Inhalten ausgesetzt werden, sobald sie auf öffentliche Online-Kommunikationsdienste zugreifen, die solche Inhalte zur Verfügung stellen.

In diesem Zusammenhang sieht Artikel 1 des SREN-Gesetzes explizit vor, dass gezielte Dienste, die pornografische Inhalte ausstrahlen, verpflichtet sind, einen Bildschirm anzuzeigen, der keine pornografischen Inhalte enthält, „bis das Alter des Benutzers verifiziert wurde“.

Darüber hinaus müssen die gezielten Dienste, die pornografische Inhalte ausstrahlen, gemäß dem SREN-Gesetz sicherstellen, dass kein Benutzer auf pornografische Inhalte zugreift, bis er seine Volljährigkeit bewiesen hat.

Dieser Schutz von Minderjährigen kann standardmäßig gewährleistet werden, z. B. durch vollständige Ausblendung der Startseite des Dienstes. Herausgeber können außerdem den pornografischen Charakter ihres Dienstes melden. Um dies zu tun, können sie sich auf einen Selbsterklärungsmechanismus wie das RTA-Label (13) stützen, der auf jeder Seite ihrer Websites eingerichtet ist, sodass Systeme zur elterlichen Kontrolle das Mindestalter ermitteln können, das für den Zugriff auf die Inhalte auf der Website erforderlich ist, über Antwortheader (oder „headers“ [14]).

Um dem Gesetz zu entsprechen, müssen die Altersverifizierungssysteme (in diesem Fall Volljährigkeit) der betroffenen Dienste, die pornografische Inhalte ausstrahlen, in der Lage sein, zwischen minderjährigen und volljährigen Benutzern zu unterscheiden. Mit der Verbesserung der Techniken und dem Inverkehrbringen neuer Altersverifizierungssysteme werden sich voraussichtlich Lösungen ergeben, auch wenn sich kurzfristig europäische Standards herausbilden.

Beruhet die technische Lösung der betroffenen Dienste, die pornografische Inhalte ausstrahlen, auf einer Schätzung des Alters des Benutzers, erfordert die Einhaltung des Gesetzes, dass sie so konfiguriert sein muss, dass die Gefahr ausgeschlossen ist, dass ein minderjähriger Benutzer für einen Erwachsenen gehalten wird („Falschmeldungen“). Um dem Gesetz zu entsprechen, müssen sich betroffene Dienste, die pornografische Inhalte ausstrahlen, nach besten Kräften bemühen, im Einklang mit den hohen Standards der Branche in Bezug auf professionelle Sorgfalt, die Möglichkeiten der Umgehung der technischen Lösungen, die sie eingeführt haben, einzuschränken. Um das Betrugsrisiko zu begrenzen, sollten Altersverifizierungssysteme keine Weitergabe des Altersnachweises an andere Personen ermöglichen. Daher muss das System angesichts der Risiken von Angriffen robust sein, wie z. B. Deepfakes, Spoofing usw.

Beispielsweise in Bezug auf Lösungen, die auf einer Altersschätzung durch Analyse von Gesichtsmerkmalen basieren, müssen die gezielten Dienste, die pornografische Inhalte ausstrahlen, sicherstellen, dass die Lösungen einen Mechanismus zur Anerkennung lebender Personen umfassen, dessen Wirksamkeit dem Stand der Technik entspricht. Die Erkennung erfolgt anhand eines Bildes von ausreichender Qualität und schließt jegliche Abzweigung aus, die von Minderjährigen verwendet werden kann, um sich künstlich als Erwachsener

auszugeben, insbesondere durch die Verwendung von Fotos, Videoaufnahmen oder Masken. Was schließlich die technischen Lösungen zur Generierung eines Altersnachweises auf Grundlage der Vorlage eines physischen Ausweisdokuments betrifft, wird erwartet, dass die gezielten Dienste, die pornografische Inhalte ausstrahlen, sicherstellen, dass die von ihnen eingesetzten technischen Lösungen die Überprüfung folgender Punkte ermöglichen: (i) dass das Dokument echt ist und dass es sich nicht um eine bloße Kopie handelt; (ii) dass der Benutzer der Inhaber des ausgefüllten Identitätsdokuments ist. Diese Verifizierung kann insbesondere durch eine Gesichtsmerkmalerkennung mit einem Lebenserkennungsmechanismus unter den oben angegebenen Bedingungen durchgeführt werden.

