زاویه

جشنواره خدمات دیجیتال دوستدار خانواده

وزارت ارتباطات و فناوری اطلاعات

امور بانوان و خانواده

احراز سن

روش‌ها، چالش‌های کلیدی و اصول راهبردی

احراز سن

روش‌ها، چالش‌های کلیدی و اصول راهبردی

تهیه و تدوین | گروه زاویه و امور بانوان و خانواده وزارت ارتباطات و فناوری اطلاعات

ناظران | علی زرودی و سعید رحیمی

مدیر مطالعه | امین زاده‌حسین

تاریخ تنظیم | زمستان ۱۴۰۲

تعداد کلمات | ۷۶۰۰

کلیدواژه‌ها | تناسب خدمت (محتوا) با سن، احراز سن، اینترنت ایمن، تنظیم‌گری خدمات دیجیتال، خدمات دیجیتال دوستدار خانواده

جشنواره خدمات دیجیتال دوستدار خانواده

پیشگفتار

فناوری گرچه به ظاهر زاییده نیاز آدمی است؛ اما سازوکارهای تصریح این نیاز و به ثمر رسیدن خلاقیت‌های ذهنی انسان‌ها در طول تاریخ موضوعی شایسته مطالعه و توجه است. در حوزه فناوری‌های دیجیتال، یکی از اصلی‌ترین مسیرهای خلق فناوری را می‌توان در مسیر حیات اینترنت، به عنوان زیرساخت و بستر کاربرد فناوری‌های دیجیتال، دنبال نمود.

در دوره نخست عمر اینترنت در زمان ابداع پروتکل‌های اولیه شبکه در دره سیلیکون، محرک اصلی فناوری را شاید بتوان آرمان‌های لیبرالیستی مهندسان اولیه پروژه دانست؛ اما دست کم پس از آن دوره و انتقال حکمرانی اینترنت به شرق آمریکا، می‌توان کنش‌های تنظیم‌گری ملی یا بین‌المللی را یکی از اصلی‌ترین محرک‌های فناوری‌های دیجیتال دانست.

این بدان معناست که برخلاف بسیاری که تنظیم‌گری دیجیتال را صرفاً پاسخی به ظهور فناوری‌های نو می‌دانند، تعامل کنش‌های تنظیم‌گران و خالقان فناوری، تعاملی دو سویه بوده و خواهد بود و اراده تنظیم‌گران خودبه‌خود به خلق اشکال نویی از فناوری می‌انجامد. اگر فناوری را ابزاری حاوی ارزش‌های مشخصی در حوزه فردی و اجتماعی بدانیم، قبول این تعامل دو سویه، امری بدیهی خواهد بود و فناوری به همان نسبت که واکنش سیاست‌گذاران را برای کنترل فضای عمومی دیجیتال بر می‌انگیزد، خود به اهداف سیاست‌گذاران واکنش (مثبت یا منفی) داشته و تغییر می‌کند.

تا سال‌ها احراز هویت کاربران اینترنت، مطلوب تنظیم‌گران برای اطمینان از اصالت هویت مشتریان خدمات دولتی و بانکی بود. افزایش توانمندی‌های رایانشی برای تحلیل ردپای دیجیتال افراد و نگرانی حریم خصوصی و مسائل بعدی ناشی از افشای هویت افراد نزد شرکت‌های فناور که کشورهایی با جمعیتی بسیار بیشتر از حکومت‌های ملی در دنیای دیجیتال هستند، سبب تغییر ذائقه تنظیم‌گر در مواجهه اقشار آسیب‌پذیرتر با اینترنت شد.

مفهوم احراز سن به عنوان چتری از انواع سازوکارهای تخمین و یا تشخیص سن کاربر، در نتیجه این تغییر در جهان مطرح شده است.

از سوی دیگر در کشور ما، علی‌رغم تقسیم کار معنادار حوزه حفاظت از کودکان و نوجوانان در سند صیانت از کودکان و نوجوانان در فضای مجازی ابلاغی مرکز ملی به دستگاه‌های اجرایی، حوزه تطبیق سن با خدمات در بند ۱۱-۴ این سند یکی از استثنائات این نگاشت نهادی بود که بدون دستگاه مسئول باقی مانده است.

امور بانوان و خانواده وزارت ارتباطات ضمن تشکر از جوانان دلسوز گروه پژوهشی زاویه، این مستند را ذیل «جشنواره خدمات دیجیتال دوستدار خانواده» در اختیار سیاست‌گذاران و علاقه‌مندان این بحث قرار می‌دهد، باشد که روزی در آینده نزدیک رگولاتورهای بخشی حوزه عمومی با همکاری دستگاه متبوع بتوانند به شکل‌گیری ارائه‌دهندگان خدمات احراز سن در کشور برای تجمیع در سکوهای دیجیتال اقدام نمایند و قدمی در جهت حمایت از خانواده در فضای مجازی بردارند.

با استعانت از خداوند متعال...

دکتر سیده عاطفه موسوی
مشاور وزیر در امور بانوان و خانواده
وزارت ارتباطات و فناوری اطلاعات

زاویه

نگاهی نو،
به حکمرانی فضای مجازی

www.zaviehmag.ir

فهرست مطالب

خلاصه مدیریتی ۵

مقدمه ۹

۱) روش‌های احراز سن ۱۳

۱-۱) راستی‌آزمایی (اعتبارسنجی) سن ۱۴

۱-۲) تخمین سن ۱۸

۱-۳) خود اظهاری ۲۲

۲) گزینه‌های موجود برای پیاده‌سازی روش‌های احراز سن ۲۳

۳) چالش‌های کلیدی ۲۵

۴) اصول راهبردی ۲۹

۵) ضمیمه ۱ ..... ۳۹

۶) ضمیمه ۲ ..... ۴۳

۷) معرفی مؤسسه اعتماد و ایمنی دیجیتال ۴۹

خلاصه مدیریتی

سرویس‌های دیجیتال در زمینه طراحیِ تجربه‌های متناسب‌سازی محتوا یا خدمت با سن کاربر، فعالیت می‌کنند که از جمله فعالیت‌های آن‌ها می‌توان به پیاده‌سازی روش‌های «احراز سن»[۱] به‌منظور راستی‌آزمایی یا تخمین سن کاربر اشاره کرد.

برای احراز سن رویکردهای متنوعی از جمله راستی‌آزمایی سن با استفاده از مدارک هویتی یا موافقت (تأیید) والدین، تخمین سن از طریق استنباط‌های حاصل از داده‌های کاربر یا ویژگی‌های فیزیکی وی و همچنین خوداظهاری سن توسط کاربر، وجود دارند که به صورت مفصل در گزارش توضیح داده می‌شوند.

هر یک از رویکردهای احراز سن، مزایا و معایب مختص خود را دارد. بنابراین در بخش دیگری از این گزارش، به چالش‌های حاصل از پیاده‌سازی روش‌های احراز سن پرداخته می‌شود. از جمله چالش‌های کلیدی این است که روش‌های دقیق‌تر احراز سن، به جمع‌آوری داده‌های شخصی جدید و بیشتری نیاز دارند و بنابراین ممکن است با تعهدات آن سرویس نسبت به حریم خصوصی کاربران و الزامات قانونی حفاظت از حریم خصوصی، در تعارض باشند. این روش‌ها همچنین ممکن است علیه افرادی خاص تبعیض ناعادلانه‌ای قائل شوند، نابرابری‌هایی بین کاربران ایجاد کنند و از نظر اقتصادی برای شرکت‌های کوچک‌تر مقرون‌به‌صرفه نباشند.

درمورد چالش‌ها، بِده‌بِستان[۲] وجود دارد؛ یعنی علی‌رغم اینکه انتخاب یک روش منجر به بروز چالش‌هایی می‌شود؛ اما مزایای ارزشمند و مهم‌تری نیز در پی خواهد داشت؛ لذا باید به توازن و نسبت چالش‌ها با مزایایی که حاصل می‌شود توجه داشت. بنابراین راه‌حل‌های یکسان در این زمینه وجود ندارد؛ اما سرویس‌های مختلف بر اساس عوامل مختلفی همچون «کاربران سرویس»، «نوع سرویس ارائه‌شده»،

۱. Age assurance
۲. Trade off

«محاسبه ریسک»، «انتظارات در خصوص حریم خصوصی» و «امکان‌سنجی اقتصادی»، روش‌های متفاوت احراز سن را انتخاب می‌کنند.

این گزارش که با استفاده از سند «احراز سن؛ اصول راهبردی و روال‌های مطلوب»[۱] «مؤسسه اعتماد و ایمنی دیجیتال»[۲] تهیه شده است، در نهایت پنج اصل راهبردی را تعیین کرده و سپس چگونگی استفاده شرکت‌ها از این اصول برای توسعه بهترین روش‌های احراز سن را توصیف می‌کند. البته روش‌های مورد استفاده سرویس‌ها برای احراز سن، بسته به محصول یا ویژگی دیجیتال آن، متفاوت است و برحسب چالش‌ها و پیشرفت‌های محقق شده در فناوری‌های احراز سن، تکامل می‌یابند.

این پنج اصل راهبردی عبارت‌اند از:

۱. شناسایی، ارزیابی و تعدیل ریسک‌های متوجه افراد زیر سن قانونی، برای به‌کارگیری نتایج آن در روش‌های احراز سن، به عنوان بخشی از پیاده‌سازی «ایمنی در مرحله طراحی خدمات»[۳]؛

۲. در نظر گرفتن ریسک‌های مربوط به حریم خصوصی کاربر و حفاظت از داده‌ها به عنوان بخشی از توسعه، پیاده‌سازی و ارزیابی مداوم رویکردهای احراز سن؛

۳. اطمینان از شمول و دسترسی‌پذیری تمام کاربران به رویکردهای احراز سن، صرف‌نظر از سن، وضعیت اجتماعی-اقتصادی، نژاد یا سایر ویژگی‌ها؛

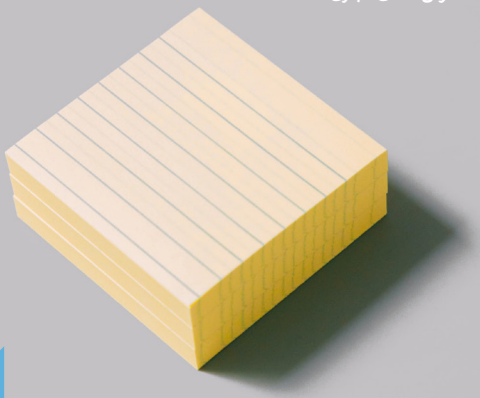
۱. این سند با عنوان «Age Assurance; Guiding Principles and Best Practices» حاصل تلاش‌های «گروه کاری شیوه‌نامه‌های مرتبط با سن» در «مؤسسه اعتماد و ایمنی دیجیتال» است که با تسهیلگری بتسی ماسیلو و درک اسلاتر، در سپتامبر ۲۰۲۳ منتشر شده است.

