ابعاد حقوقی نقض حریم‌خصوصی توسط فناوری‌های پوشیدنی هوش مصنوعی – تحلیل حقوقی و تطبیق رویکردها به سیاست‌گذاری

چکیده

گسترش روزافزون فناوری‌های پوشیدنی مبتنی بر هوش‌مصنوعی، افق‌های تازه‌ای در تعامل میان انسان و ماشین گشوده و درعین‌حال، چالش‌های عمیقی در زمینهٔ حریم‌خصوصی و حمایت از داده‌های شخصی پدیدآورده‌است که تاکنون در آثار پژوهشی فارسی کمتر مورد توجه قرارگرفته‌اند و در مقالهٔ حاضر، به‌عنوان نقطهٔ آغاز پژوهش‌های فارسی‌زبان در این حوزه، بررسی‌می‌شود. پرسش اصلی این است که رویکردهای مختلف سیاست‌گذاری تا چه اندازه می‌توانند از حریم خصوصی در برابر مخاطرات این فناوری‌ها حمایت کنند و میان این حمایت و آزادی نوآوری توازن برقرار سازند؟

هدف پژوهش، تبیین ابعاد حقوقی مخاطرات یادشده، ارزیابی تطبیقی رویکردهای سیاست‌گذاری و شناسایی الگوی مطلوب برای تنظیم‌گری این فناوری‌هاست. پژوهش حاضر با روش توصیفی-تحلیلی و با بهره‌گیری از تحلیل تطبیقی رویکردهای سیاست‌گذاری، بر پایه مطالعه اسنادی و کتابخانه‌ای منابع حقوقی و پژوهشی انجام شده استو رویکرد مطلوب از نظر نویسندگان معرفی‌شده‌است. یافته‌ها نشان‌می‌دهد نگرانی‌های ناشی از ذخیره‌سازی بلندمدت داده‌ها، نحوهٔ دسترسی اشخاص ثالث، مداخلهٔ دولت‌ها و حساسیت اطلاعات جمع‌آوری‌شده، ضرورت بازنگری در چارچوب‌های قانونی و مقرراتی موجود را با هدف افزایش کارآمدی حمایت از حریم خصوصی و متناسب‌سازی مداخلات تنظیم‌گرانه با سطح خطرات مطرح می‌سازد.پژوهش دو دسته راهکار برای صیانت از حریم‌خصوصی شناسایی‌می‌کند: نخست، راهکارهای غیرحقوقی همچون ارتقای سواد دیجیتال، خودتنظیمی کاربران و فشار هنجاری اجتماعی؛ دوم، راهکارهای حقوقی مبتنی بر سیاست‌گذاری‌های منعطف، تدریجی و متناسب با سطح واقعی خطرات و تحدید اختیارات دولت‌ها. در بخش سیاست‌گذاری، دو رویکرد اصلی مورد واکاوی قرار گرفته است: نخست، رویکرد قاعده‌گذاری پیشگیرانه یا پسینی؛ دوم، رویکرد محدودسازی داده‌ها. تحول در استانداردهای مسئولیت مدنی در دسترسی به داده‌های خصوصی از دیگر محورهای اساسی این تحلیل است. نهایتاً پژوهش بر ضرورت اتخاذ الگویی چندلایه و مشارکتی در سیاست‌گذاری تأکیددارد؛ الگویی که ضمن حفظ توازن میان امنیت داده و آزادی نوآوری، بر شفافیت نهادی، پاسخ‌گویی توسعه‌دهندگان و نظارت مستمر بر رعایت تعهدات مربوط به حریم‌خصوصی استواراست.

کلیدواژه‌ها: اینترنت اشیاء، فناوری‌های پوشیدنی، هوش‌مصنوعی، حریم‌خصوصی

مقدمه

موج بزرگ نوآوری مبتنی بر اینترنت آماده‌است تا تعامل انسان‌ها با جهان پیرامون‌شان را متحول‌کند. این پژوهش برخی از فرصت‌هایی که با ظهور اینترنت اشیاء[۱] بطور کلی و فناوری‌های پوشیدنی[۲] بطور خاص پدیدآمده‌اند، را مورد بررسی قرارمی‌دهد.

فناوری‌های پوشیدنی دستگاه‌های متصل به شبکه هستند که می‌توانند داده‌ها را جمع‌آوری، فعالیت‌ها را ردیابی و متناسب با نیازها و خواسته‌های کاربران شخصی‌سازی‌کنند و اگرچه با هوش مصنوعی از نظر مفهومی متمایزند، اما در بسیاری از کاربردهای نوین با یکدیگر پیوند می‌یابند. فناوری‌های پوشیدنی با گردآوری مستمر داده‌های مرتبط با وضعیت جسمانی، رفتار و فعالیت‌های کاربران، زمینه پردازش و تحلیل اطلاعات شخصی را فراهم می‌کنند؛ درحالی‌که به‌کارگیری الگوریتم‌های هوش مصنوعی در این ابزارها، قابلیت شناسایی الگوهای رفتاری و استنباط اطلاعات حساس یا پنهان از داده‌های اولیه را افزایش می‌دهد. ازاین‌رو، مخاطرات حریم خصوصی در این حوزه نه‌تنها از گردآوری و ذخیره‌سازی داده‌ها، بلکه از قابلیت‌های تحلیلی و استنباطی هوش مصنوعی و پیامدهای ناشی از آن‌ها نیز سرچشمه می‌گیرد. پژوهش حاضر با تمرکز بر این پیوند فناورانه، به بررسی ابعاد حقوقی مخاطرات یادشده و تحلیل رویکردهای سیاست‌گذاری در مواجهه با آن‌ها می‌پردازد. این فناوری‌ها بعنوان زیرمجموعه‌ای از اینترنت اشیاء، نسبت به سایر زیرمجموعه‌های این حوزه، سریع‌ترین رشد را داشته و انتظارمی‌رود در سال‌های آینده تأثیرات گسترده‌ای بر جامعه داشته‌باشند؛ اما همانند سایر فناوری‌های دیجیتال جدید، هنجارهای موجود را هم به‌چالش‌می‌کشند. بخصوص در حوزهٔ حقوقی، چالش‌هایی مربوط به حریم‌خصوصی و ایمنی را مطرح‌می‌کنند که مداخلات سیاست‌گذاری را ایجاب‌می‌کند.

---

۱. Internet of Things (IoT)

۲. Wearable technologies

در همین راستا در مقالهٔ حاضر پس از شناسایی مفاهیم مهم (شمارهٔ ۱) مصادیق نقض حریم‌خصوصی در فناوری‌های پوشیدنی مطرح‌می‌شوند (شمارهٔ ۲). در بخش تحلیلی، راه‌حل‌های حفظ حریم‌خصوصی در مورد فناوری‌های پوشیدنی معرفی‌می‌شوند (شمارهٔ ۳).

۱. مفهوم‌شناسی

در این قسمت ابتدا «اینترنت اشیاء» به عنوان مادر «فناوری‌های پوشیدنی» (شمارهٔ ۱-۱) و سپس بطور خاص «فناوری‌های پوشیدنی» مفهوم‌شناسی می‌شوند (شمارهٔ ۱-۲)

۱-۱. اینترنت اشیاء

«اینترنت اشیاء»، شبکه‌ای از اشیاء فیزیکی روزمره است که ما را احاطه‌کرده‌اند و به‌طور فزاینده‌ای در حال تجهیزشدن به فناوری‌هایی هستند که به آن‌ها امکان می‌دهد داده‌هایی دربارهٔ محیط اطراف خود جمع‌آوری کنند؛ سامانه‌ای متشکل از حسگرهای شبکه، محرک‌ها و اشیای هوشمند که هدف آنها اتصال همه چیز، از جمله اشیا، در زندگی است، به‌گونه‌ای‌که آنها را هوشمند، قابل برنامه‌ریزی و توانمندتر در تعامل با انسان و سایر ابزارها می‌نماید. این فناوری دستگاه‌های محاسباتی را قادرمی‌سازد که از طریق شبکه‌های سیمی یا غیرسیمی به رابط‌های دیگر (مانند انسانها و ماشین‌ها) متصل‌شوند تا با هدف جمع آوری داده‌ها، شبکه‌ای اطلاعاتی برای ارائه مدلهای تجاری، خدماتی و عملکردهای جدید الکترونیکی ایجادکنند.(Fornasier, 2019, 298–299) مختصراً «اینترنت اشیاء به مجموعه گسترده دستگاه‌های هوشمند گفته می‌شود که جمع‌آوری، پردازش داده‌ها و واکنش‌های هوشمند را ممکن می‌سازند.» (اکبریان طبری و جعفرزاده، ۱٤۰۵، ۲۸)

این دستگاه‌ها معمولاً به فناوری‌های حسگر، سامانه‌ها و قابلیت‌های ارتباط بی‌سیم (مانند وای‌فای[۱]، بلوتوث[۲]، ارتباط میدان نزدیک[۳] و جی‌پی‌اس[۴]) مجهزهستند(McLellan, 2013)، اغلب در پشت‌صحنه زندگی مصرف‌کنندگان فعالیت‌می‌کنند و تقریباً برای آن‌ها نامرئی‌اند و گاهی با سیستم‌های «هوشمند» مثل شهرهای هوشمند[۵]، هم‌معنا در نظر گرفته‌می‌شود.

برای ملموس‌شدن مفهوم اینترنت اشیا، رایانه‌هایی را درنظربگیرید که بدون کمک انسان و تنها با استفاده از داده‌هایی که خودشان جمع‌آوری‌می‌کنند، همه چیز را درباره اشیاء می‌دانند؛ آن‌گاه می‌توانستیم همه چیز را ردیابی و شمارش کنیم، میزان اتلاف، خرابی و هزینه‌ها را به‌طور چشمگیری کاهش‌دهیم. می‌دانستیم چه زمانی چیزی نیاز به تعویض یا تعمیر دارد و آیا چیزی تازه است یا از موعد مصرفش گذشته. ما باید رایانه‌ها را توانمندکنیم تا خودشان اطلاعات را گردآوری کنند. دولت‌ها در حال استقرار حسگرهایی هستند که در صورت خرابی در چراغ‌های خیابان، نشتی در سیستم‌های آب و سطل‌های زباله پُرشده به آن‌ها هشدارمی‌دهند. «میلیاردها دستگاه دیجیتال، از گوشی‌های هوشمند گرفته تا سنسورها در خانه‌ها، خودروها و ماشین‌های مختلف، با یکدیگر ارتباط برقرار خواهندکرد تا وظایف را خودکار کرده و زندگی را بهتر کنند.»(Lohr, 2013) در واقع اینترنت اشیاء دستگاه‌ها و برنامه‌های متصلی است که زندگی مصرف‌کنندگان را آسان‌تر، ایمن‌تر، سالم‌تر، ارزان‌تر و پربارتر می‌کنند (Shapiro & Chadwick, 2013, 7) و به مصرف‌کنندگان کمک‌می‌کنند کنترل بیشتری بر زندگی‌شان داشته‌باشند و با خودکارکردن وظایف و کارهای روزمره، از فناوری برای صرفه‌جویی در انرژی، افزایش کارایی، بهره‌وری، ایمنی عمومی، سلامت، آموزش و ... استفاده و وقت خود را آزادکنند.»(همان) بنابراین، جامعه به سرعت به نقطه‌ای نزدیک‌می‌شود که هر شخص و هر چیزی به شبکه متصل خواهدشد.