Um zu verhindern, dass Minderjährige pornografischen Inhalten im Internet ausgesetzt werden, ist vorgesehen, dass bei jeder Nutzung eines Dienstes eine Altersverifizierung durchgeführt wird. Somit muss die Unterbrechung dieser Abfrage eine erneute Altersverifizierung auslösen, wenn der Benutzer wieder auf pornografische Inhalte zugreifen möchte. Dies lässt unberührt die Möglichkeit für den Benutzer, Altersnachweise zu verwenden, die er selbst erneut nutzen oder neu generieren kann, sofern ein zweiter Authentifizierungsfaktor vorliegt. Dies kann erfolgen, indem die Verwendung des wiederverwendbaren Nachweises mit dem Endgerät der betroffenen Person verknüpft wird, wie es bei digitalen Brieftaschen der Fall ist.

Darüber hinaus darf das Verifizierungssystem nicht zulassen, dass dieser Nachweis mit einer anderen Person oder einem anderen Dienst geteilt wird. Im Falle eines Endgeräts, das zwischen einem Erwachsenen und einem Minderjährigen geteilt wird, ist es wichtig, zu verhindern, dass die Gültigkeitsdauer der Altersverifizierung den Zugang zu pornografischen Inhalten ohne weitere Verifizierung ermöglicht. Es kann davon ausgegangen werden, dass die Gültigkeit einer Altersverifizierung daher unterbrochen werden muss, wenn der Benutzer den Dienst verlässt, d. h. wenn die Sitzung endet, wenn der Benutzer den Browser verlässt oder wenn das Betriebssystem in den Standby-Modus wechselt und in jedem Fall nach einer Stunde Inaktivität.

Um zu verhindern, dass Minderjährige durch die Wiederverwendung von Benutzerkonten auf pornografische Inhalte zugreifen, ist davon auszugehen, dass in einem Benutzerkonto des gezielten Dienstes kein Altersnachweis gespeichert werden kann. Aus dem Gesetz ergibt sich in jedem Fall, dass die Altersverifizierungspflicht bei jedem Zugriff, mit oder ohne Benutzerkonto, besteht.

Um den Jugendschutz und die Einhaltung der Gesetze zu gewährleisten, wird erwartet, dass die Lösungen der gezielten Dienste, die pornografische Inhalte ausstrahlen, für alle Bevölkerungsgruppen wirksam sind und daher nicht zur Folge haben dürfen, dass bestimmte Bevölkerungsgruppen diskriminiert werden, insbesondere aus den in Artikel 21 der Charta der Grundrechte der Europäischen Union genannten Gründen. Daher ist die Wirksamkeit der technischen Altersverifizierungslösung unabhängig von den physikalischen Merkmalen des Benutzers gleich. Bei Systemen zur Generierung von Altersnachweisen auf Basis von maschinellem Lernen oder statistischen Modellen können Diensteanbieter beispielsweise ihre Lösung in einer Vielzahl von Datenbanken testen, um die Einhaltung dieser Anforderung sicherzustellen. Es ist wichtig, dass Alterskontrollsysteme diskriminierende Verzerrungen begrenzen, die auch zu Fehlern führen, die sowohl ihre Zuverlässigkeit als auch ihre Akzeptanz infrage stellen können.

Gezielte Dienste, die pornografische Inhalte ausstrahlen, werden aufgefordert, bei der Bewertung der Leistung ihres Altersverifizierungssystems aber auch bei allen von ihnen durchgeführten Prüfungen (siehe unten), alle diskriminierenden Vorurteile zu berücksichtigen, die auf der Grundlage der einschlägigen Diskriminierungsgründe aufgeschlüsselt sind.

## Zweiter Teil: Schutz der Privatsphäre

Mit diesem Rahmen soll auch der Schutz der Privatsphäre der Benutzer der Altersverifizierungssysteme sichergestellt werden. Diese Systeme können ein hohes Risiko für die Sicherheit personenbezogener Daten darstellen, da die Altersverifizierung der Identitätsprüfung ähnlich ist und daher die Erfassung sensibler Daten oder Identitätsdokumente erfordern kann.