۲. Digital Trust and Safety Partnership (DTSP)

۳. safety-by-design

۴. انجام عملیات اجرایی لایه‌ای[۱] برای پیاده‌سازی رویکردهای احراز سن؛
۵. اطمینان از شفافیت سیاست‌ها و روش‌های احراز سن برای عموم مردم و ارائه گزارش‌های دوره‌ای در مورد اقدامات انجام‌شده به عموم و سایر ذی‌نفعان.

۱. عملیات اجرای لایه‌ای معمولاً به استراتژی‌ای اشاره دارد که شامل اجرای اقدامات مختلف برای رسیدگی به مسائل یا تهدیدات مختلف است. این رویکرد اغلب شامل استفاده از ترکیبی از اقدامات پیشگیرانه و نظارتی برای اطمینان از انطباق با مقررات (یا پروتکل‌های امنیتی و سایر استانداردها) است. در اصل، یک رویکرد چند وجهی برای حفظ کنترل، ایمنی یا پایبندی به دستورالعمل‌های خاص با استفاده از روش‌های اجرایی متعدد و مکمل است. در اینجا به این معنا است که رویکردهای مختلف احراز سن با هم ترکیب می‌شوند و این رویکردهای مختلف، بر اساس سطوح ریسک، در بخش‌های مختلفی از یک سرویس یا محتوا اِعمال می‌شوند.



مقدمه

وابستگی جوانان[۱] به سرویس‌های دیجیتال در تمام جنبه‌های زندگی آن‌ها؛ از جمله تجربیات آموزشی، تعاملات اجتماعی با دوستان، مشارکت در سرگرمی‌ها، بازی‌ها، اخبار و اطلاعات و مواردی از این دست، روزبه‌روز افزایش می‌یابد. سرویس‌های دیجیتال به دنبال طراحی تجربیات متناسب با سن (روش‌های متناسب‌سازی خدمت یا محتوا با سن) هستند و از جمله اقداماتی که در این راستا انجام می‌دهند، طراحی ویژگی‌هایی برای افزایش ایمنی است.

۱. در زمینه بحث پیرامون تجربه‌های متناسب با سن در فضای آنلاین، هیچ تعریف استانداردی از شخص جوان، کودک، نوجوان یا بزرگ‌سال وجود ندارد. برای اهداف دنبال شده در این گزارش، در سراسر این مقاله از عبارات «جوان» یا «کاربر جوان» و «بزرگ‌سال» برای بیان تقسیم‌بندی کاربران «دارای سن» و «زیر سن» قانونی استفاده می‌کنیم، با توجه به اینکه عامل تعیین‌کننده این سن خاص در حوزه‌های قضایی سراسر جهان با هم متفاوت خواهد بود. طبق کنوانسیون سازمان ملل در مورد حقوق کودکان، اشاره ما در اینجا «به معنای هر انسانی زیر هجده سال است مگر اینکه طبق قوانین اجرایی سن بلوغ کمتر لحاظ شده باشد»، اگرچه سرویس‌ها قطعاً بر اساس گستره‌ای از عوامل، از جمله قوانین محلی، مرزبندی‌های بیشتری را انجام می‌دهند.

توسعه سرویس‌های دیجیتالی که متناسب با سن هر کدام از کاربران باشد، چالش‌های مختلفی را به همراه دارد. این چالش‌ها شامل (و نه محدود به) «پیچیدگی در تعریف محتوای متناسب با سن در جوامع مختلف فرهنگی سراسر جهان»، «احتساب نقش والدین در زندگی نوجوانان» و «تضاد ذاتی بین تعیین دقیق سن کاربر و درعین‌حال، احترام به حریم خصوصی او» است. همچنین در خصوص نحوه سنجش فعالیت‌های یک سرویس، استانداردهای مشخص و مورد پذیرش جهانی وجود ندارد؛ اگرچه تلاش‌ها برای تبیین چنین استانداردهایی در جریان است.[۱]

درحالی‌که سرویس‌های دیجیتال و همه ذی‌نفعان بر سر نیاز به «تناسب خدمت یا محتوا با سن» به توافق رسیده‌اند؛ اما بر سر راه‌حلی قابل‌اعمال برای همه سرویس‌ها با هم همسو نیستند. در حال حاضر انواعی از رویکردهای (روش‌های) احراز سن وجود دارد و هر رویکرد نیز مزایا و معایب مختص به خود را دارد. افزایش اطمینان از سن کاربران پیامدهایی برای محافظت از حقوق حریم خصوصی آن‌ها، تضمین دسترسی آن‌ها به اطلاعات و حفظ آزادی آن‌ها برای مشارکت در تجربیاتِ دیجیتالِ بدون محدودیت، به همراه دارد. این پیامدها نه‌تنها برای جوانان (افراد زیر سن قانونی) بلکه برای همه کاربران یک سرویس اهمیت دارد. علاوه بر این، ریسک‌های مرتبط با دسترسی جوانان به سرویس، بسته به ماهیت آن، متفاوت خواهد بود. به عنوان مثال ممکن است یک سرویس فقط برای بزرگسالان (افراد بالای سن قانونی)، یا با محوریت جوانان یا با هدف جذب مخاطبان مختلف ساخته شده باشد (هر کدام از این موارد، ریسک‌های مختلفی خواهند داشت). مشخصات ریسک هر سرویس و همچنین انتظارات کاربران بر اساس اصول، ارزش‌ها و ویژگی‌های سرویس متفاوت خواهد بود. علاوه بر این، گروه‌های سنی مختلف (مانند نوجوانان) پیوسته سرویس‌های مختلف را تجربه می‌کنند. همه این‌ها

۱. به عنوان مثال می‌توانید به آدرس https://www.iso.org/standard/80399.html مراجعه کنید.

مستلزم مشورت دقیق با ذی‌نفعان مختلف، از جمله با خود نوجوانان، برای توسعه بهترین روش‌های احراز سن است.

مؤسسه اعتماد و ایمنی دیجیتال، جهت کمک به تعریف چارچوبی کلی برای رویکردهای مسئولیت‌پذیری سرویس‌های دیجیتال، مجموعه انعطاف‌پذیری از «بهترین روش‌ها» را توسعه داده است که نام آن «چارچوب بهترین روش‌های اعتماد و ایمنی» است. سرویس‌های مختلف می‌توانند به عنوان اجرای بخشی از تعهدات خود نسبت به سند چارچوب بهترین روش‌های اعتماد و ایمنی، برای رفع خطرهای متوجه کاربران زیر سن قانونی و توسعه تجربیات متناسب با سن، روش‌های احراز سن را استفاده کنند.

این سند، چالش‌های مقابل ارائه‌دهندگان سرویس‌ها در زمینه احراز سن را عنوان و سپس روش‌های آنلاین احراز سن را بیان می‌کند. پنج اصل راهبردی برای توسعه و به‌کارگیری بهترین روش‌ها تعیین می‌شود و سپس شیوه‌های خاص اجرایی‌سازی این چارچوب، به اشتراک گذاشته می‌شود. البته روش‌های خاص مورد استفاده سرویس‌ها، بسته به محصول یا ویژگی دیجیتال، متفاوت است و بر حسب چالش‌ها و پیشرفت‌های ایجادشده در فناوری‌های احراز سن تکامل می‌یابد.

با وجود این‌که این سند تمرکز خود را به احراز سن محدود می‌کند؛ اما شایان ذکر است که این کار تنها بخشی از نحوه رسیدگی سرویس‌ها به موضوع طراحی تجربیات متناسب با سن در فضای آنلاین است.

درحالی‌که سرویس‌های دیجیتال و همه ذی‌نفعان بر سر نیاز به «تناسب خدمت یا محتوا با سن» به توافق رسیده‌اند؛ اما بر سر راه‌حلی قابل‌اعمال برای همه سرویس‌ها با هم اتفاق‌نظر ندارند.

۱) روش‌های احراز سن

طیف گسترده‌ای از روش‌ها برای کسب اطمینان از سن کاربر توسعه یافته‌اند و طیف گسترده‌ای از تعاریف نیز برای توصیف آن‌ها استفاده می‌شود. احراز سن در واقع یک اصطلاح کلی است که برای توصیف طیف کاملی از روش‌های مورداستفاده سرویس‌ها برای اثبات، تعیین یا تأیید سن کاربر با سطحی از اطمینان به کار می‌رود. این روش‌ها ممکن است به‌تنهایی یا در ترکیب با یکدیگر، در یک سرویس مشخص به کار روند.

۱-۱) راستی‌آزمایی (اعتبارسنجی) سن

در یک‌سوی طیف احراز سن، روش‌هایی برای راستی‌آزمایی سن[۱] کاربر وجود دارند که به مرجعی قابل‌اعتماد وابسته هستند. در این موارد، ارائه‌دهندگان سرویس‌های دیجیتال برای اطمینان از سن کاربر، به مشخصات کاربری معتبر، واحدی ثالث یا به رابط برنامه‌نویسی اپلیکیشن (API) دولتی وابسته هستند؛ یا اینکه ارائه‌دهندگان، به رضایت والدین (قیم قانونی)[۲] تکیه می‌کنند.

راستی‌آزمایی مدارک هویتی

راستی‌آزمایی مدارک هویتی[۳] سازوکاری برای جمع‌آوری اطلاعات سنی و مشخصات کاربری است. این کار مستلزم دسترسی به اسناد ثالثی است که معمولاً به شکل کارت‌های شناسایی دولتی بوده و سن افراد را تأیید می‌کند.[۴] ارائه‌دهندگان سرویس‌ها در زمینه تأیید سن معمولاً فقط اطلاعات مربوط به سن فرد را نگهداری می‌کنند و خود اسناد هویتی ارائه‌شده را معدوم می‌کنند. بااین‌وجود، کاربر باید اطلاعات بیشتری نسبت به آنچه برای احراز سن او لازم است، به پلتفرم ارائه دهد. هدف ارائه‌دهندگان سرویس‌های دیجیتال، رفع نگرانی‌های مربوط به حریم خصوصی با به حداقل رساندن اطلاعات شخصی حساسِ نگهداری شده است. علاوه بر این چالش‌ها، راستی‌آزمایی با اسناد هویتی، چالش‌هایی را در زمینه برابری ایجاد می‌کند؛ زیرا دسترسی به کارت‌های شناسایی دولتی یا سایر اسناد لازم برای تأیید سن و هویت، مانند گواهی‌های تولد، بر حسب زمینه‌های اجتماعی-اقتصادی

۱. AgeVerification

۲. در گستره این نوشتار، منظور ما از «والدین» به معنای کلی قیم کاربر جوان (زیر سن قانونی) است.

۳. Identity document verification

۴. اسنادی که می‌توان آن‌ها را برای فرایند تأیید هویت پذیرفت عبارت‌اند از: گواهی تولد، کارت‌های شناسایی مدرسه، صورت‌حساب‌های آب و برق به نام فرد، تأیید حساب بانکی یا کارت اعتباری یا اسناد مالکیت املاک.