---

۱. Wi-Fi

۲. Bluetooth

۳. NFC

۴. GPS

۵. Smart cities

۲-۱. فناوری‌های پوشیدنی

فناوری‌های پوشیدنی یا پوشیدنی‌ها بعنوان زیرمجموعه‌ای از تکنولوژی‌های اینترنت اشیاء، به دستگاه‌های الکترونیکی عمدتاً مبتنی بر هوش مصنوعی اطلاق‌می‌شوند که برای پوشیدن روی بدن طراحی‌شده‌اند، شامل «دستگاه‌های هوشمند» متصل به شبکه با تراشه‌های میکرو، حسگرها و قابلیت‌های ارتباط بی‌سیم، تکنولوژی‌های پوشیدنیِ ابتدایی مانند ساعت‌های مچی حسابگر، سمعک‌ها و هدست‌های ارتباطی بلوتوث (Metz, 2014).

دستگاه‌های پوشیدنی ثبت دیجیتال در حوزه سلامت و تناسب اندام اکنون بطور گسترده‌ای برای پیگیری مستمر فعالیت روزانه و وضعیت سلامت، مقایسهٔ نتایج و دریافت بازخورد فوری مورد استفاده قرارمی‌گیرند(Bennett, 2014)؛ مانند دستبندهای تناسب‌اندام فیت‌بیت[۱] و جوبون[۲] یا پلتفرم گوگل‌فیت[۳] یا گوشی‌های جدید سامسونگ که ضربان قلب کاربر را اندازه‌گیری‌می‌کنند. (Warren, 2014) این دستگاه‌ها[۴] با اندازه‌گیری داده‌های مربوط به قند خون، دیابت، ریتم قلب، علائم حیاتی، حملات آسم، آپنه خواب، اختلالات خلقی، تعداد قدم‌ها و ... بطور مداوم، حتی در طول خواب و زمان‌های استرس شدید(Topol, 2012, 61–73)، با اطلاع‌رسانی به افراد یا ایجاد لرزش(Trew, 2014) به آن‌ها یادآوری‌می‌کنند که فعال‌تر باشند، داروهای خود را مصرف‌کنند یا با پزشک تماس‌بگیرند؛(Olivarez-Giles, 2014) بخصوص اطلاع‌رسانی به مراقبان و خانوادهٔ افراد مسن در مواقع اضطراری پزشکی.(Rojahn, 2014)

دستبندهای پوشیدنی که به افراد نابینا کمک‌می‌کند تا محیط اطراف خود را ناوبری‌کنند (Schofield, 2014)، لنزهای هوشمند با حسگرهای الکتروشیمیایی چشمی که به دیابتی‌ها

---

۱. FitBit

۲. Jawbone

۳. Google Fit

Ben Gilbert, Google Fit Is Android's Answer to Exercise and Health Tracking, ENGADGET (June 25, 2014), http://www.engadget.com/2014/06/25/google-fit, archived at http://perma.cc/FJM6-K55X.

۴. مثل حسگرهای MBAN (Medical Body Area Network) که امکان جمع‌آوری خودکار اطلاعات بیمار، مانند دما، از حسگر دماسنج پوشیدنی را فراهم‌می‌کنند.

کمک‌می‌کند سطح قند خون خود را پایش‌کنند (Guglielmo & Olson, 2014)، پارچه‌های غنی از حسگر و فیبرهای هادی[1]، استفادهٔ جراحان از فناوری پوشیدنی برای انجام بهتر جراحی‌های پیچیده و بخصوص از راه دور(Mead, 2013)، تجهیز آمبولانس‌ها به انواع دستگاه‌های اینترنت اشیاء برای تشخیص مشکل بیمار و سپس درمان فوری در دقایق حساس بعد از حادثه(Regan, 2014)، و ... دیگر نمونه‌های فناوری‌های پوشیدنی در حوزهٔ سلامت هستند.

فناوری‌های پوشیدنی برای افزایش راحتی اشخاص هم قابل‌استفاده هستند؛ مثلاً در خانه‌ها برای تنظیم تجربه‌های محیطی، مانند تنظیم خودکار نورپردازی، دما یا گزینه‌های تفریحی. (Wilson, 2013) کاربران آیفون‌ها و آیپدهای شرکت اپل می‌توانند مجموعه‌ای از دستگاه‌های متصل به اینترنت در خانه‌هایشان را کنترل‌کنند، از قفل‌های درب گرفته تا لامپ‌ها. (Mershon, 2014)

استفادهٔ آتش‌نشان‌ها از نمایشگرهای سر به بالا[2] با امکان دسترسی فوری به نقشه‌های ساختمان یا شرایط محیطی، برای پاسخگویی سریع‌تر به آتش‌سوزی‌ها و دیگر وضعیت‌های اضطراری هم از دیگر کاربردهاست. فناوری‌های پوشیدنی می‌توانند اجرای قانون را هم دگرگون‌کنند یعنی همانطور که مقامات قانونی می‌توانند با استفاده از آنها، گزارش‌های خود را مستندسازند، شهروندان معمولی نیز قادرباشند برای مقابله با رفتارهای سوءاستفاده‌گرانه مقامات قانونی، از فناوری پوشیدنی برای ثبت وقایع و نظارت بر فعالیت‌های آنان استفاده‌کنند. (Mann, 2012)

ارائه‌دهندگان خدمات تفریحی نیز قادرخواهندبود از فناوری‌های پوشیدنی برای خدمات خود برای کاربران استفاده‌کنند مثلاً دیزنی، مَجیک‌بند[3] را برای بازدیدکنندگان از پارک‌های تفریحی دیزنی ساخته‌است تا تجربه‌های خود را در این مراکز شخصی‌سازی کنند. (Panzarino,

---

[1] فیبرهای هادی، نوعی رشتهٔ نازک رسانای جریان برق هستند و در تولید لباس‌های هوشمند، پارچه‌های الکترونیکی و فناوری‌های پوشیدنی بکار می‌روند و امکان جمع‌آوری داده‌ها، انتقال سیگنال یا حتی روشن‌کردن قطعات الکترونیکی درون لباس را فراهم‌می‌کنند.

[2]. یا HUD، نمایشگری شفاف است که اطلاعات را مستقیماً در میدان دید کاربر نمایش‌می‌دهد تا نیازی به پایین‌انداختن سر و نگاه‌کردن به محل خاصی نباشد.

[3]. MagicBand

2013) برخی کارشناسان حتی پیش‌بینی می‌کنند که «اتومبیل می‌تواند نخستین رایانه پوشیدنی بزرگ باشد»(Gitlin, 2014).

لذا پوشیدنی‌ها ویژگی‌ها و قابلیت‌های بسیار شخصی‌تری نسبت به اینترنت اشیاء دارند.

تلفیق هوش مصنوعی با فناوری‌های پوشیدنی، این ابزارها را از وسایل صرفاً گردآورنده داده به سامانه‌هایی قادر به پردازش هوشمند اطلاعات تبدیل می‌کند. این تحول، ضمن گسترش کارکردهای فناوری‌های مزبور، مسائل حقوقی تازه‌ای را در خصوص حدود پردازش داده‌های شخصی، امکان پیش‌بینی رفتار کاربران و استنباط اطلاعاتی فراتر از داده‌های آشکار مطرح می‌سازد.

۲. *چالش‌های* حقوقی استفاده از فناوری‌های پوشیدنی

۲-۱. نقض مقررات مربوط به سلامت

پیشرفت فناوری‌های پوشیدنی، در زمینه حقوقی، چالش‌هایی درمورد مقررات بهداشتی و ایمنی ایجادخواهدکرد. مثلاً سازمان غذا و داروی ایالات‌متحده[۱] و سایر آژانس‌های دولتی، مقرراتی را در ارتباط با سلامت اشخاص وضع‌کرده‌اند که استفاده از فناوری‌های پوشیدنی می‌تواند با این مقررات در تضاد باشد. مثلاً پیش‌نویس راهنمای اف‌دی‌ای برای برنامه‌های پزشکی موبایل در ۲۰۱۳، برخی برنامه‌های سلامت‌محور موبایل را بعنوان «دستگاه‌های پزشکی[۲]» (برنامه‌هایی که اگر درست عمل نکنند، می‌توانند برای ایمنی بیمار خطرناک باشند) تحت نظارت قرارداده و برخی را از این دسته خارج کرده‌است. (FDA, 2013, 4) حتی قانونی هم مطرح‌شده‌است که اختیارات نظارتی اف‌دی‌ای را در این زمینه روشن‌تر کند. (Al-Faruque, 2014)

---

۱. FDA

۲. Medical devices

بعلاوه، ارائه‌دهندگان بیمه سلامت در حال آزمایش فناوری‌های پوشیدنی مربوط به سلامت هستند تا بتوانند طرح‌ها و بیمه‌های سفارشی و متناسب‌سازی شده به مشتریان خود ارائه‌دهند که خود این امر احتمالاً در آینده نیاز به نظارت قانونی را افزایش خواهدداد. (Olson, 2014)

با وجود چالش‌ها، محدودکردن استفاده از فناوری‌های پوشیدنی، ممکن‌است از لحاظ عملی و قانونی پیچیده شود چون اگر افراد زیادی با استفاده از این فناوری‌ها در تلاش برای ارتقای توانایی‌های بدنی خود باشند، اینکه قانون استفاده از این فناوری‌ها را محدودکند، خلاف خواست عمومی خواهدشد. لذا مسئله نیاز به پاسخ‌های دقیق‌تر و جامع‌تر در زمینه سیاست‌گذاری و نظارت خواهدداشت.