Diejenigen, die an Altersverifizierungssystemen beteiligt sind, müssen daher besonders auf den Schutz der Privatsphäre ihrer Nutzer und die Sicherheit der betreffenden Informationssysteme achten, wobei die Grundsätze, für die die CNIL verantwortlich ist, insbesondere die Datenschutz-Grundverordnung (DSGVO), eingehalten werden.

### Grundsätze des Schutzes der Privatsphäre

In der Praxis müssen die Altersverifizierungssysteme als Ganzes den geltenden Rechtsvorschriften zum Schutz personenbezogener Daten und der Privatsphäre entsprechen, einschließlich der Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 5 und 25 der DSGVO).

Anbieter solcher Systeme müssen den folgenden Grundsätzen besondere Aufmerksamkeit schenken:

Genauigkeit, Verhältnismäßigkeit und Minimierung der erhobenen Daten;  
prägnante, transparente, verständliche und leicht zugängliche Nutzerinformationen;  
angemessene Aufbewahrungsfristen für Daten;  
Möglichkeit für Einzelpersonen, ihre Rechte auszuüben, nämlich das Recht auf Auskunft, das Recht auf Widerspruch, das Recht auf Berichtigung, das Recht auf Einschränkung der Verarbeitung, das Recht auf Löschung, das Recht auf Datenübertragbarkeit;  
Modernste Sicherheit für Informationssysteme, die zur Verarbeitung personenbezogener Daten verwendet werden.

### Implementierung eines datenschutzfreundlichen Altersverifizierungssystems standardmäßig und durch Voreinstellungen

Im Jahr 2022 veröffentlichte die CNIL einen datenschutzfreundlichen Altersverifizierungsmechanismus für die Übertragung eines Kennungsattributs (in diesem Fall Altersnachweis) (15), (16). Insbesondere wird durch den vorgeschlagenen Mechanismus sichergestellt, dass es zwischen den gezielten Diensten, die pornografische Inhalte ausstrahlen, die verpflichtet sind, das Alter ihrer Nutzer zu überprüfen, und Dritten, die Altersattribute vergeben, eine Trennung gibt.

Dieser Mechanismus, der seitdem als „doppelte Anonymität“ oder „doppelte Vertraulichkeit“ bekannt ist, wurde von verschiedenen öffentlichen und privaten Akteuren entwickelt und getestet, was seine technische Durchführbarkeit und seine Fähigkeit

bestätigt, den Erfordernissen des Schutzes der Privatsphäre, die mit Online-Altersverifizierungsmechanismen inhärent sind, gerecht zu werden. Er entspricht auch den allgemeinen Zielen für digitale Identitätssysteme einschließlich Attributmanagement. Dieser Mechanismus, der in diesem Dokument als „doppelte Anonymität“ bezeichnet wird, ist jedoch nicht „anonym“ im Sinne der DSGVO, garantiert jedoch ein hohes Maß an Vertraulichkeit.

Öffentliche Online-Kommunikationsdienste, die pornografische Inhalte zur Verfügung stellen, müssen ihren Nutzern mindestens ein Altersverifizierungssystem anbieten, das den Datenschutzstandards der doppelten Anonymität entspricht, wodurch sichergestellt wird, dass dieses System von einer großen Mehrheit seiner Nutzer genutzt werden kann. Diese Anforderung tritt am Ende der im dritten Teil dieses Rahmens vorgesehenen Übergangszeit in Kraft, die auf 6 Monate nach der Veröffentlichung festgelegt ist, unbeschadet der nachstehend festgelegten Mindestanforderungen. Daher müssen die Altersverifizierungssysteme bis zu diesem Zeitpunkt die nachstehenden Mindestanforderungen erfüllen, um ein akzeptables Schutzniveau für die personenbezogenen Daten ihrer Nutzer zu gewährleisten.

Die folgenden Abschnitte spezifizieren:

die Anforderungen für alle unter diesen Rahmen fallenden Altersverifizierungssysteme;  
die spezifischen Ziele für die datenschutzfreundlichsten Systeme, die als „doppelte Anonymität“ bezeichnet werden;  
die Transparenzverpflichtungen, die darauf abzielen, die Nutzer über das Niveau des Schutzes der Privatsphäre zu informieren, das mit den in den Diensten angebotenen Systemen verbunden ist;  
ebenso wie bewährte Verfahren, die als wünschenswert, aber bisher nicht erforderlich angesehen werden.