کاربران، با هم متفاوت هستند. در برخی موارد، شرایط اجتماعی یا سیاسی باعث می‌شود تا برای برخی کاربران، دستیابی به اسناد هویتی یا حمل آن خطرناک باشد.

اجرای راستی‌آزمایی هویت در خود پلتفرم، با چالش‌های عملیاتی قابل‌توجهی همراه است و مزایا و معایبی را به همراه دارد. درست مثل سایر کارکردهای اعتماد و ایمنی، راستی‌آزمایی (احراز) هویت نیز به ترکیبی از تکنیک‌های یادگیری ماشینی و بازبینی انسانی نیاز دارد تا بتواند اقدامات متقلبانه در احراز هویت و سن را شناسایی کند و فرایندهای تجدیدنظر کافی را در اختیار کاربران قرار داد. علاوه بر پیچیدگی عملیاتی پیاده‌سازی این بازبینی‌ها، جمع‌آوری این داده‌های هویتی اضافی نیز معضلاتی را در زمینه حریم خصوصی و حفاظت از داده‌ها ایجاد می‌کند.

شرکت‌های ثالثی (بی‌طرف و مستقلی) هم وجود دارند که راستی‌آزمایی هویت را به عنوان نوعی خدمت ارائه می‌دهند و این کار از فعالیت‌های عملیاتیِ اضافی (سربارهای عملیاتی) ارائه‌دهندگان سرویس‌های دیجیتال برای پیاده‌سازی راستی‌آزمایی سن می‌کاهد؛ اما همچنان باعث افزایش هزینه‌ها شده و همچنین ممکن است در زمینه روش‌های عملکرد چالش‌برانگیز در استفاده از داده‌ها برای ارائه‌دهندگان سرویس‌های دیجیتال ابهاماتی ایجاد کند.

اخیراً برخی از دولت‌ها در حال استقرار سیستم‌های شناسایی هویت هستند[۱] که از راستی‌آزمایی هویت نیز پشتیبانی می‌کنند. دولت‌ها در پیاده‌سازی استانداردهای

۱. برای مثال، اتحادیه اروپا در حال توسعه شناسه دیجیتال اروپایی است، به آدرس زیر مراجعه کنید:
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
تعدادی از ایالت‌های آمریکا نیز استقرار شناسه‌های دیجیتال یا افزودن کارت شناسایی ایالتی به گوشی‌های همراه را پیاده‌سازی کرده یا در حال توسعه هستند - به عنوان مثال، می‌توانید به برنامه شناسه دیجیتال کلرادو به آدرس https://mycolorado.state.co.us و شناسه دیجیتالی در حال توسعه کالیفرنیا به آدرس https://cdt.ca.gov/digitalid مراجعه کنید.

مشترک برای اسناد مسافرتی قابل خواندن با ماشین، موفق عمل کرده‌اند[۱] و می‌توان همین کار را به‌منظور ایجاد قالبی مشترک برای شناسه‌های دولتی دیجیتال در فضای آنلاین نیز پیاده کرد.

این کار می‌تواند سربارهای عملیاتی کسب‌وکارها را کاهش دهد، اگرچه این موضوع کاملاً به نحوه اجرا بستگی دارد. به عنوان مثال، اگر هر دولتی به‌جای تکیه بر یک استاندارد مشترک، رویکرد خود را توسعه دهد، در این صورت برای بسیاری از سرویس‌ها استفاده از شناسه‌های دیجیتالی مختلف به شیوه‌ای یکپارچه همچنان دشوار خواهد بود. علاوه بر این، اتکا به سیستم‌های هویتی دولتی قطعاً نگرانی‌هایی را در مورد جمع‌آوری داده‌ها از سوی دولت و پایش زندگی روزمره آنلاین کاربران ایجاد می‌کند.

موافقت و رضایت والدین

رضایت والدین[۲] روشی متکی به تأیید والدین (یا قیم قانونی) است و در برخی موارد، طبق مقررات موجود ضروری است. برخی از تنظیم‌گران هنگام الزام ارائه‌دهندگان سرویس‌های دیجیتال به راستی‌آزمایی سن کاربر برای دسترسی به یک سرویس، به رضایت والدین اتکا کرده‌اند. به عنوان مثال، قانون حفاظت از حریم خصوصی آنلاین کودکان[۳] در ایالات متحده آمریکا ایجاب می‌کند که اگر سرویس‌ها اطلاع دارند کاربری زیر ۱۳ سال سن دارد، باید رضایت والدین را دریافت کنند. تأثیر این قانون این بود که این سرویس‌ها به دو دسته تقسیم شدند؛ دسته‌ای که به کاربران زیر ۱۳ سال اختصاص داشته و فرایند رضایت والدین را اجرا کردند و دسته‌ای که به کاربران

۱. به آدرس زیر مراجعه کنید:
https://www.icao.int/publications/pages/publication.aspx?docnum=9303

۲. Parental consent

۳. Children's Online Privacy Protection Rule (COPPA)

زیر ۱۳ سال اجازه استفاده نمی‌دادند. قوانین مشابهی نیز در سایر حوزه‌های قضایی پیرامون جمع‌آوری و تجزیه و تحلیل داده‌های شخصی، البته برای سنین نیازمند رضایت، وجود دارند. به عنوان مثال، در اروپا، ماده ۸ مقررات عمومی حفاظت از داده‌ها[۱] به کشورهای عضو اجازه می‌دهد سن را بین ۱۳ تا ۱۶ تعیین کنند. بر اساس دستورالعمل‌های استرالیا نیز افراد زیر ۱۵ سال نمی‌توانند خودشان به‌تنهایی برای استفاده از یک سرویس رضایت دهند. در کره، قانون حفظ حریم خصوصی داده‌ها سن را ۱۴ سال تعیین می‌کند. محدوده سنی نیازمند رضایت نیز در بسیاری از حوزه‌های قضایی مورد بحث است.

وقتی بتوان رضایت والدین را کسب کرد، این اطمینان ایجاد می‌شود که والدین کودک با دسترسی کودک به آن سرویس یا ویژگی خاص مشکلی ندارند. رضایت والدین می‌تواند ابزار مهمی برای مشارکت والدین در تجربه آنلاین کاربر جوان (زیر سن قانونی) باشد؛ اما نه تضمین‌کننده این است که کاربر حداقل سن لازم را دارد و نه اطلاعاتی از سن واقعی کودک را برای ارائه‌دهندگان سرویس‌ها مشخص می‌کند. در بهترین حالت، به جای اینکه خود کاربر این کار را انجام دهد، به والدین این فرصت را می‌دهد که سن کاربر را ارائه دهند. همچنین رضایت والدین مستلزم راستی‌آزمایی مسئولیت‌پذیری والدین و رابطه بین دو حساب کاربری است؛ بزرگسال بودن دارنده یک حساب را می‌توان مثلاً با کارت اعتباری تأیید کرد؛ اما هیچ روش قابل اطمینانی برای تأیید این موضوع وجود ندارد که حساب دوم مربوط به فرزند آن بزرگسال باشد. علاوه بر این، برخی از جوانان، والدینی ندارند که بتوان برای تأیید سن کاربر به آن‌ها اعتماد کرد و حتی ممکن است والدین به اشتباه سنی را تأیید کنند. کمیسر حفاظت

۱. General Data Protection Regulation (GDPR)

از داده‌های ایرلند خاطر نشان کرده است که «هنوز راه‌های زیادی برای بررسی دقت، تناسب و امکان‌پذیری رضایت والدین وجود ندارند»[۱].

۱-۲) تخمین‌سن

گاهی اوقات ارائه‌دهندگان سرویس‌های دیجیتال به عنوان بخشی از یک سیستم جامع مدیریت ریسک، از تکنیک‌های تخمین سن[۲] برای کاهش ریسک دسترسی کاربران زیر سن قانونی به محتوا یا تجربیات نامناسب استفاده می‌کنند. این تکنیک‌ها سن کاربر را راستی‌آزمایی نمی‌کنند؛ بلکه بر اساس ارزیابی برخی ویژگی‌ها یا رفتارهای ذاتی کاربر، برای ارائه‌دهنده سرویس‌ها، با درجه‌ای از اطمینان، مشخص می‌کنند که سن کاربر بالاتر یا کمتر از مقدار مشخصی است. این تکنیک‌ها ممکن است در کنار درخواست سن (خوداظهاری سن) یا تأیید سن از طریق اسناد استفاده شود.

سنجش ظرفیت

سنجش ظرفیت[۳] روشی است که در آن از آزمونی برای تعیین ظرفیت دانش یا تفکر تحلیلی کاربر به عنوان روشی برای مشخص کردن سن او استفاده می‌شود. به عنوان مثال، ممکن است از کاربر، حل یک پازل یا انجام آزمونی ریاضی درخواست شود. آزمایش ظرفیت داده‌های بسیار کمی را پیرامون کاربر جمع‌آوری می‌کند؛ اما محدودیت‌هایی هم دارد. به عنوان مثال، ممکن است دقت کافی نداشته باشد و غیر از موارد کلی، کارایی مناسبی در زمینه تعیین تناسب سنی ارائه ندهد. همچنین

۱. به آدرس زیر مراجعه کنید:
https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_Parental Consent.pdf
۲. Age Estimation
۳. Capacity testing

ممکن است بر اساس فرصت‌های آموزشیِ در اختیار کاربران و سن رشدی آن‌ها، نتایج ناعادلانه‌ای ارائه دهد. در نهایت، با افزایش سن و بالا رفتن سطح سواد و ظرفیت کلی، این ابزار در تفکیک سنین ناکارآمد خواهد بود و ممکن است کاربران مثلاً با کمک گرفتن از شخصی دیگر، این ابزار را دور بزنند.

استنباط سن

استنباط سن[۱] روش برآورد پیشرفته‌تری است که داده‌های مربوط به یک کاربر را به‌منظور تخمین سن کاربر تجزیه و تحلیل می‌کند. این تکنیک بر روی داده‌هایی به کار می‌رود که قبلاً توسط ارائه‌دهنده سرویس‌های دیجیتال طی استفاده کاربر از سرویس جمع‌آوری شده است. داده‌ها ممکن است در اثر تعامل کاربر با خود سرویس تولید شوند و همچنین امکان استفاده از داده‌های جمع‌آوری‌شده از طریق سرویس‌های دیگر زیر نظر همان ارائه‌دهنده یا منابع ثالث نیز وجود دارد.