۲-۲. نقض حریم‌خصوصی در فناوری‌های پوشیدنی

حجم گستردهٔ اطلاعاتی که فناوری‌های پوشیدنی می‌توانند گردآوری کنند، نگرانی‌های مرتبط با حریم‌خصوصی را افزایش‌داده‌است. کاربران از تنظیمات شخصی‌سازی‌شده در این فناوری‌ها لذت‌می‌برند، اما همین قابلیت‌ها، خطرهای مربوط به حریم‌خصوصی دیجیتال را هم تشدیدمی‌کنند. (Collins et al., 2014, 6) مثلاً عینک گوگل (گوگل‌گلس)[۱]، به‌عنوان یک ابزار «زندگی‌نگاری»، به کاربران امکان‌می‌دهد تا به‌طور خودکار هر ۳۰ ثانیه از فعالیت‌های روزانه خود عکس بگیرند(Thompson, 2013). یا انواع میکروفوتوگرافی‌های پوشیدنی[۲]که به کاربران امکان‌می‌دهند در فواصل زمانی منظم عکس بگیرند و به زودی احتمالاً قادر به پخش زنده صوت و تصویر نیز خواهندبود.(Dickson, 2014) اهمیت داده‌ها و حریم خصوصی افراد به نحوی است که در پژوهشی، در زمینهٔ قانونگذاری ۱۰ کشور در حوزه هوش‌مصنوعی، تنها موضوعی که همه کشورها در خصوص آن قانونگذاری کرده بودند مالکیت داده و حریم خصوصی بود. (صادقی و جوادی پارسا، ۱٤۰۵، ۲۱۸)

---

۱. Google Glass

۲ مثل: Butterfleye، Autographer و CA7CH Lightbox

نگرانی‌های حریم‌خصوصی مثل اینکه این دستگاه‌ها چه مقدار داده از کاربران جمع‌آوری می‌کنند؟(Kelly, 2013) داده‌ها برای چه مدت نگهداری خواهندشد و چه کسانی ممکن‌است به این اطلاعات دسترسی داشته‌باشند؟ (Carter, 2014) پاسخ به این سوالات دقیقاً مشخص نیست اما سه نکتهٔ مهم وجوددارد:

الف) نگرانی‌های مربوط به حریم‌خصوصی در فناوری‌های پوشیدنی تنها به کاربران مستقیم این فناوری‌ها محدودنمی‌شود، بلکه افراد حاضر در محیط را نیز دربرمی‌گیرد (یعنی افراد حاضر در محیط‌هایی که دیگران از فناوری‌های پوشیدنی استفاده‌می‌کنند). این افراد ممکن‌است بر نحوهٔ ثبت رفتارها یا داده‌هایشان توسط این فناوری‌ها کنترل‌نداشته‌باشند و اخذ رضایت آگاهانه برای از آن‌ها، غیرممکن یا دشوارباشد. دستگاه‌های پوشیدنی می‌توانند حجم عظیمی از داده‌ها را درباره آن‌ها رصد، جمع‌آوری و به اشتراک بگذارند، آنهم گاه بدون آگاهی یا رضایت صریح آن‌ها.

ب) چنین داده‌هایی ممکن‌است بسیار حساس باشند (به‌ویژه اطلاعات مرتبط با سلامت یا شرایط خاص پزشکی) یا مورد استفادهٔ اشخاص ثالث با اهداف بازاریابی، کارفرمایان برای مقاصد شغلی، یا شرکت‌های بیمه برای تنظیم حق بیمهٔ افراد، قرارگیرند که خطر استفادهٔ تبعیض‌آمیز از داده‌ها را ایجادمی‌کند.(Helm & Georgatos, 2014, 156)

ج) استفاده از تکنولوژی‌های پوشیدنی ممکن‌است حریم‌خصوصی را در تقابل با ارزش‌های دیگری چون آزادی بیان، حقوق مطبوعات و جریان آزاد اطلاعات قراردهد؛ تقابلی که بطور سنتی وجودداشته‌است و با ظهور این تکنولوژی‌ها به‌طور قابل‌توجهی تشدیدخواهدشد.[1] جمع‌آوری داده‌ها و ضبط‌های صوتی و تصویری، بخشی از حق آزادی بیان و مطبوعات است؛ عمل ضبط یک فایل صوتی یا تصویری در ذات خود جزو حقوقی است که برای انتشار این ضبط‌ها لازم است. اگر این عمل (به بهانهٔ حریم‌خصوصی) به‌طور کامل محافظت نشود، حق نشر یا پخش نیز به‌طور قابل‌توجهی آسیب‌خواهددید. مثلاً ممنوعیت عکاسی یا یادداشت‌برداری

[1]. بعنوان مثال در آمریکا این محدودیت‌ها می‌تواند در تعارض با متمم اول قانون اساسی این کشور باشد.

در یک رویداد عمومی که به‌طور آشکار بر حق نشر عکس‌های حاصل یا انتشار گزارش مستخرج از یادداشت‌ها تأثیرخواهدگذاشت.(ACLU v. Alvarez, 2012, 595–596)

البته مدافعان آزادی بیان معتقد به حذف کامل محدودیت‌های مرتبط با حریم‌خصوصی نیستند. برخی از قوانین در دنیا قبلاً هم وجود داشته‌اند که جمع‌آوری اطلاعات را در زمینه‌های حساس محدودمی‌کنند. مثلاً اگرچه شهروندان آزادی‌های گسترده‌ای برای استفاده از دوربین‌ها و دستگاه‌های ضبط در مکان‌های عمومی دارند، اما قوانین حریم‌خصوصی جلوی ضبط مخفیانه و مزاحم در مکان‌های خصوصی و برخی مکان‌های عمومی را می‌گیرند (Bambauer, n.d., 267–268)

۲-۳. راه‌حل‌های حفظ حریم‌خصوصی در رابطه با فناوری‌های پوشیدنی

راه‌حل‌ها را می توان به دو دسته حقوقی (سیاست‌گذاری) و غیر حقوقی تقسیم کرد. در این شماره ابتدا راهکارهای غیر حقوقی مطرح‌می‌شوند (شماره ۳,۱) و سپس رویکردها به سیاست‌گذاری در مورد فناوری‌های پوشیدنی مورد بررسی قرارمی‌گیرند (شماره ۳,۲)

۲-۴. راه‌حل‌های غیر حقوقی

۲-۴-۱. سازگاری اجتماعی و فردی با اختراعات جدید

نگرش مردم نسبت به فناوری‌های جدید احتمالاً چرخه‌ای تکراری را طی‌خواهدکرد: مقاومت اولیه، سازگاری تدریجی و در نهایت همگرایی و پذیرش کامل در جامعه. (Permissionless Innovation, n.d., 53) مردم معمولاً رابطه خود با فناوری‌های جدید را با موضعی دفاعی آغاز می‌کنند. در حالت شدید، مقاومت اولیه ممکن‌است بصورت تکنوپانیک (وحشت از فناوری) ظاهرشود. (Thierer, 2014) اما با گذر زمان، معمولاً یادمی‌گیرند که چگونه با فناوری‌های جدید سازگار شوند یا دست‌کم در برابر چالش‌های آن، تاب‌آوری بیشتری نشان‌دهند. تاب‌آوری

پذیرفته شده در انتظار انتشار | ویراستاری نشده
Accepted | Awaiting Publication | Draft Version | Unedited

«ظرفیت یک سیستم، سازمان یا فرد برای حفظ هدف اصلی و یکپارچگی و تطبیق خود در مواجهه با شرایط به شدت تغییریافته» است.(Zolli & Healy, 2012, 7)

بسیاری از مردم با بدبینی و با خواستِ داشتن قطعیت بیشتر درباره آینده، باوردارند که برنامه‌ریزی پیشگیرانه کافی، می‌تواند بدترین سناریوها را پیش‌بینی و بر آن‌ها غلبه کند.(Gardner, 2010, 141) اما نظام‌های فناورانه و اجتماعی به‌طور مستقل از هم توسعه نمی‌یابند، بلکه یکدیگر را شکل‌می‌دهند و در قالب چرخه‌های بازخوردی پیچیده با هم تکامل می‌یابند و هر یک باعث تحریک، مهار یا شتاب‌بخشی در تغییر دیگری می‌شود(Brown & Duguid, 2001, 79, 82,۸۳) این فرآیند باعث‌می‌شود انسان‌ها در مواجهه با تغییرات فناورانه گسترده، تاب‌آورتر شوند و رشد کنند. (Permissionless Innovation, n.d., viii) شهروندان باید نسبت به اشکال نوظهور تغییر فناورانه ذهنی باز و خلاقانه داشته باشند چون چنین رویکردی فضایی برای نوآوری فراهم‌می‌کند. هرچند ممکن‌است در این مسیر برخی چیزها ازدست‌بروند، اما اغلب دستاوردهای ارزشمندتری مثل تجربه برای مقابله با آشفتگی‌های بعدی، به‌دست‌می‌آید. مثلاً الآن خیلی افراد گسترش عکاسی عمومی را محکوم‌می‌کنند و معتقدند «عکس‌های فوری و فعالیت‌های رسانه‌ای، به حریم مقدس زندگی خصوصی و خانوادگی تجاوز کرده‌اند» (Warren & Brandeis, 1890, 195) اما در مقابل، هنجارهای فردی و نگرش‌های فرهنگی هم به‌سرعت تحول یافته‌اند؛ چرا که دوربین‌ها به بخشی اساسی از تجربه انسانی تبدیل‌شده‌اند. در همین حال، هنجارهای اجتماعی نیز برای مواجهه با استفادهٔ نامناسب از دوربین‌ها و نقض حریم‌خصوصی، بصورت تدریجی تکامل یافته‌اند. یعنی شهروندان توانسته‌اند واکنش نشان‌دهند، تطبیق یابند و در برابر چالش فناورانه، تاب‌آورتر شوند.

براساس این راه‌حل، به‌مرور زمان مجموعه‌ای از عوامل فرهنگی، اجتماعی و هنجاری شکل‌می‌گیرند؛ افراد و جوامع به‌تدریج تاب‌آور و سپس با فناوری‌های جدید عصر خود سازگارمی‌شوند و در نهایت، سازوکارهایی برای کنار آمدن با آن پیدامی‌کنند.

البته تاب‌آوری نباید با بی‌تفاوتی نسبت به مسائل حریم‌خصوصی و امنیت اشتباه گرفته‌شود. بهرحال در کوتاه‌مدت، فناوری‌های پوشیدنی تنش‌های اجتماعی جدی‌ای ایجاد خواهندکرد که نیازمند پاسخ‌های جدی هستند. (Thierer, 2013)

۲-۴-۲. هنجارها و فشار اجتماعی

فشار عمومی خودجوش و هنجارها، بعنوان نگرش‌هایی اجتماعی که مشخص‌می‌کنند چه کاری باید انجام‌شود و چه کاری نباید انجام‌شود(Sunstein, 1996, 914)، می‌توانند نقشی قدرتمند در محدودکردن رفتارهای مشکل‌ساز از سوی توسعه‌دهندگان فناوری‌های پوشیدنی و کاربران آن ایفاکنند و گاه، تنظیم‌کننده‌ای بسیار قدرتمندتر از قوانین و مقررات برای نحوه استفاده مردم از ابزارهای جدید می‌شوند. (Permissionless Innovation, n.d., 57–58)