### Mindestanforderungen an alle Altersverifizierungssysteme

Für alle in diesem Rahmen erfassten Altersverifizierungssysteme gelten bestimmte Mindestanforderungen:

1. Unabhängigkeit des Anbieters des Altersverifizierungssystems in Bezug auf gezielte Dienste, die pornografische Inhalte ausstrahlen

Der Anbieter von Altersverifizierungssystemen ist rechtlich und technisch unabhängig von allen öffentlichen Online-Kommunikationsdiensten, die unter diesen Rahmen fallen, und stellt sicher, dass gezielte Dienste, die pornografische Inhalte ausstrahlen, unter keinen Umständen Zugriff auf die Daten haben, die zur Verifizierung des Alters des Benutzers verwendet werden.

2. Vertraulichkeit gegenüber gezielten Diensten, die pornografische Inhalte ausstrahlen  
Die personenbezogenen Daten, die es dem Benutzer ermöglichen, sein Alter mit einem Kommunikationsdienst zu überprüfen, der unter diesen Rahmen fällt, dürfen nicht von diesem Kommunikationsdienst verarbeitet werden.

Insbesondere darf die Implementierung von Altersverifizierungslösungen es den von diesem Rahmen erfassten Kommunikationsdiensten nicht gestatten, die Identität, das Alter, das Geburtsdatum oder andere personenbezogene Daten dieser Benutzer zu erfassen.

3. Vertraulichkeit gegenüber Anbietern von Altersnachweisen

Wenn das Altersverifizierungssystem es dem Nutzer nicht erlaubt, eine wiederverwendbare digitale Identität oder Altersnachweise zu erhalten, dürfen die personenbezogenen Daten, die der Nutzer zur Erlangung dieses Attributs zur Verfügung stellt, nicht vom Anbieter für die Generierung von Altersnachweisen aufbewahrt werden.

Darüber hinaus sollte diese Art von System nicht die Sammlung von amtlichen Identitätsdokumenten erfordern, wenn kein wiederverwendbarer Altersnachweis erstellt wird.

Diese Anforderung gilt unbeschadet der Einhaltung gesetzlicher und regulatorischer Verpflichtungen, die ansonsten für bestimmte Anbieter von Altersnachweisen gelten.

4. Vertraulichkeit gegenüber anderen Dritten, die am Altersverifizierungsverfahren beteiligt sind

Wenn andere Dritte als Anbieter von Altersnachweisen am Altersverifizierungsverfahren beteiligt sind, z. B. für die Verwaltung von Nachweisen oder die Abrechnung des Dienstes, dürfen diese Dritten keine personenbezogenen Daten der Nutzer des Systems speichern, mit Ausnahme der Speicherung des Nachweises auf Wunsch des Nutzers.

5. Garantien für die Rechte und Freiheiten von Einzelpersonen durch Altersüberprüfer

Bei der Feststellung, ob ein Nutzer auf der Grundlage der dem öffentlichen Online-Kommunikationsdienst vorgelegten Nachweise auf ihn zugreifen kann, trifft der gezielte Dienst, der pornografische Inhalte ausstrahlt, eine automatisierte Entscheidung im Sinne von Art. 22 DSGVO. Durch die Verweigerung des Zugangs zu einem Dienst kann diese Entscheidung Rechtswirkungen auf die betroffenen Personen haben oder zumindest erhebliche Auswirkungen, die Personen in ähnlicher Weise betreffen.

Die CNIL ist der Auffassung, dass eine solche Entscheidung auf der in Artikel 22 Absatz 2.b DSGVO vorgesehenen Ausnahme beruhen kann, soweit der gezielte Dienst, der pornografische Inhalte ausstrahlt, einer Altersverifizierungspflicht nach Art. 227-24 des Strafgesetzbuches und den Bestimmungen des SREN-Gesetzes unterliegt. Artikel 22.2.b DSGVO schreibt vor, dass in den Bestimmungen zur Ermächtigung dieser automatisierten Entscheidung geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten und Schutzinteressen der betroffenen Person vorgesehen sind.