به عنوان مثال، سایت شبکه اجتماعی می‌تواند سیگنال‌های رفتاری را بر اساس نحوه تعامل کاربر با سرویس ارزیابی کند یا پلتفرم رسانه‌ای می‌تواند سیگنال‌ها را بر اساس نوع محتوای مورداستفاده کاربر ارزیابی کند. اگر کاربر بیشتر به دنبال تماشای کارتون‌های مخصوص نوجوانان باشد، استنباط سرویس این‌گونه است که خود کاربر نیز شخصی نوجوان است؛ در مقابل، اگر کاربر اساساً به دنبال موضوعاتی مانند اطلاعات وام مسکن باشد، استنباط سرویس این‌گونه است که آن شخص بزرگسال است. اگر سرویس به سطحی از اطمینان برسد که کاربر، زیر سن قانونی است، ممکن است کاربر را وادار به ارائه شواهد دیگری از سن خود کند؛ به طور مشابه، اگر به نظر برسد کاربر خود را به عنوان یک فرد نوجوان جا زده تا به سایر

۱. Age inference

کاربران نوجوان دسترسی داشته باشد، ممکن است سرویس کاربر را وادار به ارائه شواهد دیگری از سن خود کند.

از آنجایی‌که این روش لزوماً به سیگنال‌های جمع‌آوری‌شده در طول استفاده از یک سرویس دیجیتال وابسته است، نمی‌توان روش استنباط سن را به‌راحتی و به‌محض ایجاد حساب کاربری به کار برد. در عوض، این روش معمولاً به عنوان بخشی از یک برنامه احراز سن گسترده‌تر اجرا می‌شود که شامل چندین روش است و ممکن است در خود پلتفرم یا توسط شرکت‌های ثالثی ساخته و اجرایی شود.

شاید روش استنباط، به جمع‌آوری داده‌های اضافی (حداقل قبل از درخواست اطلاعات بیشتر) بستگی نداشته باشد؛ اما همچنان نگرانی‌هایی را در مورد حفظ حریم خصوصی و داده‌ها ایجاد می‌کند. به عنوان مثال، ممکن است استفاده از تاریخچه وب‌گردی کاربر برای احراز سن در سرویس جداگانه‌ای متعلق به همان ارائه‌دهنده، نگرانی‌هایی را ایجاد کند.

تأییداجتماعی

تأیید اجتماعی[۱] به معنای استفاده از ارتباطات اجتماعی کاربر برای افزودن لایه‌های تأیید بیشتری به احراز سن وی است. این تکنیک متکی بر پرسش از سایر کاربرانی است که سن و یا هویت آن‌ها قبلاً با درجه‌ای از اطمینان تأیید شده است و از آن‌ها درخواست می‌شود که سن اعلام‌شده توسط یک کاربر خاص را تأیید کنند.

۱. Social vouching

تخمین «سن فیزیکی»

تخمین «سن فیزیکی»[۱] نیز به معنای استفاده از مشخصه‌های فیزیکی، به‌ویژه تصاویر چهره، برای تخمین سن کاربر است. این روش متکی به جمع‌آوری داده‌ها در هنگام ایجاد حساب کاربری یا طی فرایند احراز سن پس از مشکوک شدن به کاربری با زیر سن قانونی است. معمولاً این داده‌ها برای ارائه خدمات جمع‌آوری نمی‌شوند. این روش جمع‌آوری داده‌های اضافی، ریسک‌های مربوط به حریم خصوصی را برای کاربر افزایش می‌دهد و ارائه‌دهنده یا شرکت ثالث باید در این زمینه استانداردهای حفاظت از داده‌ها را به طور دقیق رعایت کند. به خاطر کاهش ریسک، تخمین سن با استفاده از تصاویر چهره، روشی است که تا به امروز بیشتر توسط شرکت‌های ثالث به کار گرفته شده است تا اینکه به طور داخلی توسط ارائه‌دهندگان خدمات انجام شود.

درحالی‌که این نوع از برآورد سن امکان ارائه درجه بالایی از دقت را در تخمین سن کاربر دارد؛ اما با محدودیت‌هایی در رابطه با تقاضای مجموعه‌ای اضافی از داده‌های شخصی کاربران مواجه است. برخی کاربران ممکن است نگرانی‌هایی در خصوص جمع‌آوری اطلاعات اضافی داشته باشند و استفاده از شرکت‌های ثالث تخصصی احراز سن نیز لزوماً این نگرانی را برطرف نمی‌کند. در واقع وقتی شرکتی سرویس تشخیص چهره کاربران را به ارائه‌دهنده سرویس‌های دیجیتال عرضه می‌کند، ممکن است درک نحوه استفاده و حفاظت از داده‌ها، برای کاربران بسیار چالش‌برانگیزتر باشد. در رابطه با چالش‌های تکنیک‌های تخمین سن فیزیکی علاوه بر موارد فوق، بایستی به مسائل احتمالی پیرامون دقت و سوگیری، از جمله سوگیری احتمالی نژادی نیز توجه شود.

۱. Physical age estimation

۱-۳) خوداظهاری

خوداظهاری[۱] (که گاهی اوقات «احراز سن ادعایی» نیز نامیده می‌شود) به معنای درخواست از کاربر برای اعلام سن خود است. برخی از روش‌های خوداظهاری صرفاً از کاربران می‌خواهند که سن قانونی خود را تأیید کنند و با پرسیدن سؤال، نسبت به اینکه آیا کاربر بالاتر از سنی مشخص است یا خیر، این کار را انجام می‌دهند؛ مابقی روش‌ها، سؤال با پاسخ «بله یا خیر» نیستند و از کاربر می‌خواهند سن خود را اعلام کند. این روش گسترده‌ترین روشی است که تا به امروز برای احراز سن استفاده شده است؛ اما آسیب‌پذیری بالایی در برابر آن دسته از کاربرانی دارد که اطلاعات نادرست ارائه می‌دهند. این روش اغلب به عنوان یک روش در یک سیستم مدیریت ریسک گسترده‌تر استفاده می‌شود. به عنوان مثال، ممکن است سرویسی از خوداظهاری استفاده کند و بعد از آن روش تخمین «سن فیزیکی» را برای همه کاربران به کار گیرد.

۱. Self-declaration

۲) گزینه‌های موجود برای پیاده‌سازی روش‌های احراز سن

انتخاب‌های مختلفی برای پیاده‌سازی روش‌های احراز سن وجود دارد. برای مثال:

- احراز سن توسط پلتفرم‌ها و دستگاه‌ها: برخی از پلتفرم‌ها و سازندگان دستگاه‌ها (ابزارهای الکترونیک) ممکن است روشی را برای احراز سن پیاده‌سازی کنند تا سنی را برای کاربر مشخص کنند و سپس آن سن را در اختیار برنامه‌ها و سایر سرویس‌های آن دستگاه الکترونیک قرار دهند.
- راستی‌آزمایی از سوی واحدی ثالث: راستی‌آزمایی از سوی واحدی ثالث (بی‌طرف یا مستقل) در زمینه تأیید هویت و احراز سن، به دخالت یک نهاد یا ارائه‌دهنده سرویس بیرونی برای راستی‌آزمایی و تأیید هویت یا سن یک فرد اشاره دارد. پلتفرم‌ها به‌جای تکیه صرف بر فرایندهای داخلی یا خوداظهاری، از سرویس‌ها یا سیستم‌های ثالث بیرونی برای تأیید درستی اطلاعات ارائه‌شده توسط کاربران استفاده می‌کنند. به عنوان مثال ممکن است یک بانک، تشکیلات یا

نهاد اعتباری، اطلاعاتی مبنی بر این که شخصی، مشتری آن‌ها است را در اختیار سرویس ثالثی قرار دهند تا سن او را مشخص کنند. ممکن است این کار به شکل راستی‌آزمایی دولتی باشد، مانند برنامه‌های هویت دیجیتالی که در بالا بررسی شدند.

- احراز سن توسط شرکت‌ها: برخی از سرویس‌ها برای اجرای روش‌های احراز سن، شرکت‌هایی را به کار می‌گیرند که در این زمینه از فناوری‌های اختصاصی یا جمع‌آوری داده‌های منابع مختلف بهره می‌برند. پس از انتقال داده‌های شخصی کاربر به این شرکت‌ها، آن‌ها مسئولیت انجام آزمایش احراز سن واقعی و همچنین پیاده‌سازی روش‌های حفظ حریم خصوصی و امنیت داده‌ها را بر عهده می‌گیرند.
- سرویس‌های داخلی: برخی از ارائه‌دهندگان سرویس‌ها، روش‌های احراز سن را به طور کامل در پلتفرم خود و با ترکیب فناوری‌های اختصاصی، نرم‌افزارهای منبع‌باز و سازوکارهای اجرایی عملیاتی، پیاده‌سازی می‌کنند. ارائه‌دهنده همچنین ممکن است که این خدمات خود را در اختیار واحدهای ثالث نیز قرار دهد.

سرویس‌ها ممکن است که به شیوه‌های پیاده‌سازی مختلفی متکی باشند و ممکن است در مناطق جغرافیایی مختلف، روش‌های مختلفی را بر اساس نیازهای محلی، اعمال کنند.

۳) چالش‌های کلیدی

توسعه رویکردهای احراز سن با چندین چالش روبه‌رو است. مشخصه‌های کلیدی مورد توجه ارائه‌دهندگان سرویس‌های دیجیتال در توسعه این رویکردها عبارت‌اند از:

- کارآمدی: اطمینان از اینکه کاربر سن معینی دارد به ارائه‌دهنده سرویس‌های دیجیتالی اجازه می‌دهد تا تجربه‌ای متناسب با سن کاربر را ارائه نمایند؛ به نحوی که دقیق بوده و دور زدن آن دشوار باشد.
- در دسترس، فراگیر و عادلانه: احراز سن نباید به نتایج ناعادلانه برای یک کاربر منجر شود و پیچیدگی فرایندها نیز نباید بیش از حد به کاربر فشار بیاورد به گونه‌ای که مانع استفاده مناسب او از سرویس شود.
- رعایت حریم خصوصی و حفاظت از داده‌ها: حفاظت از حریم خصوصی کاربر، به ویژه حریم خصوصی یک کاربر جوان (زیر سن قانونی)، مستلزم رعایت اصول

کلیدی حفظ حریم خصوصی از جمله حداقل‌سازی دریافت داده‌ها و همچنین پیاده‌سازی اقدامات امنیتی برای محافظت از داده‌ها است.

- مقرون به صرفه: هزینه‌های پیاده‌سازی باید معقول و متناسب باشند.
- تناسب با ریسک: رویکردهای به‌کارگرفته‌شده باید متناسب با ریسک‌های مرتبط با دسترسی افراد زیر سن قانونی به یک سرویس معین و همچنین ریسک‌های ناشی از تعیین نادرست سن باشند.

گنجاندن هر کدام از این مشخصه‌ها مستلزم ایجاد توازن (یعنی توجه به چالش‌ها و کاهش آن‌ها) است و هیچ راه‌حل یکسانی برای همه موارد وجود ندارد. روش‌های بسیار دقیق احراز سن، به جمع‌آوری داده‌های شخصی جدید مانند تصاویر چهره یا کارت شناسایی صادرشده توسط دولت بستگی دارند. برخی از روش‌های مقرون‌به‌صرفه ممکن است در بین کاربران نابرابری ایجاد کنند. هر سرویس و حتی ویژگی[۱] ممکن است نمایه[۲] ریسک متفاوتی برای کاربران کم سن و سال‌تر داشته باشد؛ برای مثال، ویژگی‌هایی که برای تسهیل ملاقات کاربران در زندگی واقعی طراحی شده‌اند، در مقایسه با سرویس‌هایی که دسترسی به انواع مختلف محتوا را فراهم می‌کنند، ریسک‌های بسیار متفاوتی نسبت به هم دارند.