گرچه هنجارها گاهی به‌شکل محدودیت‌های رسمی که خود مؤسسات اعمال می‌کنند ظاهرمی‌شوند، ولی اغلب بصورت طبیعی و از پایین به بالا و به‌صورت خودجوش از سوی افراد شکل‌می‌گیرند. مثلاً در خیلی از کشورها هنجارهای اجتماعی، مخالف استفاده از تلفن‌های هوشمند در محیط‌هایی مانند رستوران‌ها، سینماها و اتاق‌های رختکن باشگاه‌های ورزشی، هستند. مثلاً سینماها از پیام‌های پیش از نمایش برای فشارآوردن به تماشاگران برای خاموش‌کردن یا بی‌صداکردن دستگاه‌های الکترونیکی استفاده‌می‌کنند، اما تماشاگران هم ممکن‌است نارضایتی خود را از وقفه‌های ایجادشده به فرد متخلف نشان‌دهند.(Mallozzi, 2011, A17) یا مراکز ورزشی اغلب با نصب تابلوهایی استفاده از تلفن‌های هوشمند در اتاق‌های رختکن را ممنوع می‌کنند، ولی استفاده‌کننده، احتمالاً به سرعت با خشم مشتریان ناراضی هم روبه‌رو خواهدشد. (Newman, 2013)

در نهایت، توجه رسانه‌ها نیز نقش مهمی در کاهش رفتارهای بالقوه مشکل‌ساز ایفامی‌کند. در سال‌های اخیر، رسانه‌های معتبر به مسائل حریم‌خصوصی مصرف‌کنندگان توجه بیشتری کرده‌اند و از افراط در برخی روش‌های جمع‌آوری داده‌ها پرده‌برداشته‌اند.(Ramirez, 2014, 12)

۳-۴-۲. افزایش سواد دیجیتال

واقعیت این است که «ما در جامعه‌ای «چشم‌چران» زندگی می‌کنیم: فناوری‌های نوین ابزارهای قدرتمندی برای نفوذ به حریم‌خصوصی را در اختیار افراد عادی قرارداده‌اند.» (Friedman, n.d., 259, 269) لذا یکی از راه‌حل‌های غیرحقوقی برای رفع نگرانی‌های مربوط به حریم‌خصوصی ناشی از فناوری‌های پوشیدنی، افزایش آگاهی عمومی از طریق برنامه‌های آموزشی درباره پیامدهای منفی احتمالی این فناوری‌ها و تمایز میان کاربردهای مناسب و نامناسب آن‌هاست. (Beales, Craswell, & Salop, 1981, 531)

سواد دیجیتال (یعنی درک چگونگی گردآوری، اشتراک‌گذاری و استفاده از داده‌های شخصی) کمک می‌کند تا افراد خطرات احتمالی اشتراک‌گذاری بیش‌ازحد اطلاعات خود و دیگران را بهتر درک‌کنند و هر از گاهی اطلاعات غیرضروری آنلاین و ردپای دیجیتالی خود را پاک کرده یا به شیوه‌های دیگر بپوشانند. (Collier, 2009; Magid, 2010)

درست مانند حریم‌خصوصی آنلاین، در سال‌های نخستِ مطرح‌شدنِ مباحثِ ایمنی کودکان در اینترنت، سیاست‌گذاری‌ها عمدتاً بر راه‌حل‌های بالا به پایین (مثلاً سانسور محتوای نامناسب) تمرکزداشتند(Precautionary Principle, n.d., 479–482) که با چالش‌های فنی و حقوقی مواجه‌شدند: از منظر فنی، طراحی مکانیزم‌های فیلترینگ کارآمد برای اینترنت بسیار دشوار و دست‌نیافتنی بود. از منظر حقوقی نیز، محدودیت‌هایی مثل آزادی بیان باعث‌می‌شد تدوین محدودیت‌های قانونی امکان‌پذیر نباشد. (Klosowski, 2014)

لذا پس از سال‌ها ناکامی در تحمیل چنین محدودیت‌هایی، سیاست‌گذاران، تمرکز خود را به‌جای مقررات‌گذاری، بر راه‌حل‌های آموزشی و توانمندسازی کاربران معطوف‌کردند. (Thierer, 2009, 1–2)

راهبردهایی چون «سواد رسانه‌ای»، مهارت‌های تفکر انتقادی، مفهوم «شهروندی دیجیتال» (اهمیت آموزش رفتار درست در فضای مجازی یا همان «آداب اینترنتی»[۱])، (Common Sense

[۱]. Netiquette

Media, 2009, 1 نحوهٔ تعامل صحیح با رسانه‌های اجتماعی، مدیریت شهرت دیجیتال، انتخاب گذرواژه‌های قوی و...

ضرورت به‌رسمیت شناختن «سواد دیجیتال به‌عنوان یکی از مهارت‌های حیاتی قرن بیست‌ویکم» در گزارش دولت وقت آمریکا منعکس‌شده‌است: «برای اطمینان از اینکه دانش‌آموزان، شهروندان و مصرف‌کنندگان در هر سنی بتوانند از خود در برابر سوءاستفاده از داده‌ها محافظت‌کنند، ضروری است که مهارت درک نحوه گردآوری و اشتراک‌گذاری داده‌ها، نحوه و هدف به‌کارگیری الگوریتم‌ها و ابزارها و روش‌های حفاظت از خود را فرا بگیرند. اگرچه این مهارت‌ها جایگزین حمایت‌های قانونی نخواهندشد، اما به افراد کمک‌می‌کند تا بهتر در جهانی آکنده از داده زندگی‌کنند.(Fordham Center on Law & Information Policy, 2013)»

کمیسیون تجارت فدرال آمریکا[۱] آموزش به مصرف‌کنندگان و کسب‌وکارها را نخستین خط دفاعی در برابر کلاهبرداری و فریب می‌داند (U.S. Federal Trade Commission, 2009, 4) و با همکاری بیش از دوازده نهاد فدرال دیگر وب‌سایتی را راه‌اندازی و پشتیبانی کرده که مجموعه‌ای از توصیه‌ها و نکات مربوط به امنیت، ایمنی و حریم‌خصوصی را برای مصرف‌کنندگان و کسب‌وکارها ارائه‌می‌دهد.(Onguard Online, n.d) .

۴-۴-۲. خودتنظیمی

حریم‌خصوصی و امنیت داده‌ها در حوزه فناوری‌های پوشیدنی می‌تواند از طریق خودتنظیمی[۲] نیز مدیریت‌شود (Bracy, 2014) یعنی مسئولیت‌پذیری و امانت‌داری سازمان‌ها در قبال اطلاعاتی که جمع‌آوری و استفاده می‌کنند: حفظ امنیت داده‌ها، شفافیت و صراحت در مورد نحوه استفاده از داده‌ها و استفاده نکردن از آن‌ها به روشی که به منافع کاربران آسیب‌برساند یا به ضرر آن‌ها باشد، بدون کسب رضایت صریح آن‌ها. این مسئولیت‌ها در تقریباً تمامی کدهای حریم‌خصوصی

---

۱. Federal Trade Commission [FTC]

۲. Self-regulation

و سیاست‌های حریم‌خصوصی بزرگ‌ترین شرکت‌های اینترنتی دیده‌می‌شود.(Wasch, n.d., p. 8)

مزایای خودتنظیمی عبارتند از:

الف) برای توسعه‌دهندگان فناوری: «تنها از طریق طراحی راه‌حل‌هایی که به‌روشنی احترام به حریم‌خصوصی افراد را نشان‌دهند و اختصاص منابع کافی برای آگاه‌سازی و تبیین فناوری برای عموم مردم است که شرکت‌ها می‌توانند به پذیرش گسترده فناوری‌های اینترنت اشیاء امیدوار باشند.» (INFSO D.4 Networked Enterprise & RFID)

ب) «در مقایسه با مقررات‌گذاری سنتی از سوی دولت، خودتنظیمی این پتانسیل را دارد که در مواجهه با تغییرات مدل‌های کسب‌وکار یا فناوری‌ها، پاسخ‌گوتر، انعطاف‌پذیرتر و سریع‌تر عمل‌کند.»(Ohlhausen, 2014, 3)

ج) «نسبت به سیستم‌های مقرراتی کلان که برای اصلاحشان باید قانون‌گذاری سازمانی صورت‌گیرد، بازطراحی آن آسان‌تر است.»(همان)

د) «در مقایسه با فرآیندهای رسمی حقوقی، می‌تواند سازوکاری کم‌تنش‌تر و کارآمدتر برای حل اختلافات فراهم کند.»

و) با استفاده از آن «می‌توان منابع نظارتی دولتی را برای موارد شدید آسیب به مصرف‌کننده حفظ کرد.»

ه) «هزینه‌های فرآیند خودتنظیمی بر عهده شرکت‌هاست، نه مالیات‌دهندگان.»(همان)

ی) «در برخی از فعالیت‌ها بخصوص فناوری‌های پوشیدنی که مداخله دولت به‌دلیل محدودیت‌های ناشی از آزادی بیان امکان‌پذیر نیست، خودتنظیمی ممکن‌است تنها گزینهٔ موجود باشد (همان) که می‌تواند به شکل «حریم‌خصوصی از ابتدا[1]» باشد، یعنی تلاش‌های توسعه‌دهندگان برای «گنجاندن» برخی شیوه‌های حفاظتی حریم‌خصوصی و امنیتی در زمان طراحی و پیاده‌سازی فناوری‌های جدید. (Cavoukian, 2012, 4)

[1]. Privacy by design

گرچه ترس از مسئولیت قانونی و فشار مقامات دولتی می‌تواند، دو توضیح احتمالی برای خودتنظیمی داوطلبانه باشد، اما اغلب این امر به سود کسب‌وکار خود توسعه‌دهنده برمی‌گردد. بسیاری از مشتریان بالقوه، به حریم‌خصوصی و امنیت دستگاه‌های پوشیدنی خود اهمیت زیادی می‌دهند.(The Economist, 2014) در اقتصاد سخت کنونی، کسب‌وکارهای موفق بیشتر به اعتماد مشتریان خود در مورد محصولات و خدماتشان اهمیت‌می‌دهند. اگر شرکتی در این اعتمادسازی شکست بخورد، عواقب بازار مالی اغلب سریع و قاطع خواهدبود (مثلاً افت قیمت سهام شرکت) و شرکت را مجبور می‌کند تا به سرعت رویه‌های تجاری خود را با انتظارات مصرف‌کننده همسوکند. آخرین چیزی که توسعه‌دهندگان می‌خواهند واکنش منفی مصرف‌کنندگان یا توجه رسانه‌ها به دلیل مشکلات مربوط به حریم‌خصوصی یا امنیت داده‌ها است. درست است که «خاطیان باید مجازات شوند، اما بهترین راه برای ایمن‌سازی اینترنت اشیا، رقابت است. یا شرکت‌های فناوری راه‌هایی برای قابل اعتمادتر کردن گجت‌های وب‌محور پیدا می‌کنند، یا مردم تصمیم‌می‌گیرند که می‌توانند بدون آنها زندگی‌کنند.»(The Economist, 2014)

چندین گام عملی برای خودتنظیمی توسعه‌دهندگان فناوری‌های پوشیدنی وجود دارد:

۱) **راهنماهای استفاده صحیح**: باید با درج هشدارهای واضحی در بسته‌بندی محصولات، خطرات استفاده نادرست از فناوری‌های خود را به مالکان جدید توضیح‌دهند.