Um die Anforderungen an den Schutz der Privatsphäre zu wahren, die darauf abzielen, die Fähigkeit der Dienste zur Identifizierung von Personen zu beschränken, dürfen solche Maßnahmen nicht durch den gezielten Dienst, der pornografische Inhalte ausstrahlt, sondern durch den Anbieter der technischen Altersverifizierungslösung, unabhängig davon, ob es sich um den Anbieter von Attributen oder den Nachweisaussteller handelt, eingeführt werden. Diese Maßnahmen sollten es den Nutzern im Falle eines Fehlers ermöglichen, das Ergebnis der Analyse ihres Attributs infrage zu stellen, um einen Altersnachweis zu erhalten. Für die Ausübung dieser Rechtsbehelfe sollten diese Anbieter von Altersverifizierungslösungen den Nutzern die Möglichkeit bieten, verschiedene Attributanbieter oder je nach Lösungen unterschiedliche Aussteller von Nachweisen zu verwenden.

Der gezielte Dienst, der pornografische Inhalte ausstrahlt, ist jedoch, ebenso wie Anbieter technischer Lösungen zur Altersverifizierung, verpflichtet, den Informationspflichten der DSGVO nachzukommen, und die Benutzer über die Möglichkeit einer Beschwerde beim Anbieter der Altersverifizierungslösung zu informieren.

In jedem Fall müssen Attributanbieter auch Einzelpersonen die Möglichkeit geben, ihre Daten gemäß Art. 16 DSGVO zu berichtigen.

Besondere Anforderungen an die Systeme zum Schutz der Privatsphäre unter Beachtung des Grundsatzes der „doppelten Anonymität“

Die folgenden Ziele ergänzen die Ziele der Mindestgrundlage zur Festlegung eines datenschutzfreundlichen Standards für die Online-Altersverifizierung.

6. Verbesserte Vertraulichkeit gegenüber gezielten Diensten, die pornografische Inhalte ausstrahlen

Die in Nr. 2 genannten Anforderungen werden wie folgt ergänzt.

Ein Altersverifizierungssystem mit „doppelter Anonymität“ sollte es den von diesem Rahmen erfassten Kommunikationsdiensten nicht ermöglichen, einen Benutzer, der das System bereits genutzt hat, auf der Grundlage der im Rahmen des Altersverifizierungsverfahrens generierten Daten zu erkennen.

Die Verwendung von Altersverifizierungssystemen mit „doppelter Anonymität“ sollte es diesen Diensten nicht ermöglichen, die Quelle oder Methode zur Erlangung des Altersnachweises zu kennen oder abzuleiten, die im Altersverifizierungsverfahren eines Nutzers involviert ist.

Ein Altersverifizierungssystem mit „doppelter Anonymität“ darf es diesen Diensten nicht ermöglichen, erkennen zu können, dass zwei Volljährigkeitsnachweise aus derselben Altersnachweisquelle stammen.

7. Verbesserte Vertraulichkeit gegenüber Emittenten von Altersattributen

Die in Nr. 3 genannten Anforderungen werden so ergänzt, dass ein Altersverifizierungssystem mit „doppelter Anonymität“ es Anbietern von Altersnachweisen nicht erlauben darf, zu wissen, für welchen Dienst die Altersverifizierung durchgeführt wird.

8. Verbesserte Vertraulichkeit gegenüber anderen Dritten, die am Altersverifizierungsverfahren beteiligt sind

Die in Nr. 4 genannten Anforderungen werden durch folgende Anforderungen ergänzt: Ein Altersverifizierungssystem mit „doppelter Anonymität“ sollte es nicht zulassen, dass andere an dem Prozess beteiligte Dritte einen Nutzer erkennen, der das System bereits genutzt hat. Zum Beispiel sollte ein Dritter, der einen Altersnachweis vorlegt oder seine Gültigkeit bescheinigt, nicht in der Lage sein, zu wissen, ob er bereits den Nachweis desselben Nutzers verarbeitet hat.

9. Verfügbarkeit und Abdeckung der Bevölkerung

Die unter diesen Rahmen fallenden Kommunikationsdienste müssen sicherstellen, dass ihre Nutzer über mindestens zwei verschiedene Verfahren zur Erlangung eines Altersnachweises durch ein Altersverifizierungssystem mit „doppelter Anonymität“ verfügen. In der Praxis muss ein Diensteanbieter, der eine Lösung mit doppelter Anonymität anbietet, mindestens zwei Methoden zur Erlangung des Altersnachweises kombinieren (z. B. eine Lösung auf der Grundlage von Identitätsdokumenten und eine auf der Grundlage der Altersschätzung).