سرویس‌ها بر اساس سطح بلوغ و اندازه و همچنین ماهیت ریسک‌های مرتبط با خدماتشان، با چالش‌های متفاوتی روبرو خواهند بود. برخی از روش‌های احراز سن برای شرکت‌های کوچک‌تر مقرون‌به‌صرفه نیستند و اگر این روش‌ها متناسب با ریسک نباشند ممکن است بی‌جهت باری را بر دوش این شرکت‌ها اضافه کنند. درحالی‌که ممکن است ارائه‌دهندگان بزرگ‌تر، استفاده از این روش‌ها را سرمایه‌گذاری مناسبی برای خود بدانند، به ویژه اگر خدماتشان مشتمل بر فعالیت‌های با ریسک

۱. Feature
۲. Profile

بالاتر باشد؛ اما ممکن است شرکت‌های کوچک‌تر با تحمیل این هزینه‌ها، نتوانند کسب‌وکار خود را حفظ کنند. بنابراین مهم است که شرکت‌ها ریسک‌های مرتبط با سن را با روش‌های مختلفی کاهش دهند، برای مثال ریسک آسیب‌های مربوط به افراد زیر سن قانونی در یک سرویس را قبل از پیاده‌سازی روشی پرهزینه برای احراز سن کاهش دهند.

به طور مشابه، روش‌های احراز سن ممکن است تعارضاتی با تعهدات حفظ حریم خصوصی یک سرویس در قبال کاربران داشته باشند و نیاز به ایجاد توازن[1] در آن‌ها احساس شود. حفظ انعطاف‌پذیری سرویس‌ها در قبال اتخاذ این تصمیم‌ها برای پیاده‌سازی احراز سن در زمینه گسترده‌تر کاهش ریسک‌های مرتبط با سن، از جمله بر اساس ماهیت سرویس‌های ارائه‌شده، مهم است.

احراز سن مناسب، بر اساس ارزیابی ریسک‌ها و مزایای هر روش در یک حوزه خاص، میان سرویس‌های مختلف با هم متفاوت است و برای احراز سن، رویکرد (روش) واحدی وجود ندارد. ممکن است سرویسی از روش‌های متفاوتی برای جنبه‌ها یا ویژگی‌های مختلف سرویس استفاده کرده و از رویکردی چندلایه استفاده کند.

اصول و روش‌های زیر نشان می‌دهند که چگونه شرکت‌های اجراکننده، می‌توانند احراز سن را در چارچوب یک برنامه اعتماد و ایمنی گسترده، اجرایی کنند.

۱. سبک‌سنگین کردن مزایا و معایب هر تصمیم و انتخاب تصمیم بهینه.

برخی از روش‌های احراز سن برای شرکت‌های کوچک‌تر مقرون به صرفه نیستند و اگر این روش‌ها متناسب با ریسک نباشند ممکن است بی‌جهت باری را بر دوش این شرکت‌ها اضافه کنند.

۴) اصول راهبردی

اصل ۱: شناسایی، ارزیابی و تعدیل ریسک‌های متوجه افراد زیر سن قانونی، برای به‌کارگیری نتایج آن در روش‌های احراز سن، به عنوان بخشی از پیاده‌سازی «ایمنی در مرحله طراحی خدمات»[۱]

- هدف: اطمینان از اینکه شرکت‌ها در خصوص ریسک‌های خاص متوجه جوانان (افراد زیر سن قانونی)، دوراندیشی کافی دارند و این احتیاط‌ها را در روش‌های احراز سن به کار می‌گیرند.
- تفسیر: شرکت‌های اجراکننده عمیقاً به توسعه تجربیات متناسب با سن و محافظت از ایمنی و احترام به حقوق و منافع جوانان (افراد زیر سن قانونی)،

۱. safety-by-design

از جمله حقوق آن‌ها در دسترسی به اطلاعات و حق آن‌ها برای حفظ حریم خصوصی اهمیت می‌دهند.[۱]

شرکت‌های اجراکننده، برای توسعه رویکردی متناسب برای احراز سن، ریسک‌های مختص جوانان (افراد زیر سن قانونی) را ارزیابی می‌کنند؛ ریسک‌هایی مثل محتوایی که ممکن است برای کاربران جوان‌تر نامناسب باشند یا ارتباط برقرار کردن بزرگسالان با آن‌ها با این هدف که آن‌ها را اغفال کنند. چنین ریسک‌ها و اثراتی، هم‌زمان با توسعه محصولات و ویژگی‌ها ارزیابی می‌شوند و ممکن است در طول زمان و پس از راه‌اندازی یک محصول یا ویژگی نیز تکامل یابند. پس به نوبه خود، ارزیابی و راستی‌آزمایی پیوسته ریسک‌ها و اثرات آن‌ها حیاتی است. همچنین چگونگی اثرگذاری روش‌های احراز سن بر جوانان و سایر کاربران نیز ارزیابی می‌شود.

نمونه‌هایی از شیوه‌های خاص ارزیابی و تجزیه و تحلیل ریسک‌های مربوط به جوانان (افراد زیر سن قانونی) در زمان اجرای احراز سن عبارت‌اند از:

- شناسایی و دسته‌بندی ریسک‌های متوجه جوانان (افراد زیر سن قانونی)؛ ریسک‌هایی مربوط به محتوا، رفتار، تماس (ارتباط) با سایر اشخاص و روابط تجاری ایجادشده بر بستر محصول؛
- توسعه تخصص، بینش و قابلیت‌های تجزیه و تحلیل تخصصی مرتبط با ریسک‌های دارای اثرگذاری بالا بر جوانان و اقدامات کاهنده مناسب؛
- توسعه و پیاده‌سازی چارچوب‌ها و بهترین روش‌ها برای ارزیابی ریسک و تأثیرات آن، که این موارد را در نظر می‌گیرد: احتمال مشغول شدن جوانان به یک سرویس یا ویژگی؛ مخاطبی که سرویس برای آن طراحی شده است؛

۱. به کنوانسیون سازمان ملل در مورد حقوق کودکان، دفتر کمیساریای عالی سازمان ملل، نوامبر ۱۹۸۹؛ تبصره کلی شماره ۲۵ (۲۰۲۱) در مورد حقوق کودکان در رابطه با محیط دیجیتال، OHCHR، مارس ۲۰۲۱، مراجعه کنید.

ظرفیت‌های روبه‌رشد جوانان با افزایش سن آن‌ها؛ ریسک قابل پیش‌بینی و بهترین منافع و مصالح جوانان؛

- مشورت با اشخاص ثالث از جمله جوانان و خانواده‌ها، برای ارزیابی ریسک‌ها و اثرات آن‌ها و انتخاب روش‌های احراز سن؛
- ورود متخصصان به موضوع جوانان و ایمنی آن‌ها در کل فرایند توسعه محصول و ارائه بازخوردهای مداوم (هم قبل از راه‌اندازی و هم پس از آن) درباره ریسک‌های متوجه جوانان و همچنین حمایت از حقوق آن‌ها.

اصل ۲: در نظر گرفتن ریسک‌های مربوط به حریم خصوصی کاربر و حفاظت از داده‌ها به عنوان بخشی از توسعه، پیاده‌سازی و ارزیابی مداوم رویکردهای احراز سن.

- هدف: اطمینان از اینکه روش‌های احراز سن به حفاظت از داده‌ها و حقوق حریم خصوصی، به ویژه حریم خصوصی جوانان احترام می‌گذارند.
- تفسیر: هنگام ارزیابی مناسب‌ترین روش برای یک محصول (یا ویژگی‌های آن)، باید حریم خصوصی و حفاظت از داده‌ها را مدنظر قرار داد. هر روش احراز سن، تأثیرات متفاوتی بر حریم خصوصی کاربر دارد و سرویس‌های مختلف شیوه‌های متفاوتی را برای حفظ حریم خصوصی دارند که بر انتظارات کاربر تأثیر می‌گذارد. جدای از بررسی بهترین روش احترام به حریم خصوصی در زمان پیاده‌سازی روش‌های احراز سن، چالش دیگری که برای ارائه‌دهندگان سرویس‌های دیجیتال وجود دارد، کسب بینش و اعتماد نسبت به شیوه‌های حفظ حریم خصوصی در شرکت‌های ثالث احراز سن است که نه‌تنها برای اجرای تعهدات خود نسبت به کاربران ضروری است؛ بلکه برای اجرای مناسب مسئولیت‌های تنظیم‌گرانه و انطباق با قوانین نیز ضرورت دارد.

نمونه‌هـایی از شیوه‌هـای خـاص محافظـت از حـقوق حریـم خصوصـی کاربـران عبارت‌انـد از:

- حداقل‌سازی جمع‌آوری داده‌های شخصی برای احراز سن متناسب با ریسک ارزیابی‌شده و طراحی شیوه‌های سفارشی برای نگهداری، حذف و استفاده از داده‌ها؛
- استفاده از داده‌های حساس جمع‌آوری‌شده صرفاً برای احراز سن و حذف سریع این داده‌ها پس از انجام احراز سن؛
- برای جلوگیری از انتقال داده‌های شخصی به سرورهایی (از جمله سرورهای ارائه‌دهنده سرویس‌های دیجیتال) که خارج از کنترل کاربر هستند، تحلیل داده‌های شخصی در صورت امکان فقط روی دستگاه کاربر انجام گیرد؛
- برای احراز سن، از روش‌های تخمین سن بر روی داده‌های جمع‌آوری شده استفاده شود تا از جمع‌آوری داده‌های شخصی جدید جلوگیری شود؛
- در پیاده‌سازی احراز سن از طریق شرکت، تمام داده‌های شخصی جدید جمع‌آوری شده (مثلاً عکس‌های سلفی) فقط برای شرکت انجام دهنده احراز سن ارسال شوند، نه اینکه ابتدا برای ارائه‌دهنده سرویس‌های دیجیتال ارسال گردند؛
- الزام شرکت‌ها به اعمال استانداردهای سطح بالای امنیت و حریم خصوصی و سپس اطمینان از بررسی و تأیید آن شرکت‌ها از این جهت که این استانداردها را رعایت می‌کنند؛
- داشتن شفافیت نسبت به کاربران در زمینه نحوه جمع‌آوری، استفاده و نگهداری از داده‌های آن‌ها؛

- تکمیل ارزیابی تأثیر[۱] حفاظت از داده‌ها قبل از پیاده‌سازی هر روش جدید احراز سن (یعنی هر روش احراز سن، مانند پیوست فرهنگی، یک پیوست حفاظت از داده داشته باشد)؛
- در صورت امکان، اتکا به راه‌حل‌های تعامل‌پذیر احراز سن که مسئولیت ارائه اطلاعات اضافی به سرویس‌های جدید را به حداقل می‌رساند و ریسک‌های حفاظت از داده متوجه کاربر را کاهش می‌دهد.