۲) **شفافیت**: باید داده‌هایی را که دستگاه‌هایشان درباره مصرف‌کنندگان جمع‌آوری‌می‌کنند، کاربردهای این داده‌ها، اینکه آیا داده‌های جمع‌آوری‌شده توسط دستگاه‌هایشان توسط شرکت ذخیره‌می‌شود و اگر می‌شود، این داده‌ها ممکن‌است با چه کسانی به اشتراک گذاشته‌شوند، را بخصوص در وب‌سایت‌های خود به‌وضوح اعلام کنند.(Ramirez, n.d., p. 4)

۳) **انتقال یا حداقل‌سازی داده‌ها**: باید فرآیند انتقال یا حذف داده‌ها به هنگام درخواست کاربران را آسان‌تر کنند و نیز داده‌های غیرضروری که ممکن‌است در آینده آسیب‌های حریم‌خصوصی یا امنیتی ایجاد کنند، به حداقل رسانده یا حذف‌کنند.

Accepted Article | Publication Draft Version | Under Publication

٤) **اطلاع‌رسانی و به‌روزرسانی‌های نرم‌افزاری امنیتی مداوم**: اینکار برای اطمینان از برطرف‌شدن آسیب‌پذیری‌ها و جلوگیری از اقدامات هکرها، ضروری‌است.

٥) **امنیت بهتر از طریق رمزنگاری**: رمزنگاری، ناشناس‌سازی و شناسایی‌زدایی داده‌ها (ذخیره‌سازی و به اشتراک‌گذاری داده‌ها بدون افشای هویت افراد درگیر) (Cavoukian & Castro, 2014, 1) نیز اهمیت زیادی دارد(Barth-Jones, 2014).

بهرحال خود تنظیمی راه‌حلی کامل نیست و نمی‌تواند به‌طور کامل جایگزین مقررات شود و باید با اجرای قانون پشتیبانی‌شود.

۳. راه‌حل‌های حقوقی

۱-۳. رویکردها به سیاست‌گذاری در مورد فناوری‌های پوشیدنی)

گرچه فناوری‌های پوشیدنی پتانسیل‌های زیادی برای بهبود کیفیت زندگی دارند، اما نگرانی‌هایی از جمله امنیت داده‌ها، حریم‌خصوصی و دسترسی غیرمجاز به اطلاعات کاربران، حقوق مالکیت داده‌ها، استفاده‌های تجاری از اطلاعات شخصی و چگونگی نظارت نیز در مورد آنها وجوددارند که مدیریت آنها را یکی از چالش‌های اساسی سیاست‌گذاران و نهادهای نظارتی تبدیل و نوعی رویکرد نظارتی جامع و دقیق برای تنظیم آنها ضروری کرده‌است. این رویکرد باید به گونه‌ای باشد که هم از نوآوری‌ها حمایت‌کند و هم از خطرات احتمالی آنها جلوگیری نماید. در این زمینه چندین مدل رویکرد سیاست‌گذاری در دنیا و بخصوص ایالات‌متحدهٔآمریکا به چشم می‌خورد که بررسی تطبیقی آن‌ها می‌تواند برای سیاست‌گذاری آینده در ایران مفیدباشد:

۱-۱-۳. رویکردهای قاعده‌گذاریِ پیشگیرانه یا پسینی

دو رویکرد سیاستی اصلی وجود دارد: نوآوری بدون نیاز مجوز[۱] و اصل احتیاط[۲] که به شدت با یکدیگر در تضاد هستند. طبق رویکرد نخست محدودیت‌های زیاد می‌توانند نوآوری را کاهش‌دهند و مانع از دستاوردهای جدید شوند؛ لذا پیشرفت‌های فناوری باید آزادانه و بدون دخالت‌های دولتی یا نظارتی انجام‌شود تا نوآوری به حداکثر برسد. (Permissionless Innovation, n.d., vii)

از سوی دیگر، طبق رویکرد اصل احتیاط یا پیشگیرانه، باید پیش از پذیرش فناوری‌های جدید، خطرات بالقوه آن‌ها به دقت ارزیابی‌شوند. حفاظت از سلامت عمومی، حریم‌خصوصی و امنیت شهروندان باید در اولویت قرار گیرد و به همین دلیل ممکن‌است نیاز به مقررات شدید برای کنترل استفاده از فناوری‌های نوین باشد. (Weaver, 2014)

رویکرد اول از آزمایشات آزاد و بدون مداخله حمایت می‌کند تا توسعه و پیشرفت فناوری‌های جدید به سرعت و بطور طبیعی رخ‌دهد، اما اصل احتیاط به کنترل و نظارت بر فناوری‌های نوین تأکید دارد تا از خطرات و عواقب نامطلوب آن‌ها جلوگیری کند و ممکن‌است با ایجاد محدودیت‌هایی برای این فناوری‌ها، به عنوان یک عامل بازدارنده عمل کند.

لذا بحث اصلی این است که چگونه می‌توان این دو رویکرد را متوازن کرد تا هم از نوآوری حمایت و هم از خطرات آن جلوگیری گردد؟

در اینجا یک پرسش اساسی به نام «سوال مجوز[۳]» وجوددارد: آیا پیش از بهره‌برداری از فناوری‌ها، باید از مقامات عمومی مجوز دریافت شود؟

در پاسخ به این سؤال، طبق رویکرد احتیاط، نوآوری‌ها باید محدود یا ممنوع شوند تا زمانیکه توسعه‌دهندگان آن‌ها ثابت‌کنند که هیچ‌گونه آسیبی به افراد، گروه‌ها، نهادهای خاص، هنجارهای فرهنگی یا قوانین و سنت‌های موجود واردنمی‌کنند. سیاست‌گذاران باید فناوری‌های

---

۱. Permissionless innovation

۲. Precautionary principle

۳ The permission question

جدید را زود به زود، مکرراً و تا پیش از آنکه مشکلات اجتماعی و اقتصادی آن‌ها بروز کنند، پیش‌بینی، تنظیم، مدیریت و نظارت کنند.

در مقابل، بر اساس رویکرد عدم نیاز به مجوز، فناوری‌های جدید باید به طور پیش‌فرض مجاز باشند و فرصت کافی به آنها داده‌شود، مگر اینکه دلیلی قانع‌کننده برای ایجاد خطرات جدی و آسیب‌زا درپی‌داشته‌باشد. اگر باعث آسیب جدی به افراد نشوند، باید اجازه‌داد که نوآوری‌ها بدون وقفه ادامه‌یابند و مشکلات، درصورتیکه پیش آیند، بعداً حل‌شوند. بار اثبات بر دوش کسانی است که خواهان کنترل‌های پیشگیرانه و احتیاطی هستند تا توضیح دهند چرا فناوری جدید باید ممنوع‌شوند.

تحلیل رویکردهای دستهٔ «الف»:

بنظر می‌رسد مشکل رویکرد احتیاطی این است که اگر ما مدام از تلاش برای پیشرفت به دلیل ترس از بدترین سناریوها اجتناب‌کنیم، بجای جلوگیری از خطرات، از تجربه‌های جدید و فرصت‌ها و پتانسیل‌ها برای رشد و پیشرفت چشم‌پوشی کرده‌ایم یا هزینه‌های آن‌ها را بسیار افزایش‌داده‌ایم. (Abelson et al., n.d., 291)

زمانی که ورود به بازار برای نوآوران، کارآفرینان یا حتی کاربران عادی هزینه‌بر و پیچیده می‌شود، تنها شرکت‌های بزرگ با منابع مالی و حقوقی گسترده قادرند به فعالیت ادامه‌دهند که منجر به تمرکز قدرت، کاهش رقابت و کاهش تنوع محصولات و خدمات خواهدشد. ازاینرو، یکی از پیامدهای سیاست‌گذاری احتیاط‌محور این است که نوآوران مستقل و کارآفرینان نوظهور بجای تلاش برای خلق محصولات و خدمات جدید، ممکن‌است از ترس پیچیدگی‌های قانونی یا هزینه‌های بالای تبعیت، از نوآوری صرف‌نظرکنند. در نتیجه، جامعه از مزایای نوآوری‌های بالقوه‌ای که هرگز به بازار نرسیده‌اند، محروم‌بماند. درست است که پیش‌بینی و احتیاط در مواجهه با خطرات ضروری‌است، اما باید دقت‌کرد که این رویکرد نباید به مانعی برای کشف و پیاده‌سازی ایده‌های جدید تبدیل‌شود. باید نقطه تعادلی میان ایمنی و نوآوری و آزادی ایجادکرد تا بتوان بدون دچارشدن به آسیب، از فرصت‌های موجود بهره‌برداری کرد. بنابراین، محدودیت‌های

پیش‌گیرانه و احتیاطی باید برای شرایطی که تهدید فوری و شدید برای امنیت یا حریم‌خصوصی وجوددارد، باقی‌بمانند (Permissionless Innovation, n.d., viii)

در مقابل، پذیرش رویکرد «نوآوری بدون نیاز به مجوز» مستلزم آن است که قانون‌گذاران و نهادهای نظارتی، بعنوان فاکتوری از سیاست‌گذاری، در قبال نوآوری‌های نوظهور مانند پوشیدنی‌ها صبوری به‌خرج‌دهند، مخصوصاً وقتیکه فناوری‌ها به‌سرعت در حال تکامل‌اند و پیامدهای بالقوه آن‌ها هنوز به‌درستی شناخته‌نشده‌است. (Calo, n.d., 1035) سیاست‌گذاران با یک تحلیل دقیق هزینه–فایده، تا حد امکان، باید خویشتنداری کنند و به فناوری‌های نوپا اجازه‌دهند تا در فرآیند آزمون و خطا و از طریق تعامل با مصرف‌کنندگان تکامل پیداکنند، مگر آنکه تهدید فوری و جدی برای ایمنی عمومی یا حقوق اساسی افراد وجودداشته‌باشد. به‌جای تدوین مقررات سخت‌گیرانه بر اساس ترس‌های احتمالی، بهتراست اجازه داده‌شود نوآوری‌ها در یک محیط باز و پویا و بصورت طبیعی رشدکنند و تنها درصورت بروز خطرات واقعی و قابل‌توجه، مداخلات هدفمند و متناسب صورت‌گیرد. (Thierer, 2013, 1066–1069) بخصوص که قوانین، با سرعتی بسیار کندتر از فناوری (به‌ویژه بازارهای فناوری اطلاعات) حرکت‌می‌کنند. بنابراین، تلاش برای تنظیم‌گری پیش‌دستانه و برنامه‌ریزی برای آینده‌ای نامعلوم، اغلب منجر به پیامدهای ناخواسته‌ای می‌شود که نه‌تنها نوآوری را محدودمی‌کند، بلکه می‌تواند به ضرر مصرف‌کنندگان نیز تمام‌شود. (Thierer, 2013, 2–3)

نتیجه اینکه، تا جاییکه نیاز به اقدام اصلاحی برای رفع آسیب‌ها باشد، اقدامات پسینی[۱] معمولاً بهتر هستند. رویکردهای انعطاف‌پذیرتر و پایین‌به‌بالا برای حل مسائل پیچیده، تقریباً همیشه بر رویکردهای پیشگیرانه، محتاطانه و از بالابه‌پایین برتری دارند.