Die von diesem Rahmen abgedeckten Kommunikationsdienste müssen sicherstellen, dass ein Altersverifizierungssystem mit „doppelter Anonymität“ für mindestens 80 % der erwachsenen Bevölkerung mit Wohnsitz in Frankreich zur Verfügung steht.

Beispiele und Anwendung:

In der Praxis müssen Lösungen mit „doppelter Anonymität“ mehrere Anbieter für die Generierung von Altersnachweisen (z. B. verschiedene Internetzugangsanbieter und/oder Banken) und andere Lösungen unterschiedliche Methoden der Altersnachweisgenerierung (z. B. Analyse von Gesichtsmerkmalen und Bereitstellung von Identitätsdokumenten) bieten.

Information der Nutzer über das Datenschutzniveau im Zusammenhang mit Altersverifizierungssystemen

#### 10. Explizite Anzeige des Schutzniveaus des Datenschutzes der Nutzer

Jede Altersverifizierungslösung muss explizit mit dem Schutz der Privatsphäre in Verbindung gebracht werden, damit Lösungen, die den Standards der „doppelten Anonymität“ entsprechen, klar und lesbar dargestellt werden. In jedem Fall sollten andere Lösungen nicht verwechselt oder gefördert werden, um den Nutzer zugunsten weniger datenschutzrechtlicher Lösungen in die Irre zu führen.

Wenn ein Dritter, der am Altersverifizierungsverfahren beteiligt ist, Kenntnis von dem Dienst haben kann, für den die Altersverifizierung durchgeführt wird, muss der Nutzer klar darüber informiert werden.

In Bezug auf Altersverifizierungssysteme, die dem Grundsatz der „doppelten Anonymität“ entsprechen, muss der Nutzer klar darüber informiert werden, dass diese Lösung sicherstellt, dass der Anbieter der Altersverifizierung den Dienst, für den diese Verifizierung durchgeführt wird, nicht kennen kann.

#### Wünschenswerte Ziele und bewährte Verfahren

Die folgenden Ziele werden von Altersverifizierungssystemen für die Einhaltung dieses Rahmens noch nicht gefordert, stellen aber eine Reihe von bewährten Verfahren dar, auf die Altersverifizierungslösungen hinarbeiten sollten.

Fähigkeit für Nutzer, den Altersnachweis selbst vertraulich zu generieren:

der Nutzer kann einen Altersnachweis lokal generieren, ohne den ursprünglichen Aussteller über seine Altersattribute oder einen anderen Dritten zu informieren;

der Nutzer kann über einen Online-Dienst einen Altersnachweis generieren, der ohne Zugriff auf seine personenbezogenen Daten genutzt werden kann.

Vertraulichkeit der Systeme zur Altersverifizierung insgesamt:

das System basiert auf Null-Wissen-Beweis („zero-knowledge proof“);

das System basiert auf Verschlüsselungstechniken mit den komplexesten Angriffswiderstandseigenschaften, auch in der Zukunft.

#### **Dritter Teil: Vorübergehend akzeptierte alternative Lösungen zur Nachweisgenerierung**

Gemäß Artikel 10 des Gesetzes Nr. 2004-575 vom 21. Juni 2004 über das Vertrauen in die digitale Wirtschaft müssen die Dienste, die den Bestimmungen unterliegen, innerhalb von 3 Monaten nach ihrer Veröffentlichung ein Altersüberprüfungssystem einführen, das den technischen Merkmalen dieses Rahmens entspricht. Nach Ablauf dieser 3 Monate gilt jedoch für eine Übergangszeit von 3 Monaten ab der Veröffentlichung dieses Rahmens, der es den ihnen unterliegenden Diensten ermöglichen soll, eine Altersverifizierungslösung zu identifizieren und zu implementieren, die alle im ersten und zweiten Teil festgelegten Kriterien erfüllt, und bei dem Lösungen unter Verwendung von Bankkarten implementiert

werden, die unter den folgenden Bedingungen als den technischen Merkmalen des Rahmens entsprechend gelten.

