



گسترش جهانی قوانین تأیید سن در فضای مجازی

بحث گسترش قوانین تأیید سن در فضای مجازی به یکی از جدی‌ترین مباحث حقوقی و سیاست‌گذاری دیجیتال در دهه اخیر تبدیل شده است.

بحث گسترش قوانین تأیید سن در فضای مجازی به یکی از جدی‌ترین مباحث حقوقی و سیاست‌گذاری دیجیتال در دهه اخیر تبدیل شده است.

به گزارش خبرنگار مهر؛ اینترنت، به عنوان یک بستر جهانی از یک سو فرصت‌های بی‌سابقه‌ای برای آموزش، ارتباط، تجارت الکترونیکی، سرگرمی و دسترسی به خدمات دولتی ایجاد کرده و از سوی دیگر، زمینه‌ساز تهدیدهای تازه برای کودکان و نوجوانان، از دسترسی به محتوای جنسی و خشونت‌آمیز گرفته تا مواجهه با تبلیغات هدفمند و حتی خطرات ناشی از هوش مصنوعی مولد، شده است.

این دوگانه فرصت و تهدید، سیاست‌گذاران را در موقعیتی دشوار قرار داده است. چگونه می‌توان همزمان از حقوق، سلامت روانی و امنیت کودکان در فضای آنلاین حمایت کرد و در عین حال به حریم خصوصی، آزادی‌های بنیادین و حق دسترسی آزاد بزرگسالان به اطلاعات لطمه وارد نکرد؟ این مسئله نه تنها به ابعاد حقوقی بلکه به پیامدهای اجتماعی، فرهنگی، اقتصادی و امنیتی نیز گره خورده است.

از همین روی، خبرنگار مهر در این نوشتار کوتاه با اتکا به برخی گزارش‌ها، قوانین و تجربیات برخی کشورها ابعاد چندلایه و پیچیده این موضوع مورد بررسی قرار می‌دهد.

مفهوم و کارکرد تأیید سن

تأیید سن (Age Verification) در شکل جدید خود به معنای بارگذاری اسناد رسمی هویتی، داده‌های بیومتریک یا استفاده از فناوری‌های نوینی چون تطبیق چهره و تحلیل صوتی توسط کاربر و به منظور اطمینان از سن او است. این رویکرد تفاوت جدی با مدل‌های اولیه تأیید سن، مانند انتخاب گزینه «بالای ۱۳ سال هستم» در چارچوب قانون «COPPA» یا «Children's Online Privacy Protection Act» مصوب ۱۹۹۸ در ایالات متحده دارد.

در دهه ۲۰۲۰، روند غالب احراز سن این بود که کاربران باید برای دسترسی به محتوا یا خدمات خاص، کارت شناسایی، گذرنامه، گواهینامه رانندگی یا اسکن چهره خود را در سامانه‌های تأیید شخص ثالث یا مستقیماً در پلتفرم‌های دیجیتال ثبت کنند. در چنین شرایطی، برخی کشورها حتی به سمت استفاده از فناوری‌های تحلیل رفتار آنلاین برای تشخیص سن تقریبی کاربران رفته‌اند. به زعم بسیاری از کارشناسان، این تغییرات، هرچند با هدف حفاظت از کودکان صورت گرفته، اما پرسش‌های جدی درباره امنیت داده، احتمال نشت اطلاعات حساس، ایجاد پایگاه‌های داده ملی از هویت دیجیتال افراد و پیامدهای اجتماعی و فرهنگی آن ایجاد کرده است.

ضرورت‌های تدوین قوانین تأیید سن

انگیزه اصلی قانون‌گذاران در بسیاری از کشورها، حفاظت از کودکان در برابر مواجهه با محتوای خطرناک است. محتوای هرزه‌نگاری، اطلاعات مربوط به مواد مخدر و محیط‌های پرخطر آنلاین از جمله تهدیدهایی هستند که بارها پیامدهای مرگباری برای کاربران زیر سن قانونی داشته‌اند.

برای نمونه، گزارش‌های مستندی وجود دارد که نوجوانان به دلیل دسترسی آزاد به شبکه‌های اجتماعی و خرید داروهای آلوده به فنتانیل جان خود را در بسیاری از کشورها از دست داده‌اند. این شواهد نشان می‌دهد که تأخیر در ایجاد محدودیت‌های مذکور می‌تواند آسیب‌های غیرقابل جبران به همراه داشته باشد و به همین دلیل، قانون‌گذاران تأیید سن را به عنوان سپری محافظتی ضروری تلقی می‌کنند.

علاوه بر محتوای پرخطر، فناوری‌های نوینی مانند چت بات‌های هوش مصنوعی نیز تهدیدهای تازه‌ای برای کاربران کودک و نوجوان ایجاد کرده‌اند. برخی از این سامانه‌ها با کودکان وارد گفت‌وگو می‌شوند و حتی آنان را به رفتارهای پرخطر یا تصمیمات

نادرست تشویق می کنند. این وضعیت موجب شده است که بحث محافظت از کودکان در مواجهه با هوش مصنوعی مولد جدی تر مطرح شود تا اطمینان حاصل گردد که ابزارهای دیجیتال نوین تنها در محیط های امن و کنترل شده برای کودکان در دسترس قرار می گیرند.