۲-۱-۳. رویکردهای ایجاد محدودیت در جمع‌آوری داده‌ها یا استفاده از آنها

دو رویکرد کلی در این مورد وجود دارد:

۱. Ex post

الف) محدودکردن جمع‌آوری و نگهداری داده‌های قابل حصول از فناوری‌های پوشیدنی (رویکرد سنتی)
ب) عدم محدودیت جمع‌آوری و نگهداری داده‌ها و انتقال محدودیت‌ها به زمان استفاده از فناوری‌های پوشیدنی (رویکرد نوین)

بطور سنتی، سیاست‌گذاران تمایل‌دارند که برای جلوگیری از وقوع بدترین سناریوهای فرضی در مورد حریم‌خصوصی، مقررات پیش‌گیرانه وضع‌کنند.(Tummarello, 2014) مثلاً در آمریکا این امر خود را در «اصول بکارگیری منصفانهٔ اطلاعات(Fair Information Practice Principles [FIPPs], n.d.)» نشان‌داده‌است؛ (Gellman, 2014, 12–14, 16–26) شامل اصولی چون کنترل فردی (اطلاع‌رسانی و کسب رضایت)، شفافیت، احترام به زمینهٔ داده‌ها، امنیت، دسترسی، دقت، محدودیت در جمع‌آوری داده‌ها و پاسخگویی. دولت وقت (اوباما) تأکیدداشت که این اصول باید در جمع‌آوری و استفاده از داده‌ها در بخش خصوصی رعایت‌شوند و بصورت یک منشور حقوق حریم‌خصوصی مصرف‌کنندگان مصوب کنگره، رسمی‌شوند. با اینحال، تاکنون کنگره اقدامی در این زمینه انجام‌نداده است.

اما فناوری‌های پوشیدنی، ذاتاً همواره در حال حس‌کردن، جمع‌آوری و برقراری ارتباط هستند. این ویژگی، چالش‌های بزرگی برای سیاست‌گذاری مبتنی بر اصول سنتی ایجادمی‌کند (Ramirez, 2013, 4) مثلاً اینکه آیا مصرف‌کنندگان می‌دانند که اشیاء روزمره‌ای که پیش‌تر غیرفعال بودند، اکنون در حال جمع‌آوری و اشتراک‌گذاری داده‌هایی دربارهٔ آن‌ها هستند؟(همان) چطور ممکن‌است این دستگاه‌ها یا اشیاء در زمان مناسب به مصرف‌کننده اطلاع‌رسانی کنند و امکان انتخاب بدهند، در حالیکه اصلاً هیچ صفحه‌نمایش یا رابط کاربری برای برقراری ارتباط وجودندارد؟ آیا ما می‌توانیم از مصرف‌کنندگان بخواهیم که تعداد زیادی تصمیم منطقی دربارهٔ جمع‌آوری و استفاده از داده‌های خود بگیرند؟ اصلاً آیا اصول پایه‌ایِ حریم‌خصوصی مثل انتخاب ساده و شفاف بودن، باید برای اینترنت اشیا هم اجرا شوند یا نه. مهم‌تر اینکه، چطور می‌توان این اصول را با ویژگی‌های خاص اینترنت اشیا هماهنگ کرد؟

«اطلاع‌رسانی و ایجاد امکان انتخاب در اینترنت اشیا، بدلیل همگانی‌بودن جمع‌آوری داده‌ها و موانع عملی برای ارائه‌ی اطلاعات بدون رابط کاربری، چالش‌برانگیز است(The Internet of Things: Privacy and Security in a Connected World, n.d., v)». لذا با توجه به ماهیت فناوری‌های پوشیدنی، اصول سنتی پیش‌گیرانه بر مبنای محدودکردن جمع‌آوری و نگهداری داده‌ها، ممکن‌است همیشه عملی نبوده (Future of Privacy Forum, n.d., 3) و با مشکلات ذیل مواجه‌باشند:

- در عصری که دستگاه‌ها بطور فزاینده‌ای کوچک‌تر می‌شوند، اغلب غیرممکن‌است که مصرف‌کنندگان سیاست حریم‌خصوصی سازمان ارائه‌دهندهٔ فناوری را بخوانند، زیرا بسیاری از این فناوری‌ها آن‌قدر کوچک‌اند که حتی صفحه‌نمایشی نخواهندداشت(Food & Drug Administration [FDA], 2014, 7).
- پیچیدگی بسیاری از این دستگاه‌ها و حجم بالای داده‌هایی که جمع‌آوری می‌کنند، باعث‌می‌شود که طراحی یک رژیم اطلاع‌رسانی و انتخاب کارآمد دشوارباشد. (Executive Office of the President, n.d., 53–54)
- نمی‌توان هر سوءاستفاده ممکن را پیش‌بینی‌کرد. فناوری‌های داده‌های کلان، همراه با حسگرهایی که بر روی اینترنت اشیاء نصب‌می‌شوند، به بسیاری از فضاهایی نفوذ می‌کنند که قبلاً خصوصی بودند. فناوری‌های پوشیدنیِ همیشه روشن و حجم انبوه حسگرهایی که همه‌جا حضوردارند، هرچند ممکن‌است هدف مفیدی داشته‌باشند، ولی کنترل و محدودکردن جمع‌آوری داده را بسیار دشوار و شاید غیرممکن کرده‌اند.

از جمله به همین دلایل است که تردیدهایی در مورد رویکرد سنتی بوجودآمده‌است: مثلاً کاخ سفید به این نتیجه رسیده‌است که باید به چارچوب «اطلاع‌رسانی و انتخاب» که بیش از چهار دهه است اصول حریم‌خصوصی بر اساس آن سازماندهی شده‌است، نگاهی دقیق‌تر بیندازد چون این مدل سنتی در برابر توانایی‌های پیش‌بینی‌ناپذیر و قدرتمند فناوری‌های داده‌های کلان، ناکارآمد شده‌است (President’s Council of Advisors on Sci. & Tech., 2014, 38)

برخی صاحبنظران پیشنهادکرده‌اند که از رویکرد سیاستی مبتنی بر اطلاع‌رسانی و انتخاب به سمت یک رژیم جدید مبتنی بر اعمال محدودیت‌ها در هنگام استفاده حرکت‌کنیم. (Bambauer, n.d., 270–271) «دولت باید مقررات و سیاست‌های حریم‌خصوصی تجاری را بر اساس پیامدهای استفاده و سوءاستفاده از اطلاعات برای مصرف‌کنندگان بناکند. (Beales & Muris, 2008, 109)» مشاور ارشد مایکروسافت می‌گوید، «زمان آن فرارسیده‌است که رویکردی جدید اتخاذکنیم: تمرکز را از محدودکردن جمع‌آوری و نگهداری داده‌ها به کنترل داده‌ها در مهم‌ترین نقطه، لحظه‌ای که از آنها استفاده‌می‌شود، تغییردهیم. (Mundie, 2014, 28–29)» این سیستم تکاملی در حفاظت از حریم‌خصوصی، مسئولیت را از جمع‌آورندگان و نیز کاربر، که معمولاً قادر به درک یا مخالفت با اطلاع‌رسانی‌های مربوط به اخذ رضایت در بازار کنونی نیست، به استفاده‌کنندگان از داده‌ها منتقل‌می‌کند و افراد اخیر باید به‌خاطر نحوه مدیریت داده‌ها مسئول شناخته‌شوند، نه فقط به‌خاطر اینکه آیا رضایت صاحبان اطلاعات را در زمان جمع‌آوری داده‌ها به‌دست‌آورده‌اند یا نه(Executive Office of the President, n.d., 56) . بخصوص که زمینه‌ای که اطلاعات شخصی در آن استفاده خواهدشد و ارزشی که در زمان جمع‌آوری خواهندداشت، اغلب در زمان جمع‌آوری داده‌ها نامشخص است.(Cate, Cullen, & Mayer-Schönberger, 2013, 8)به‌نظر می‌رسد که سیاست‌گذاران در حال تغییر سیاستی و حرکت به این سمت هستند؛ از جمله کاخ سفید «رویکرد استفاده مسئولانه» را واجد مزایای زیادی می‌داند.

تحلیل رویکردهای دستهٔ «ب»:

در رویکرد نوین، با درنظرگرفتن آسیب‌ها و پیامدهای واقعی در دنیای واقعی، بر داده‌ها و چگونگی استفاده از آنها، تمرکزمی‌شود. اما بنظرمی‌رسد تمایل به رویکرد نوین نباید به معنای کنارگذاشتن کامل اطلاع‌رسانی و رضایت (رویکرد سنتی) باشد. باید زمینهٔ پیاده‌سازی و مزایای اجتماعی بالقوه استفاده از اطلاعات را بررسی‌کنیم و ببینیم برای محافظت از حریم‌خصوصی، چه کنترل‌هایی در چارچوب جمع‌آوریِ محدود و چه کنترل‌هایی در چارچوب استفادهٔ محدود مورد نیاز است. باید ببینیم در کجاها می توان مدل اطلاع‌رسانی و رضایت را مدیریت کرد و آنرا

با نیازهای دنیای جدید داده‌ها تطبیق داد و هرجا نشد، از مدل کنترل استفاده، بهره‌بُرد. (Valenstein, 2014) مثلاً ممکن‌است لازم‌باشد استفاده از فناوری‌های پوشیدنی در برخی از محیط‌های حساس مانند سرویس‌ها یا اتاق‌های تعویض لباس یا نقاط نظامی و امنیتی، ممنوع‌شود.