Eine Lösung mit einer Bankkarte wäre eine erste Methode, um einen Teil der Minderjährigen herauszufiltern. Diese temporäre Lösung basiert auf einer Infrastruktur, die bereits bereitgestellt wurde und mobilisiert werden kann.

Vorbehaltlich der Einhaltung der nachstehenden Anforderungen würde diese Lösung zunächst in der Lage sein, die jüngsten Minderjährigen zu schützen. Die Filterung muss durch starke Authentifizierung (d. h. Zwei-Faktor-Authentifizierung) erfolgen. Dies kann beispielsweise entweder über eine starke Authentifizierung allein (ohne Zahlung) oder über eine Zahlung (einschließlich eines Betrags von null Euro) in Verbindung mit einer starken Authentifizierung erfolgen.

Diese Verifizierungssysteme:

dürfen nicht direkt durch die gezielten Dienste, die pornografische Inhalte ausstrahlen, eingesetzt werden, sondern durch von dem Dienst unabhängige Dritte; werden die Sicherheit der Verifizierung gewährleisten müssen, um die damit verbundenen Phishing-Risiken zu vermeiden. Es ist daher wichtig, sicherzustellen, dass Zahlungsinformationen auf vertrauenswürdigen Websites eingegeben werden. In diesem Zusammenhang wäre es ratsam, dass die gezielten Dienste, die pornografische Inhalte ausstrahlen, und Lösungsanbieter eine koordinierte Kampagne zur Sensibilisierung für Phishing-Risiken einleiten, insbesondere unter Berücksichtigung dieser neuen Praxis; müssen es ermöglichen, zumindest die Existenz und Gültigkeit der Karte zu verifizieren, was eine einfache Überprüfung der Konsistenz der Kartenummer ausschließt; setzen die starke Authentifizierung gemäß der Europäischen Richtlinie (EU) 2015/2366 über Zahlungsdienste (bekannt als „PSD2“) um, indem sie sich beispielsweise auf das 3-D-Secure-Protokoll in seiner zweiten Version in Kraft stützen, um mittels einer Zwei-Faktor-Authentifizierung sicherzustellen, dass der Nutzer des Dienstes der Karteninhaber ist.

#### **Vierter Teil: Prüfung und Bewertung von Altersverifizierungslösungen**

Das SREN-Gesetz sieht vor, dass „Die Regulierungsbehörde für Audiovisuelle und Digitale Kommunikation kann von den Veröfentlichern und Diensteanbietern verlangen, dass sie [...] eine Prüfung der von ihnen implementierten Altersverifizierungssysteme durchführen, um zu bescheinigen, dass diese Systeme die im Rahmen festgelegten technischen Anforderungen erfüllen. In dem Rahmen werden die Verfahren für die Durchführung und Veröffentlichung dieser Prüfung festgelegt, die einer unabhängigen Stelle mit nachgewiesener Erfahrung übertragen werden.“

Die folgenden Abschnitte zielen darauf ab, die wichtigsten Grundsätze zu präzisieren, die geeignet sind, die für die Durchführung einer solchen Prüfung erforderlichen Dienste für die Übertragung pornografischer Inhalte zu leiten.

Bewertung der unter realen Bedingungen eingerichteten Systeme

Um ein hohes Schutzniveau für Minderjährige zu gewährleisten, wird Arcom die technischen Altersverifizierungslösungen von Fall zu Fall bewerten, sobald sie von den Veröfentlichern implementiert wurden, d. h. in concreto. Da bestimmte Lösungen durch die

gezielten Dienste, die pornografische Inhalte selbst ausstrahlen, konfiguriert werden können, ist es notwendig, eine Bewertung unter tatsächlichen Betriebsbedingungen durchzuführen. Gezielte Dienste, die pornografische Inhalte ausstrahlen, sind verpflichtet, sicherzustellen, dass die eingesetzten Lösungen die Anforderungen des Rahmens systematisch erfüllen können, indem gegebenenfalls ihre Betriebsgrundsätze und Parameter angepasst werden.

### Fehlerquoten, Umgehung und Angriffsrisiken

Die technische Prüfung konzentriert sich darauf, im Allgemeinen zu beurteilen, ob die Altersverifizierungslösung mit dem Gesetz und diesen Rahmenbedingungen insgesamt übereinstimmt.