با وجود تمام نگرانی ها، اینترنت بستری ارزشمند برای آموزش، سلامت از راه دور و ارتباطات اجتماعی به شمار می رود. از همین روی، حذف کامل کاربران زیر سن قانونی از این فضا نه ممکن است و نه نتایج مطلوب در پی دارد. بنابراین قوانین تأیید سن تلاش می کنند میان این دوگانه تعادل برقرار کنند. رویکرد غالب آن است که دسترسی به برخی محتواهای پرخطر صرفاً برای افراد احراز هویت شده امکان پذیر باشد، در حالی که سایر کاربردهای مثبت و فرصت های آموزشی و ارتباطی همچنان برای همگان آزاد باقی بماند.

چالش های حقوقی و امنیتی

یکی از اصلی ترین نگرانی ها در اجرای قوانین تأیید سن، نقض احتمالی حریم خصوصی است. ذخیره سازی داده های بیومتریک یا اطلاعات هویتی مانند کارت شناسایی، همواره خطر نشت و سوءاستفاده از داده های حساس را به همراه دارد. نمونه افشای داده ها در برخی موارد نشان می دهد حتی پلتفرم هایی که مدعی بودند اطلاعات کاربران را ذخیره نمی کنند، در عمل دچار نقض گسترده امنیت می شوند. چنین رخدادهایی اعتماد عمومی را کاهش و نشان می دهد که خطر نقض حریم خصوصی در این حوزه جدی است.

مسئله دیگر، امکان استفاده ابزاری از داده های هویتی برای اهداف سیاسی یا امنیتی است. منتقدان مدعی هستند که حذف ناشناسی کاربران در برخی کشورها می تواند ابزاری برای سرکوب مخالفان و محدودسازی فعالیت های مدنی و سیاسی مشروع باشد. این امر حتی در دموکراسی های غربی نیز نمونه های مشهود و برجسته دارد.

همچنین چالش بعدی در این زمینه، فقدان تعریف واحد از مفهوم «محتوای مضر» است. به عنوان مثال، تفاوت تعاریف قانونی در ایالت های مختلف آمریکا و کشورهای گوناگون سبب شده است محتواهایی همچون برخی آموزش های جنسی در برخی مناطق به عنوان مضر تلقی شوند و محدود گردند. این امر نه تنها دسترسی آزاد به اطلاعات را تهدید می کند، بلکه می تواند چالش های دیگری برای جامعه ایجاد کند.

سرانجام، باید به ضعف های ذاتی در سازوکارهای اجرایی قوانین اشاره کرد. به ادعای بسیاری از متخصصان، تاکنون هیچ روشی برای تأیید سن ارائه نشده که همزمان کاملاً دقیق و در عین حال کاملاً مبتنی بر حریم خصوصی باشد. هر یک از روش های موجود یا از دقت کافی برخوردار نیستند یا ریسک های امنیتی بالایی به همراه دارند. این تناقض ذاتی، اجرای قوانین را پیچیده تر کرده و پرسش هایی اساسی درباره کارآمدی آنها ایجاد می نماید.

پیامدهای اجتماعی و سیاسی

منتقدان مدعی هستند که تضعیف ناشناسی آنلاین یکی از مهم ترین پیامدهای این نوع قوانین به شمار می رود. آن ها ادعا می کنند که حذف امکان ناشناس ماندن باعث می شود کاربران نتوانند به راحتی افشاگری های ضدفساد انجام دهند یا در فعالیت های مدنی و سیاسی مشارکت نمایند و این امر می تواند به کاهش اعتماد عمومی نسبت به فضای مجازی منجر شود.

همچنین، پیامد دیگر، تقویت بازار ابزارهای دور زدن محدودیت مانند «VPN» ها است. تجربیات حتی در کشورهای غربی و مدعی آزادی فضای مجازی، نشان می دهند که قوانین سخت گیرانه عملاً کاربران را به استفاده گسترده از این ابزارها سوق می دهند. هرچند این موضوع در ظاهر دسترسی آزاد را باز می گرداند، اما در عمل خود تبعات امنیتی تازه ای دارد، زیرا بسیاری از ابزار رایگان موجود برای دور زدن محدودیت های دسترسی ناامن هستند و می توانند زمینه نشت داده ها و حملات سایبری را فراهم کنند.

با وجود این نگرانی ها، اکثریت کارشناسان باور دارند که تصویب چنین قوانینی به واسطه آسیب های بی شمار موجود در بستر اینترنت برای کودکان و نوجوانان، حیاتی و اجتناب ناپذیر است. بنابراین، نمی توان انتقادات مطرح شده را مبنای تصمیم گیری سیاسی و تنظیم گری این حوزه قرار داد.

جمع بندی

در نهایت، می توان گسترش قوانین تأیید سن در فضای مجازی را نمایانگر تلاش دولت ها برای پاسخ به یکی از چالش های

اساسی عصر دیجیتال دانست: چگونه می توان کودکان را در برابر تهدیدهای اینترنتی حمایت کرد بدون آنکه آزادی بنیادین کاربران نقض شود؟

مرور تجربیات کشورهای جهان نشان می دهد که اجرای این قوانین، همواره با چالش های جدی در حوزه حریم خصوصی، آزادی بیان و امنیت داده ها همراه است. علاوه بر این، ابهام در تعاریف قانونی و اجرای فنی ناکارآمد می تواند پیامدهایی معکوس به همراه داشته باشد. به همین دلیل، در کنار راهکارهایی چون تأکید صرف بر تأیید سن مبتنی بر مدارک هویتی یا بیومتریک، باید به دنبال راه حل های ترکیبی مانند ارتقای سواد دیجیتال خانواده ها، ابزارهای کنترل والدین و چارچوب های حقوقی شفاف تر بود.

تنها با این رویکرد است که می توان میان حفاظت از کودکان و صیانت از دسترسی آزاد به محتوای آنلاین در فضای مجازی تعادل برقرار کرد.