دلیلِ اینکه نمی‌شود اصل را بر رویکرد نوین گذاشت این است که حریم‌خصوصی بسیار وابسته به نظر شخصی است و نمی‌توان به سیاست‌گذاران اجازه داد که بر اساس ترجیحات خود، نتایج را تعیین‌کنند. «قوانین حریم‌خصوصی این خطر را دارند که بیش از حد دیکتاتورگونه شوند. قوانین حریم‌خصوصی که از رضایت عبورمی‌کنند، آزادی انتخاب افراد را محدودمی‌کنند (Thierer, n.d., 414–421) درحالیکه نظرات افراد متفاوت است: بعضی‌ها معتقدند آسیب‌های روانی استفاده از اطلاعاتِ ابزارهای پوشیدنی بدون رضایت زیاد است و باید ممنوع‌شود، ولی برخی معتقدند استفاده از این اطلاعات مزایای اجتماعی زیادی دارند و باید اجازه داده‌شوند. پس باید از سیاست‌هایی که به‌طور غیرضروری انتخاب‌های شخصی افراد را از آنها سلب‌می‌کنند، پرهیزشود. باید به افراد این امکان را داد که تصمیماتی که برایشان مناسب است را بگیرند حتی اگر به نفعشان نباشد، به جای اینکه تصمیمات آن‌ها توسط دیگران (سیاست‌گذاران) محدودشود. مردم درخیلی جاها، از حقوق خود چشم‌پوشی می‌کنند و ریسک‌های بدی می‌کنند و قانون اغلب جلوی آنها را نمی‌گیرد. خیلی اوقات، ما ازدست‌دادن حریم‌خصوصی خود را درازای کارآیی، راحتی و تخفیف‌های قیمتی کوچک می‌پذیریم. واقعیت این است که ما به‌طور داوطلبانه اطلاعاتی از خود را می‌دهیم، چون مزایای آن را بر هزینه‌ها ترجیح‌می‌دهیم. البته تأکید بر آزادی انتخاب افراد به معنای کارآمدی مطلق رضایت یا کفایت آن به‌عنوان تنها مبنای حمایت از حریم خصوصی نیست. با توجه به پیچیدگی فناوری‌های پوشیدنی و محدودیت توانایی کاربران در پیش‌بینی تمام پیامدهای پردازش داده‌ها، رضایت فردی باید در کنار سایر تضمین‌های حقوقی مورد توجه قرار گیرد. بنابراین، هدف از حمایت حقوقی نه جایگزین‌کردن تصمیم افراد با تشخیص سیاست‌گذاران، بلکه فراهم‌آوردن شرایطی است که آزادی انتخاب در چارچوبی شفاف و همراه با حمایت مؤثر از حریم خصوصی اعمال شود.

لذا محدودیت در استفاده باید در موارد آسیبی واقعی و نه احتمالی یا فرضی، در دستور کار قرارگیرد؛ تازه باید این آسیب را بصورت مضیق هم تفسیرکرد یعنی اقداماتی که تهدیدی مستقیم برای سلامت یا اموال انسان ایجادمی‌کند نه مثلاً تهدید علیه آسیب‌های عاطفی یا روانی ناشی از نقض حریم‌خصوصی؛ برای اثبات آسیب‌های اخیر، معیار بسیار بالاتری مورد نیاز است (Calo, 2011, 1133) چون وقتی می‌خواهیم ادعای آسیب‌های حریم‌خصوصی را قانونی کنیم، یک مانع بزرگ وجوددارد (Thierer, 2014, 473–477) یعنی تقابل آن با ارزش‌های دیگری مانند آزادی بیان، آزادی‌های خبری، نوآوری اقتصادی و انتخاب مصرف‌کنندگان. (Abelson et al., n.d., 20) لذا باید بین این ارزش‌های مختلف توازن برقرارکرد. البته تأکید بر ضرورت احراز آسیب واقعی و پرهیز از محدودیت‌های مبتنی بر خطرات صرفاً فرضی، به معنای انکار اهمیت حقوقی نقض حریم خصوصی یا محدودکردن حمایت از آن به موارد ورود خسارت مادی نیست. باید میان معیارهای توجیه مداخله سیاست‌گذار در فعالیت‌های فناورانه و شرایط تحقق مسئولیت حقوقی ناشی از نقض حریم خصوصی تفکیک قائل شد. ممکن است مداخله غیرمجاز در خلوت شخص، با توجه به ماهیت و شرایط آن، واجد وصف ناقض حریم خصوصی باشد، حتی اگر خسارت مالی مستقلی اثبات نشده باشد. ازاین‌رو، تأکید بر آزادی نوآوری و ضرورت پرهیز از محدودیت‌های نامتناسب، نباید به معنای نادیده‌گرفتن نقض حریم خصوصی یا نفی حمایت حقوقی از آن تلقی شود.

به همین دلایل، محدودیت‌های مبتنی بر استفاده نباید به یک چارچوب نظارتی سختگیرانه و طبق یک الگوی ثابت و یکسان و به‌طور یکنواخت برای همه تبدیل‌شوند. انعطاف‌پذیری مهم است (Future of Privacy Forum, n.d., 6) نوآوری‌های مبتنی بر داده‌ها تنها در محیطی سیاستی که پذیرای آزمایش و خطا باشد، می‌تواند به‌وجودآید.(Permissionless Innovation, n.d., 1, 17, 81) به همین دلیل است که پیشنهادات منعطف در زمینه جمع‌آوری و استفاده از داده‌ها، در نهایت به مصرف‌کنندگان، بهتر از دستورالعمل‌های نظارتی یکسان و از بالا به پایین خدمت خواهندکرد. مثلاً اگر سیاست‌گذاران بخواهند استفاده از داده‌های جمع‌آوری شده توسط ابزارهای

پوشیدنی را به دلیل احتمال استفاده‌شدن در راستای تبعیض علیه کاربران، ممنوع‌کنند، باید این قانون را به‌طور دقیق برای مقابله با اشکال واقعی تبعیض نژادی، جنسی یا دینی تنظیم‌کنند (Pfeifle, 2014). مثلاً واژه «تبعیض» نباید به هر شکلی از تفاوت در خدمات، مانند ارائه محصولات متناسب که به گسترش دامنه خدمات مصرف‌کنندگان کمک‌می‌کند، اطلاق‌شود (Varian, 1989, 597–598)

مقررات محدودکنندهٔ استفاده از داده‌ها، می‌توانند اثرات مضر زیادی داشته‌باشند، از جمله افزایش هزینه‌ها برای مصرف‌کنندگان، کاهش محتوای تولیدی و خدماتی که از جمع‌آوری داده‌ها و تبلیغات پشتیبانی‌می‌کنند، افزایش هزینه‌ها برای اپراتورهای کوچک‌تر و استارت‌آپ‌های جدید (که به معنای کاهش رقابت در کل است) و شاید حتی کاهش مزیت رقابتی کشور در اقتصاد دیجیتال جهانی. (Thierer, 2013, 2–3) تمامی این ملاحظات درمورد تکنولوژی‌های پوشیدنی نیز وجود دارد.

بنابراین، به‌جای اعمال محدودیت‌ها در زمینه حریم‌خصوصی به‌صورت سفت و سخت در قالب مقررات، بهترین شیوه‌ها باید به‌طور تدریجی و انعطاف‌پذیر و غالباً خارج از محدوده سیاست‌های عمومی اعمال‌شوند. مثلاً ارائه اطلاعات کافی به مصرف‌کنندگان در مورد شیوه‌های مختلف جمع‌آوری داده‌ها همچنان یکی از بهترین شیوه‌های معقول برای توسعه‌دهندگان است، حتی اگر اجرای آن از طریق قانون دشوارباشد. همچنین، توسعه‌دهندگان فناوری‌های پوشیدنی باید در مورد سیاست‌های استفاده از داده‌های خود بسیار شفاف باشند و جمع‌آوری داده‌ها را به عملکردهای اصلی محدودکنند، مدت زمان نگهداری داده‌ها را محدود کنند؛ از اشتراک‌گذاری آن با تعداد زیادی اشخاص ثالث جلوگیری‌کنند و داده‌ها را در برابر نفوذ غیرمجاز یا نقض داده‌ها محافظت‌نمایند.

بعنوان جمع‌بندی، هیچ راه‌حل معجزه‌آسایی برای مسائل پیچیده حریم‌خصوصی وجود ندارد. «وسعت چالش‌ها به این معنا است که یک رویکرد یکسان برای سیاست‌ها و یا مقررات، به

احتمال زیاد مؤثرنخواهدبود. (Collins et al., n.d., 2)» آنچه مورد نیاز ا ست یک رویکرد لایه‌ای و چندوجهی است که با بهره‌گیری از راهکارهای گوناگون، به نگرانی‌ها پاسخ‌دهد.

۳-۱-۳. تکامل استانداردهای مسئولیت

اغلب در مقررات در سطح دنیا، چهار نوع تجاوز به حریم‌خصوصی درنظر گرفته شده که عبارتند از: افشای عمومی اطلاعات خصوصی، ورود به خلوت شخصی، نمایش نادرست و سوء استفاده از نام یا شباهت شخص(Privacilla.org, n.d., 5–7)

مثلاً تجاوز به حریم‌خصوصی از طریق ورود به خلوت شخصی می‌گوید: «کسیکه عمداً به تنهایی یا به هر نحو دیگری به خلوت یا حریم‌خصوصی دیگری واردشود، یا امور خصوصی او را زیرنظربگیرد، درصورتیکه این ورود برای یک فرد معقول و عادی به‌طور جدی توهین‌آمیز باشد، ممکن‌است مسئول جبران خسارت در قبال ورود به حریم‌خصوصی او باشد. (Restatement (Second) of Torts, 1977, 652B

موارد دیگری هم در قوانین پیش‌بینی شده‌است. (Singleton, 2014) مثلاً در ایالات متحدهٔ آمریکا «قانون پیشگیری از تماشای پنهانی» که نگاه‌کردن به داخل خانه‌ها یا جاسوسی مخفیانه در اماکن عمومی را ممنوع‌می‌کند. «قانون جلوگیری از ویدئوگرافی» نیز جریمه‌ها و حتی زندان را برای کسانیکه تصویر ناحیهٔ خصوصی یک فرد را بدون رضایت او گرفته و اینکار را در شرایطی که فرد انتظار حریم‌خصوصی معقول دارد انجام‌دهند، اعمال‌می‌کند. «قانون گزارش‌دهی اعتباری منصفانه» به افراد حق دسترسی به سوابق اعتباری خود و اصلاح آن در صورت وجود خطا، را می‌دهد.

این مقررات ممکن‌است در آینده شامل اطلاعات حاصل از ابزارهای پوشیدنی هم بشود. (Va. Code Ann., 2014, 18.2-130

قراردادها هم می‌توانند نقش مهمی در جلوگیری از سوءاستفاده از فناوری‌های پوشیدنی داشته‌باشند؛ به اینصورت که افراد و سازمان‌ها می‌توانند با تعیین شروط روشن در قراردادها، نحوهٔ استفاده از این فناوری‌ها را تعیین‌کنند.

قواعد مربوط به حقوق مالکیت هم به موضوع تجاوز به حریم‌خصوصی پرداخته‌اند؛ به این معنی که افراد وقتی به خانه می‌روند و درب‌ها را می‌بندند و پرده‌ها را می‌کشند تا دیگران نتوانند ببینند چه

اتفاقی در داخل می‌افتد، از حمایت قانونی برخوردارند. (Harper, 2010) ممکن‌است در آینده دادگاه‌ها این حقوق را به انواع جدیدی از آسیب‌ها در ارتباط با فناوری‌های پوشیدنی گسترش‌دهند.