In diesem Zusammenhang wird insbesondere Folgendes bewertet:

die Fähigkeit der technischen Lösung, minderjährige Nutzer zu erkennen;  
das Fehlen diskriminierender Voreingenommenheit;  
Widerstand gegen mögliche Umgehungspraktiken (zum Beispiel Deepfakes) und gegen Angriffsrisiken (17).

### Unabhängigkeit des Prüfungsanbieters

Um die Glaubwürdigkeit der Prüfung nicht zu untergraben, sollte der Prüfer über nachgewiesene Sachkenntnis und Erfahrung verfügen und unabhängig von beiden Unternehmen sein, die Altersverifizierungslösungen anbieten, und den gezielten Diensten, die pornografische Inhalte ausstrahlen, die die genannte(n) technische(n) Lösung(en) verwenden.

Arcom kann in einer späteren Fassung dieses Rahmens die Bedingungen festlegen, unter denen Prüfungen durchgeführt und der Öffentlichkeit zugänglich gemacht werden müssen. Zum gegenwärtigen Zeitpunkt und in Erwartung weiterer Klärungen durch ARCOM werden Unternehmen aufgefordert, technische Prüfungen ihrer Altersverifizierungssysteme durchzuführen, zunächst innerhalb von 6 Monaten nach der Veröffentlichung dieses Rahmens und dann zumindest jedes Jahr.

Gezielte Dienste, die pornografische Inhalte ausstrahlen, werden ebenfalls ermutigt, ihren Prüfbericht auf einer leicht zugänglichen Seite ihrer Online-Schnittstelle und in einem leicht verständlichen Format aus Gründen der Transparenz zu veröffentlichen, insbesondere im Hinblick auf die Nutzer.

(1) Arcom, Besuche von „Erwachsenenseiten“ durch Minderjährige (auf der Grundlage von Daten von Médiamétrie) veröffentlicht am 25. Mai 2023:

(2) Herr Arzano, C. Rozier, Alice au pays du porno (Alice im Pornoland): Ados: leurs nouveaux imaginaires sexuels (Jugendliche: ihre neuen sexuellen Vorstellungen) Ramsay, 2005.

(3) Siehe: <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Quelles-solutions-pour-protger-votre-enfant-des-images-a-caractere-pornographique-sur-internet>; und B. Smaniotto (Forscherin in Psychopathologie und Klinische Psychologie), „Pornographie :

- quels impacts sur la sexualité adolescente ? ', The Conversation, 28. August 2023:  
<https://theconversation.com/pornographie-quels-impacts-sur-la-sexualite-adolescente-207142>.
- (4) Kassationsgerichtshof, Strafabteilung, 23. Februar 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, Beratung Nr. 2021-069 vom 3. Juni 2021 über eine Stellungnahme zu einem Entwurf eines Dekrets über Durchführungsbestimmungen für Maßnahmen zum Schutz Minderjähriger vor dem Zugang zu pornografischen Seiten (siehe: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044183781>).
- (7) Siehe: <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne>
- (8) Siehe:
- (9) Siehe: <https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee>
- (10) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr.
- (11) Siehe Pressemitteilung der CNIL vom 21. Februar 2023: <https://www.cnil.fr/fr/controle-de-lage-pour-laces-aux-sites-pornographiques>
- (12) CSA, Stellungnahme Nr. 2021-11 vom 23. Juni 2021 zu dem Entwurf eines Dekrets über Durchführungsbestimmungen für Maßnahmen zum Schutz Minderjähriger vor dem Zugang zu Websites, die pornografische Inhalte ausstrahlen,
- (13) Beschränkt auf Erwachsene“.
- (14) Die Headers sind Informationen, die der Website-Server zum Zeitpunkt einer Anfrage an den Browser des Nutzers zurückgibt.
- (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) Die Beurteilung des Risikos eines Angriffs auf eine Altersverifizierungslösung besteht darin, festzustellen, ob das System zu betrügerischen Zwecken missbraucht werden kann.

Geschehen am 9. Oktober 2024,

Für die Aufsichtsbehörde für Audiovisuelle und Digitale Kommunikation:  
Der Vorsitzende,  
R.-O. Maistre