اصل ۳: اطمینان از شمول و دسترسی‌پذیری تمام کاربران به رویکردهای احراز سن، صرف‌نظر از سن، وضعیت اجتماعی-اقتصادی، نژاد یا سایر ویژگی‌ها.

- هدف: تضمین عدم ممانعت بی‌جهت احراز سن در دسترسی به سرویس، با توجه به اثرات مختلفی که روش‌های احراز سن دارند.
- تفسیر: اگر احراز سن منجر به قطع دسترسی دسته‌ای از کاربران به سرویس‌های دیجیتال باشد که سرویس‌های مدنظر آن‌ها بوده است، در این صورت، آن روش احراز سن زیان‌آور خواهد بود. به‌کارگیری روشی برای احراز سن که مثلاً متکی به کارت‌های شناسایی صادره از سوی دولت است، شاید باعث ایجاد تبعیض در میان کاربران جوان‌تر و کاربرانی شود که در منطقه محلی خود نیازی به دریافت کارت‌های شناسایی صادره از سوی دولت نداشته‌اند. به طور مشابه، انواع خاصی از تخمین سن مانند تخمین‌های مبتنی بر تصاویر چهره ممکن است برای افراد یک قومیت یا جمعیتی در یک بازه سنی خاص، سطح اطمینان بیشتر یا کمتری ارائه کنند. شرکت‌های اجراکننده باید این اثرات مختلف را در طراحی رویکرد احراز سن به طور فراگیر در نظر گیرند.

۱. Impact Assessment

نمونه‌هایی از شیوه‌های خاص تضمین فراگیری و دسترسی‌پذیری برای همه کاربران عبارت‌اند از:

- تا آنجا که امکان‌پذیر است و با الزامات قانونی هم‌خوانی دارد، شرکت‌های تأیید سنی انتخاب شوند که گزینه‌هایی فراتر از اسناد شناسایی صادره از سوی دولت (که ممکن است برخی افراد نداشته باشند) مثل «گواهی تولد» و «کارت شناسایی مدرسه» (که همه دارند) یا «ترکیبی از یک شناسه حساب کاربری منحصر به فرد و تصویری از کاربر» را ارائه می‌دهند تا اطمینان حاصل شود که تأیید کاربران بدون دسترسی به مدارک شناسایی صادره از سوی دولت امکان‌پذیر است و تبعیضی صورت نمی‌گیرد؛
- ارائه سازوکار در دسترس و با قابلیت استفاده آسان جهت ارسال درخواست تجدیدنظر برای آن دسته از کاربرانی که در روش تخمین سن با مشکل مواجه شده‌اند (مثلاً به دلیل استفاده همزمان فرزند و والد از یک حساب کاربری، پلتفرم مبتنی بر جستجوی محتوای کودکانه از سوی فرزند، سن کاربر را کودک تشخیص داده است و والد نمی‌تواند از همه خدمات پلتفرم استفاده کند. در نتیجه والد باید درخواست تجدیدنظر ارسال کند)؛
- انجام تحلیل تأثیرات[۱] قبل از به‌کارگیری تکنیک‌های تخمین سن برای جمعیت خاصی از کاربران جهت درک هرگونه پیامدهای تبعیض‌آمیز و کاهش آن‌ها؛
- ارائه فرایند پرچم‌گذاری برای کاربران که یک کاربر زیر سن قانونی را گزارش دهند و ارائه دسترسی به کاربر مورد نظر جهت ارسال درخواست تجدیدنظر برای اثبات سن خود؛
- بازبینی (بررسی) اجرای روش‌های احراز سن، از سوی شرکت‌های ثالث معتبر یا در صورت لزوم ارائه‌دهندگان سرویس‌ها؛
- مشورت با اشخاص ثالث برای ارزیابی اثرات روش‌های مورد نظر برای احراز سن.

۱. Impact Analysis

اصل ۴: انجام عملیات اجرایی لایه‌ای برای پیاده‌سازی رویکردهای احراز سن.

- هدف: اطمینان از وجود ظرفیت عملیاتی برای جلوگیری از دسترسی کاربران به سرویس‌ها یا ویژگی‌های نامتناسب با سطح ریسک، محدود کردن دسترسی برای افرادی که به سرویس‌ها یا ویژگی‌های نامتناسب با سطح ریسک دسترسی پیدا کرده‌اند و ارائه فرایند تجدیدنظر برای آن دسته از کاربرانی که دسترسی آن‌ها تحت تأثیر فرایندهای احراز سن قرار گرفته و محدود شده است.
- تفسیر: سرویس‌ها یک عملکرد اجرایی را در شرکت تعریف و به تیم‌های مربوطه در شرکت آموزش می‌دهند که توانایی اجرای سیاست‌های دسترسی متناسب با سن را بر اساس خروجی روش‌های احراز سن دارد. شرکت‌ها بر اساس ارزیابی ریسک‌ها روی طیف وسیعی از فناوری‌ها و کارکنان سرمایه‌گذاری می‌کنند تا هم روش‌های مناسب برای احراز سن را انتخاب کنند و هم از اجرای مداوم آن‌ها اطمینان یابند. این عملیات، «لایه‌ای» است به این معنا که روش‌های مختلف احراز سن با هم ترکیب می‌شوند و روش‌های مختلف بر اساس سطوح ریسک برای بخش‌های مختلفی از یک سرویس، محتوا یا قابلیت‌های سرویس اعمال می‌شوند. همچنین سرویس‌ها این عملیات را بر اساس فناوری‌های در حال تحول و بهترین روش‌های عملکردی، مجدداً ارزیابی کرده و تنظیم می‌کنند.

نمونه‌هایی از شیوه‌های خاص عملیات اجرایی لایه‌ای برای پیاده‌سازی روش‌های احراز سن عبارت‌اند از:

- قراردادن محدودیت‌های پیش‌فرض برای دسترسی و کار با سرویس (یا ویژگی‌های مشخص یا محتوایی خاص)؛ مشروط به وجود اعلان‌هایی درون خود محصول درباره تناسب سنی آن محتوا یا خدمت؛

- برچسب‌گذاری کردن و در صورت لزوم، دسته‌بندی سرویس‌ها به‌عنوان سرویس‌های مناسب برای سنین خاص و هماهنگی با پلتفرم‌های توزیع[۱] به‌منظور اعمال محدودیت برای دانلود و دسترسی کاربران زیر سن قانونی؛
- بررسی احراز سن برای وقتی که کاربر در خوداظهاری، سن خود را از «کمتر از ۱۸ سال» به «بالای ۱۸ سال» تغییر می‌دهد؛
- تجزیه و تحلیل رفتار همه کاربرانی که در هنگام ایجاد حساب کاربری سن خود را اعلام می‌کنند، شناسایی کاربرانی که ممکن است اطلاعات نادرستی را وارد کرده و زیر سن قانونی باشند و بررسی پیوسته این کاربران با استفاده از آزمون‌های بیشتر احراز سن. پیام تبریک تولد ۱۱ سالگی خود کاربر یا تعامل بیشتر او با محتواهای مختص نوجوانان، نمونه‌هایی است از رفتارهایی که نشان‌دهنده نادرست بودن خوداظهاری سن هستند؛
- آموزش تیم‌های اجرایی برای شناسایی نشانه‌هایی از کاربری که سن خود را اشتباه گزارش کرده است (مثلاً ظاهرشان نشان می‌دهد که جوان‌تر هستند) و به‌کارگیری روشی برای بررسی‌های بیشتر در زمینه احراز سن؛
- ایجاد امکان ارسال گزارش کاربران نسبت به آن دسته از کاربرانی که سن خود را اشتباه گزارش کرده‌اند و بنابراین باید از سرویس‌ها یا ویژگی‌های خاصی محروم شوند؛
- پیاده‌سازی روش‌های فنی به‌منظور ایجاد ممانعت برای دور زدن کنترل‌ها توسط کاربرانی که در آزمون احراز سن مردود شده و واجد شرایط تشخیص داده نشده‌اند (مثلاً ایجاد ممانعت برای ثبت‌نام فوری با استفاده از حساب کاربری دیگر)؛

۱. Distribution platforms

- اجرای آزمون‌های جدید احراز سن برای کاربران موجود، وقتی که شرکت، فرایندهای احراز سن خود را بهبود بخشیده یا تغییر می‌دهد یا تغییرات مرتبطی را در محصول یا قابلیت‌های آن ایجاد می‌کند؛
- ارائه قابلیت حساب‌های خانوادگی همراه با راستی‌آزمایی والدین با اتصال حساب یک فرد جوان (زیر سن قانونی) به حساب والدین (یا قیم قانونی)؛
- ایجاد قابلیت تعیین الزامات سنی برای تعامل با محتوا یا انجمن‌های خاصِ درون یک سرویس، برای کاربران یا مدیران انجمن.

اصل ۵: اطمینان از شفافیت سیاست‌ها و روش‌های احراز سن برای عموم مردم و ارائه گزارش‌های دوره‌ای در مورد اقدامات انجام‌شده به عموم و سایر ذی‌نفعان.

- هدف: اطمینان از اینکه کاربران و عموم مردم نسبت به روش‌های احراز سن یک سرویس آگاهی دارند.
- تفسیر: شفافیت، کارکردی کلیدی در آگاهی‌بخشی به عموم مردم و آموزش ذی‌نفعان مختلف پیرامون روش‌های احراز سن یک شرکت دارد و درعین‌حال با گذشت زمان، نسبت به کفایت استاندارد مدنظر صنعت، اعتماد ایجاد می‌کند. با این حال، شفافیت را باید در کنار ریسک دستیابی کاربران به روشی برای دور زدن سیستم‌های احراز سن در نظر گرفت.

نمونه‌هـایی از شیوه‌هـای خـاص ایجـاد شـفافیت پیـرامون اقدامـات احـراز سـن عبارت‌انـد از:

- توضیح درمورد این که چرا به عنوان بخشی از فرایند ثبت‌نام، سن یا تاریخ تولد کاربر، جمع‌آوری می‌شود؛
- پیاده‌سازی راهکارهای منبع‌باز احراز سن، به‌گونه‌ای که ذی‌نفعان و متخصصان بیرونی به‌راحتی بتوانند کدنویسی انجام شده را بررسی کنند؛
- فراهم کردن دسترسی محققان مستقل (بی‌طرف) به جزئیات پیاده‌سازی و داده‌های مربوط به اثربخشی احراز سن، به‌گونه‌ای که ارزیابی مناسب بودن روش مورد نظر توسط عاملان بیرونی امکان‌پذیر باشد؛
- انتشار داده‌های مربوط به هزینه‌ی روش‌های مختلف احراز سن برای ارائه‌دهندگان در مقیاس‌های مختلف؛
- انتشار مطالب در مرکز راهنمایی[۱] سرویس، مبنی بر مشارکت ارائه‌دهنده سرویس با شرکت احرازکننده سن، مشتمل بر داده‌های به اشتراک گذاشته شده با شرکت و مروری بر شیوه‌های کار با این داده‌ها توسط آن شرکت؛
- ارائه اطلاعات کمّی و کیفی درمورد اجرای سیاست‌ها و روش‌های احراز سن.

۱. Help center

۵) ضمیمه۱

تعاریف

تعاریف زیر متناسب با اهداف چارچوب بهترین روش‌های مرتبط با سن «مؤسسه اعتماد و ایمنی دیجیتال» ارائه می‌شوند:

- احراز سن[۱]: اصطلاحی کلی برای توصیف طیف کاملی از روش‌های سرویس‌ها برای دستیابی به احتمالی قابل‌اطمینان از سن کاربر، مشتمل بر راستی‌آزمایی سن و راه‌حل‌های تخمین سن است. کلمه «احراز» به سطوح مختلفی از قطعیت راه‌حل‌های مختلف در تعیین سن یا محدوده سنی اشاره دارد.
- تخمین سن[۲]: به طیفی از روش‌ها با هدف کسب درجه‌ای از اطمینان نسبت به سن کاربر مبنی بر بالاتر یا پایین بودن سن از مقداری مشخص اشاره دارد تا بتوان با نتیجه آن دسترسی یا عدم دسترسی به محتوا یا سرویس‌های آنلاین با محدودیت سنی را تعیین کرد.

۱. Age Assurance
۲. Age Estimation

- راستی‌آزمایی سن[۱]: اقداماتی که سن فرد را با درجه قطعیت بالا و معمولاً از طریق اتکا به مستندات ثالث (مدارک هویتی) یا رضایت والدین برای تأیید سن کاربر، تعیین می‌کنند.
- تعهد[۲]: اقداماتی که شرکت‌های اجراکننده، به عنوان بخشی از چارچوب کلی بهترین روش‌های مؤسسه اعتماد و ایمنی دیجیتال، برای شناسایی و رسیدگی به ریسک‌های مرتبط با محتوا و رفتار به آن‌ها متعهد شده‌اند. این سند شامل تعهدات جدیدی نیست؛ بلکه شیوه‌هایی در آن ارائه شده تا برای پیاده‌سازی تعهدات کلی استفاده شوند.
- ریسک‌های مرتبط با محتوا و رفتار[۳]: اشاره به احتمال وجود محتوا یا رفتار غیرقانونی، خطرناک یا آسیب‌رسان، از جمله ریسک‌های متوجه حقوق بشر که به واسطه سیاست‌ها و شرایط و ضوابط سرویس‌های مربوطه ممنوع شده‌اند.
- ریسک‌های مرتبط با تماس (ارتباط)[۴]: به احتمال ارتباط غیرقانونی، خطرناک یا آسیب‌رسان از سوی اشخاص ثالث با کاربران جوان (زیر سن قانونی) اشاره دارد که به واسطه سیاست‌ها و شرایط و ضوابط سرویس‌های مربوطه ممنوع شده‌اند.
- ریسک‌های روابط تجاری[۵]: اشاره به احتمال روابط تجاری و قراردادی غیرقانونی، خطرناک یا آسیب‌رسان یا فشارهایی که ممکن است کاربری جوان (زیر سن قانونی) در استفاده از یک سرویس تجربه کند.

(ارجاعات به «ریسک‌ها» بایستی به‌صورت مجموعی از ریسک(های) مرتبط با محتوا، رفتار، ارتباط و روابط تجاری تفسیر شوند.)

۱. Age Verification
۲. Commitment
۳. Content- and Conduct-Related Risks
۴. Contact-Related Risks
۵. Commercial Relationship-Risks

- شرکت‌های اجراکننده[۱]: ارائه‌دهندگان محصولات یا سرویس‌هایی که تعهدات تشریح شده در چارچوب کلی بهترین روش‌های «مؤسسه اعتماد و ایمنی دیجیتال» را انجام می‌دهند.
- اعتماد و ایمنی[۲]: به زمینه و شیوه‌هایی اشاره دارد که چالش‌های مربوط به ریسک(های) مرتبط با محتوا و رفتار را مدیریت می‌کنند که شامل لحاظ کردن «ایمنی در مرحله طراحی»، «نظارت بر محصول»، «ارزیابی، شناسایی و پاسخ به ریسک»، «تضمین کیفیت» و «شفافیت» است.
- جوان و کاربر جوان[۳]: برای اهداف دنبال شده در این گزارش، در سراسر آن از عبارات «جوان» یا «کاربر جوان» و «بزرگسال» برای بیان تقسیم‌بندی کاربران «زیر سن» و «دارای سن» قانونی استفاده شده است، با توجه به اینکه سن تعیین‌کننده در حوزه‌های قضایی سراسر جهان متفاوت است. طبق کنوانسیون سازمان ملل متحد در مورد حقوق کودکان، منظور ما در اینجا از جوان، «هر انسانی زیر هجده سال است مگر اینکه طبق قوانین اجرایی، سن قانونی زودتر تعیین شده باشد»، اگرچه سرویس‌ها بر اساس طیفی از عوامل از جمله قوانین محلی، تقسیم‌بندی‌های بیشتری انجام می‌دهند.

۱. Practicing Companies
۲. Trust and Safety
۳. Youth and Young User

اقداماتی که سن فرد را با درجه قطعیت بالا و معمولاً از طریق اتکا به مدارک هویتی یا رضایت والدین تعیین می‌کنند، راستی‌آزماییِ سن نامیده می‌شوند.

۶) ضمیمه۲

تطبیق اصول و روش‌های احراز سن با چارچوب بهترین روش‌های (روال‌های مطلوب) مؤسسه اعتماد و ایمنی دیجیتال

اصل راهبردی ۱: شناسایی، ارزیابی و تعدیل ریسک‌های متوجه افراد زیر سن قانونی، برای به‌کارگیری نتایج آن در روش‌های احراز سن، به عنوان بخشی از پیاده‌سازی «ایمنی در مرحله طراحی خدمات».

اصول و روش‌های احراز سن	چارچوب بهترین روش‌های DTSP				
بهترین روش‌ها	توسعه محصول	نظارت بر محصول	اجرای محصول	بهبود محصول	شفافیت محصول
شناسایی و دسته‌بندی ریسک‌های متوجه جوانان (افراد زیر سن قانونی)؛ ریسک‌هایی مربوط به محتوا، رفتار، تماس (ارتباط) با سایر اشخاص و روابط تجاری ایجادشده بر بستر محصول.	●			●	
توسعه تخصص، بینش و قابلیت‌های تجزیه و تحلیل تخصصی مرتبط با ریسک‌های دارای اثرگذاری بالا بر جوانان و اقدامات کاهنده مناسب.	●			●	
توسعه و پیاده‌سازی چارچوب‌ها و بهترین روش‌ها برای ارزیابی ریسک و تأثیرات آن، که این موارد را در نظر می‌گیرد: احتمال مشغول شدن جوانان به یک سرویس یا ویژگی؛ مخاطبی که سرویس برای آن طراحی شده است؛ ظرفیت‌های روبه‌رشد جوانان با افزایش سن آن‌ها؛ ریسک قابل پیش‌بینی و بهترین منافع و مصالح جوانان.	●			●	
مشورت با اشخاص ثالث از جمله جوانان و خانواده‌ها، برای ارزیابی ریسک‌ها و اثرات آن‌ها و انتخاب روش‌های احراز سن.	●			●	
ورود متخصصان به موضوع جوانان و ایمنی آن‌ها در کل فرایند توسعه محصول و ارائه بازخوردهای مداوم (هم قبل از راه‌اندازی و هم پس از آن) درباره ریسک‌های متوجه جوانان و همچنین حمایت از حقوق آن‌ها.	●			●	

اصل راهبردی ۲: در نظر گرفتن ریسک‌های مربوط به حریم خصوصی کاربر و حفاظت از داده‌ها به عنوان بخشی از توسعه، پیاده‌سازی و ارزیابی مداوم رویکردهای احراز سن.

اصول و روش‌های احراز سن	چارچوب بهترین روش‌های DTSP			
بهترین روش‌ها	توسعه محصول	نظارت بر محصول	اجرای محصول	بهبود محصول	شفافیت محصول
حداقل‌سازی جمع‌آوری داده‌های شخصی برای احراز سن متناسب با ریسک ارزیابی‌شده و طراحی شیوه‌های سفارشی برای نگهداری، حذف و استفاده از داده‌ها.	●	●	●		
استفاده از داده‌های حساس جمع‌آوری‌شده صرفاً برای احراز سن و حذف سریع این داده‌ها پس از انجام احراز سن.		●	●		
برای جلوگیری از انتقال داده‌های شخصی به سرورهایی (از جمله سرورهای ارائه‌دهنده سرویس‌های دیجیتال) که خارج از کنترل کاربر هستند، تحلیل داده‌های شخصی در صورت امکان فقط روی دستگاه کاربر انجام گیرد.		●	●		
برای احراز سن، از روش‌های تخمین سن بر روی داده‌های جمع‌آوری شده استفاده شود تا از جمع‌آوری داده‌های شخصی جدید جلوگیری شود.		●	●		
در پیاده‌سازی احراز سن از طریق شرکت، تمام داده‌های شخصی جدید جمع‌آوری شده (مثلاً عکس‌های سلفی) فقط برای شرکت انجام دهنده احراز سن ارسال شوند، نه اینکه ابتدا برای ارائه‌دهنده سرویس‌های دیجیتال ارسال گردند.		●	●		
الزام شرکت‌ها به اعمال استانداردهای سطح بالای امنیت و حریم خصوصی و سپس اطمینان از بررسی و تأیید آن شرکت‌ها از این جهت که این استانداردها را رعایت می‌کنند.		●	●		
تکمیل ارزیابی تأثیر حفاظت از داده‌ها قبل از پیاده‌سازی هر روش جدید احراز سن (یعنی هر روش احراز سن، مانند پیوست فرهنگی، یک پیوست حفاظت از داده داشته باشد).	●	●			
در صورت امکان، اتکا به راه‌حل‌های تعامل‌پذیر احراز سن که مسئولیت ارائه اطلاعات اضافی به سرویس‌های جدید را به حداقل می‌رساند و ریسک‌های حفاظت از داده متوجه کاربر را کاهش می‌دهد.		●	●		

اصل راهبردی ۳: اطمینان از شمول و دسترسی‌پذیری تمام کاربران به رویکردهای احراز سن، صرف‌نظر از سن، وضعیت اجتماعی-اقتصادی، نژاد یا سایر ویژگی‌ها.

اصول و روش‌های احراز سن	چارچوب بهترین روش‌های DTSP			
بهترین روش‌ها	توسعه محصول	نظارت بر محصول	اجرای محصول	بهبود محصول	شفافیت محصول
تا آنجا که امکان‌پذیر است و با الزامات قانونی هم‌خوانی دارد، شرکت‌های تأیید سنی انتخاب شوند که گزینه‌هایی فراتر از اسناد شناسایی صادره از سوی دولت (که ممکن است برخی افراد نداشته باشند) مثل «گواهی تولد» و «کارت شناسایی مدرسه» (که همه دارند) یا «ترکیبی از یک شناسه حساب کاربری منحصر به فرد و تصویری از کاربر» را ارائه می‌دهند تا اطمینان حاصل شود که تأیید کاربران بدون دسترسی به مدارک شناسایی صادره از سوی دولت امکان‌پذیر است و تبعیضی صورت نمی‌گیرد.		●	●		
ارائه سازوکار در دسترس و با قابلیت استفاده آسان جهت ارسال درخواست تجدیدنظر برای آن دسته از کاربرانی که در روش تخمین سن با مشکل مواجه شده‌اند.			●		
انجام تحلیل تأثیرات قبل از به‌کارگیری تکنیک‌های تخمین سن برای جمعیت خاصی از کاربران جهت درک هرگونه پیامدهای تبعیض‌آمیز و کاهش آن‌ها.	●				
ارائه فرایند پرچم‌گذاری برای کاربران که یک کاربر زیر سن قانونی را گزارش دهند و ارائه دسترسی به کاربر مورد نظر جهت ارسال درخواست تجدیدنظر برای اثبات سن خود.			●		
بازبینی (بررسی) اجرای روش‌های احراز سن، از سوی شرکت‌های ثالث معتبر یا در صورت لزوم ارائه‌دهندگان سرویس‌ها.				●	
مشورت با اشخاص ثالث برای ارزیابی اثرات روش‌های مورد نظر برای احراز سن.	●	●			

اصل راهبردی ۴: انجام عملیات اجرایی لایه‌ای برای پیاده‌سازی رویکردهای احراز سن.

اصول و روش‌های احراز سن	چارچوب بهترین روش‌های DTSP				
بهترین روش‌ها	توسعه محصول	نظارت بر محصول	اجرای محصول	بهبود محصول	شفافیت محصول
قراردادن محدودیت‌های پیش‌فرض برای دسترسی و کار با سرویس (یا ویژگی‌های مشخص یا محتوایی خاص)؛ مشروط به وجود اعلان‌هایی درون خود محصول درباره تناسب سنی آن محتوا یا خدمت.			●	●	
برچسب‌گذاری کردن و در صورت لزوم، دسته‌بندی سرویس‌ها به‌عنوان سرویس‌های مناسب برای سنین خاص و هماهنگی با پلتفرم‌های توزیع به‌منظور اعمال محدودیت برای دانلود و دسترسی کاربران زیر سن قانونی.		●	●	●	
بررسی احراز سن برای وقتی که کاربر در خوداظهاری، سن خود را از «کمتر از ۱۸ سال» به «بالای ۱۸ سال» تغییر می‌دهد.			●	●	
تجزیه و تحلیل رفتار همه کاربرانی که در هنگام ایجاد حساب کاربری سن خود را اعلام می‌کنند، شناسایی کاربرانی که ممکن است اطلاعات نادرستی را وارد کرده و زیر سن قانونی باشند و بررسی پیوسته این کاربران با استفاده از آزمون‌های بیشتر احراز سن. پیام تبریک تولد ۱۱ سالگی خود کاربر یا تعامل بیشتر او با محتواهای مختص نوجوانان، نمونه‌هایی است از رفتارهایی که نشان‌دهنده نادرست بودن خوداظهاری سن هستند.			●	●	
آموزش تیم‌های اجرایی برای شناسایی نشانه‌هایی از کاربری که سن خود را اشتباه گزارش کرده است (مثلاً ظاهرشان نشان می‌دهد که جوان‌تر هستند) و به‌کارگیری روشی برای بررسی‌های بیشتر در زمینه احراز سن.			●	●	
ایجاد امکان ارسال گزارش کاربران نسبت به آن دسته از کاربرانی که سن خود را اشتباه گزارش کرده‌اند و بنابراین باید از سرویس‌ها یا ویژگی‌های خاصی محروم شوند.			●	●	
پیاده‌سازی روش‌های فنی به‌منظور ایجاد ممانعت برای دور زدن کنترل‌ها توسط کاربرانی که در آزمون احراز سن مردود شده و واجد شرایط تشخیص داده نشده‌اند (مثلاً ایجاد ممانعت برای ثبت‌نام فوری با استفاده از حساب کاربری دیگر).			●	●	
اجرای آزمون‌های جدید احراز سن برای کاربران موجود، وقتی که شرکت، فرایندهای احراز سن خود را بهبود بخشیده یا تغییر می‌دهد یا تغییرات مرتبطی را در محصول یا قابلیت‌های آن ایجاد می‌کند.			●	●	

اصول و روش‌های احراز سن	چارچوب بهترین روش‌های DTSP				
بهترین روش‌ها	توسعه محصول	نظارت بر محصول	اجرای محصول	بهبود محصول	شفافیت محصول
ارائه قابلیت حساب‌های خانوادگی همراه با راستی‌آزمایی والدین با اتصال حساب یک فرد جوان (زیر سن قانونی) به حساب والدین (یا قیم قانونی).		●	●	●	
ایجاد قابلیت تعیین الزامات سنی برای تعامل با محتوا یا انجمن‌های خاصِ درون یک سرویس، برای کاربران یا مدیران انجمن.		●	●	●	

اصل راهبردی ۵: اطمینان از شفافیت سیاست‌ها و روش‌های احراز سن برای عموم مردم و ارائه گزارش‌های دوره‌ای در مورد اقدامات انجام‌شده به عموم و سایر ذی‌نفعان.

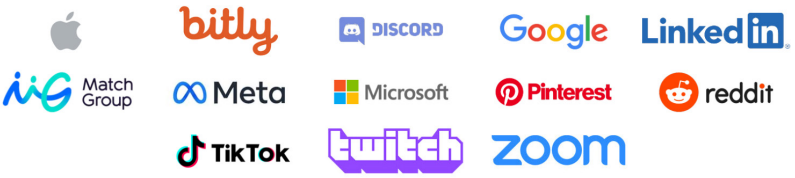
اصول و روش‌های احراز سن	چارچوب بهترین روش‌های DTSP				
بهترین روش‌ها	توسعه محصول	نظارت بر محصول	اجرای محصول	بهبود محصول	شفافیت محصول
توضیح درمورد این که چرا به عنوان بخشی از فرایند ثبت‌نام، سن یا تاریخ تولد کاربر، جمع‌آوری می‌شود.					●
پیاده‌سازی راهکارهای منبع‌باز احراز سن، به‌گونه‌ای که ذی‌نفعان و متخصصان بیرونی به‌راحتی بتوانند کدنویسی انجام شده را بررسی کنند.	●	●			●
فراهم کردن دسترسی محققان مستقل (بی‌طرف) به جزئیات پیاده‌سازی و داده‌های مربوط به اثربخشی احراز سن، به‌گونه‌ای که ارزیابی مناسب بودن روش مورد نظر توسط عاملان بیرونی امکان‌پذیر باشد.					●
انتشار داده‌های مربوط به هزینه‌ی روش‌های مختلف احراز سن برای ارائه‌دهندگان در مقیاس‌های مختلف.					●
انتشار مطالب در مرکز راهنمایی سرویس، مبنی بر مشارکت ارائه‌دهنده سرویس با شرکت احرازکننده سن، مشتمل بر داده‌های به اشتراک گذاشته شده با شرکت و مروری بر شیوه‌های کار با این داده‌ها توسط آن شرکت.		●			●
ارائه اطلاعات کمّی و کیفی درمورد اجرای سیاست‌ها و روش‌های احراز سن.					●

Digital Trust
& Safety Partnership

۷) معرفی مؤسسه اعتماد و ایمنی دیجیتال

«مؤسسه اعتماد و ایمنی دیجیتال» یک طرح ابتکاری است که با مشارکت تیم‌های «اعتماد و ایمنی»[۱] شرکت‌های خدمات دیجیتال پیشرو در جهان، به وجود آمده و بر ترویج اینترنت ایمن‌تر و قابل اعتمادتر متمرکز شده است. این مجموعه در سایت خود اعلام کرده که متعهد به توسعه، استفاده و ترویج بهترین روش‌های[۲] مورد استفاده در صنعت برای اطمینان از اعتماد و ایمنی کاربران خدمات دیجیتال هستند؛ روش‌هایی که از طریق ارزیابی‌های شخص ثالث (بی‌طرفانه) بررسی می‌شوند.

۱. Trust and Safety
۲. Best practices



شرکت‌های مشارکت‌کننده در طرح ابتکاری اعتماد و ایمنی دیجیتال

تیم‌های اعتماد و ایمنی در پلتفرم‌ها تلاش خود را صرف ایمن نگه داشتن کاربران از آسیب‌ها می‌کنند. جیسون سیترون، مدیرعامل پلتفرم دیسکورد، بیان می‌کند که کارشناسان اعتماد و ایمنی این پلتفرم، دسته‌های مختلف محتوا را در این پلتفرم رصد کرده و محتوای نامطلوب و غیرمجاز را شناسایی و گزارش می‌کنند. وی معتقد است این کارشناسان عناصر جدایی‌ناپذیر اقدامات این پلتفرم برای تقویت ایمنی کودکان و ایجاد محیط ایمن برای کاربران هستند.[۱] موضوع مهم در این عرصه این است که پلتفرم‌ها نیازمند رهنمودهایی برای اقدامات ایمنی‌بخش خود هستند. این در حالی است که «مؤسسه اعتماد و ایمنی دیجیتال» معتقد است که تابه‌حال، در حوزه اعتماد و ایمنی، انواع بهترین روش‌ها شناسایی نشده و همچنین ارزیابی‌هایی که برای بلوغ و ساماندهی حوزه‌های فناوری مانند امنیت سایبری حیاتی است، انجام نشده است و به همین دلیل است که شرکت‌های پیشرو در فناوری، در قالب این نهاد، گرد هم آمده‌اند تا این امر را محقق کنند.

«مؤسسه اعتماد و ایمنی دیجیتال» همچنین با حامیان مصرف‌کننده و کاربر، سیاست‌گذاران، مجریان قانون، سازمان‌های مردم‌نهاد مرتبط و کارشناسان مختلف در سراسر صنعت تعامل خواهد کرد تا بهترین روش‌ها را در عرصه اعتماد و ایمنی شناسایی کند.[۲]

۱. https://www.youtube.com/watch?v=a8waUqfalYg
۲. https://dtspartnership.org/

پایان

زاویه

نگاهی نو،
به حکمرانی فضای مجازی

نشانی: تهران، ضلع غربی میدان فلسطین، خیابان آیت‌الله طالقانی، پلاک ۳۹۷
تلفن: ۸۶۰۵۴۲۹۱-۰۲۱
وبسایت: www.zaviehmag.ir
شبکه‌های اجتماعی: @zaviehmag