پس استانداردهای قانونی و مسئولیت‌ها به تدریج تکامل می‌یابند، همانطور که برای بسیاری از تکنولوژی‌های دیگر نیز رخداده‌است. واقعیت این است که توسعه‌دهندگان فناوری‌های پوشیدنی ممکن‌است داده‌های حجیم جدیدی جمع‌آوری کنند که می‌تواند آنها را در معرض اشکال جدیدی از مسئولیت قراردهد. مثلاً در زمینه خودروهای هوشمند و خودران، هنجارهای مسئولیت احتمالاً تحت تأثیر سطح دانش و کنترل تولیدکنندگان بر این سیستم‌ها، قرارخواهدگرفت. (Villasenor, 2014; Smith, 2014, 1779) یعنی در آینده احتمالاً از توسعه‌دهندگان فناوری‌های انتظار برود که دامنه وسیع‌تری از کاربردهای مرتبط با محصول، سوءاستفاده‌ها و آسیب‌ها را پیش‌بینی کنند و همانطور که داده‌های بیشتری از محل استفادهٔ کاربران بدست‌می‌آورند، به همان نسبت مسئولیت آنها هم ممکن‌است در طول زمان گسترش‌یابد (همان).

بنابراین، سیاست‌گذاران بجای تلاش برای مدیریت دقیق تکنولوژی‌های اینترنت اشیاء و تلاش برای پیش‌بینی هر سناریوی فرضی از ریسک‌ها، باید صبور باشند تا هنجارهای حقوقی در خصوص مسئولیت بطور طبیعی تکامل‌یابند و بروزشوند. (The Internet of Things: To Be Hacked, 2014).

۲-۳. محدودیت‌ها بر مقامات عمومی

یکی از ملاحظاتی که در تدوین راه‌حل‌های حقوقی باید مدنظر قرارگیرد، تفاوت در مخاطب سیاست‌گذاری‌ها از حیث عمومی یا خصوصی بودن است. استفاده از فناوری‌های پوشیدنی توسط مقامات عمومی (دولتی) مانند مجریان قانون و دسترسی آنها به داده‌های خصوصی، نیاز به بررسی ویژه و حفاظت‌های قانونیِ بیشتر دارد. تفاوت‌های قابل‌توجهی بین نهادهای عمومی و خصوصی وجوددارد که سیاست‌گذاران باید آن‌ها را درنظربگیرند.(Thierer, 2014) نهادهای خصوصی برعکس دولت‌ها، بدلیل نداشتن قدرت الزام‌آور، نمی‌توانند مردم را جریمه، مالیات یا زندانی کنند. ضمناً شاید بتوان از کالاها و خدمات شرکت‌های خصوصی استفاده‌نکرد، اما این

پذیرفته شده در انتظار انتشار | نسخه اولیه ویراستاری نشده
Accepted | Awaiting Publication | Draft Version | Unedited

موضوع در مورد دولت‌ها صادق نیست و از تسلط آن‌ها نمی‌توان گریخت. بنابراین، نیاز به حفاظت‌های ویژه‌ای در مورد استفاده از فناوری‌های پوشیدنی توسط نهادهای عمومی وجوددارد. دسترسی دولت‌ها به داده‌های خصوصی جمع‌آوری‌شده از دستگاه‌های پوشیدنی، باید دقیقاً و تنها براساس دلایل قانونی و با رعایت مقررات و تضمین‌های قوی قانونی و صرفاً با اخذ حکم قضائی انجام‌شود؛ قدرت نظارتی دولت‌ها باید محدود و از جمع‌آوری بی‌رویه داده‌ها توسط آن‌ها جلوگیری‌شود. (Kennedy, 2011, 129–130, 154)

۴. نتیجه‌گیری

فناوری‌های پوشیدنی به دستگاه‌های الکترونیکی عمدتاً مبتنی بر هوش مصنوعی اطلاق‌می‌شوند که برای پوشیدن روی بدن طراحی‌شده‌اند. این فناوری بعنوان زیرمجموعهٔ اینترنت اشیا، ویژگی‌های بسیار شخصی‌تری نسبت به آن دارد و نگرانی‌هایی را در خصوص مقررات بهداشتی، ایمنی و حریم‌خصوصی ایجادمی‌کند.

در ارتباط با حریم‌خصوصی، میزان و مدت نگهداری از داده‌ها، افراد دارای دسترسی به داده‌ها، درگیربودن کاربران مستقیم این فناوری‌ها و نیز افراد حاضر در محیط اطراف، حساس‌بودنِ داده‌های جمع‌آوری شده و نیز تقابل با آزادی بیان و مطبوعات، از جمله نگرانی‌های جدی است. راهکارهای حفظ حریم‌خصوصی در رابطه با فناوری‌های پوشیدنی به دوستهٔ **غیرحقوقی** (شامل: سازگاری اجتماعی و فردی با اختراعات جدید، تغییر هنجارها و فشار اجتماعی، افزایش سواد دیجیتال، و خودتنظیمی) و **حقوقی** (رویکردهای مختلف به سیاست‌گذاری، تکامل‌یافتن استانداردهای مسئولیت، و ملاحظهٔ تفاوت‌ها در مخاطبِ سیاست‌گذاری‌ها از حیث عمومی یا خصوصی بودن) قابل تقسیم است.

بعنوان مهمترین بخش پژوهش، با یک بررسی تطبیقی، رویکردها به سیاست‌گذاری در مورد فناوری‌های پوشیدنی، در دو دسته معرفی‌شد:

الف) رویکردهای قاعده‌گذاریِ پیشگیرانه یا پسینی (یا همان رویکردهای اصل احتیاط ونوآوری بدون نیاز مجوز): طبق رویکرد احتیاط، نوآوری‌ها باید محدود یا ممنوع شوند تا

زمانیکه توسعه‌دهندگان آن‌ها ثابت‌کنند که هیچ‌گونه آسیبی به افراد، گروه‌ها، نهادهای خاص، هنجارهای فرهنگی یا قوانین و سنت‌های موجود واردنمی‌کنند. اما طبق رویکرد پسینی باید اجازه داده‌شود نوآوری‌ها در یک محیط باز و پویا رشدکنند و تنها درصورت بروز خطرات واقعی و قابل‌توجه، مداخله صورت‌گیرد.

ب) رویکردهای ایجاد محدودیت در جمع‌آوری داده‌ها یا استفاده از آنها: رویکرد نخست مبتنی ایجاد محدودیت در جمع‌آوری و نگهداری داده‌ها براساس اطلاع‌رسانی و انتخاب است اما رویکرد نوین مبتنی بر محدودیت‌های استفاده از داده‌ها و انتقال مسئولیت از جمع‌آورندگان داده‌ها به استفاده‌کنندگان از داده‌هاست.

در کنار این دو دسته رویکرد سیاست‌گذاری، باید به دو راه‌حل حقوقی دیگر هم توجه کرد:

۱) استانداردها و هنجارهای حقوقی در خصوص مسئولیت، بخصوص در مورد فناوری‌های جدید (پوشیدنی‌ها)، بطور طبیعی در حال تکامل است و بعید نیست در آینده کسانی مسئول قلمداد شوند که در گذشته مسئولیتی برای آنها متصورنبود.

۲) در سیاست‌گذاری‌ها باید به تفاوت مخاطب از حیث عمومی یا خصوصی بودن توجه کرد. بعنوان جمع‌بندی باید دانست که نگرانی‌ها درباره‌ی حریم‌خصوصی کاملاً منطقی و مهم‌اند و باید به آن‌ها توجه‌کرد. اما واکنش به این نگرانی‌ها نباید با روش‌های خشک، دستوری و از بالا به پایین (مثل صدور قوانین سختگیرانهٔ بدون انعطاف) باشد. حریم‌خصوصی و امنیت ارزشمندند، ولی در کنار آن‌ها، اموری مثل نوآوری، کارآفرینی، رشد اقتصادی، رقابت، و آزادی انتخاب مصرف‌کننده هم به همان اندازه اهمیت دارند. به همین دلیل، تا وقتی دلیل و مدرک واضحی از خطر جدی برای سلامت مردم یا امنیت یا حریم‌خصوصی وجود ندارد، سیاست‌گذاران نباید استفاده از این فناوری‌ها را با قوانین سخت محدودکنند. باید اصل بر آزادی استفاده باشد، مگر اینکه دلیل قانع‌کننده‌ای برای خطرناک‌بودن آن ارائه‌شود. نظارت پیشگیرانه (قبل از وقوع آسیب‌ها) معمولاً بسیار ناکارآمد و حتی خطرناک است. مقررات آینده‌نگر که بر اساس حدس و

پذیرفته‌شده در انتظار انتشار | نسخه‌ی اولیه ویراستاری‌نشده
Accepted Awaiting Publication | Draft Version Unedited

گمان درباره آسیب‌های آینده تنظیم شوند، احتمالاً نوآوری و فرصت‌های رشد را خواهندگرفت. هنگامی که اقدامات اصلاحی برای رسیدگی به آسیب‌های جدی‌تر ضروری باشد، اقدامات بعد از وقوع آسیب، بطور کلی معقول‌ترند.

روش مناسب این است که با رویکردی باز، منعطف و مرحله‌ای، همزمان با رشد فناوری، به نگرانی‌ها هم رسیدگی‌شود. این مدل «چندلایه و از پایین به بالا» کمک می‌کند که نوآوری‌ها زنده بمانند و جلوی پیشرفت‌های مفید گرفته نشود. ضمن اینکه باید نهادی وجود داشته باشد که فرایندی مستمر از ارزیابی و رسیدگی به خطرات را مدیریت و اطمینان حاصل‌کند که توسعه‌دهندگان فناوری‌های پوشیدنی به وعده‌های حریم‌خصوصی خود به مصرف‌کنندگان عمل‌می‌کنند.

۵. منابع

منابع فارسی:

[۱] اکبریان طبری، معصومه و جعفرزاده، میرقاسم. (۱٤۰۵). حمایت از داده‌های اینترنت اشیاء به‌مثابه یک مال فکری؛ مطالعه تطبیقی حقوق مالکیت فکری اتحادیه اروپا و ایران. تحقیق و توسعه در حقوق فناوری و مالکیت فکری، ۱(۱)، ۲٤-٦۲. https://doi.org/10.22034/jtlip.2026.736034

[۲] صادقی، محسن و جوادی پارسا، کسری. (۱٤۰٤). مطالعه تطبیقی سیاست‌گذاری حقوقی حوزه هوش مصنوعی در اتحادیه اروپا: ارائه الگوی بایسته برای حقوق ایران. فصلنامه تحقیق و توسعه در حقوق تطبیقی، ۹(۳۱)، ۱۹۸-۲٤٦. https://doi.org/10.22034/law.2025.2065565.1673

References:

Books:

[1] Brown, John Seely & Paul Duguid. A Response to Bill Joy and the Doom-and-Gloom Technofuturists, in AAAS Science and Technology Policy Yearbook 2001 77, 79, 82 (Albert H. Teich, Stephen D. Nelson, Celia McEnaney & Stephen J. Lita eds., 2001).

[2] Gardner, Dan. Future Babble: Why Expert Predictions Fail and Why We Believe Them Anyway 141 (2010).

[3] Topol, Eric. The Creative Destruction of Medicine: How the Digital Revolution Will Create Better Health Care. (2012).

[4] Varian, Hal. Price Discrimination, in 1 Handbook of Industrial Organization 597, 598 (Richard Schmalensee & Robert Willig eds., 1989).

[5] Zolli, Andrew & Ann Marie Healy. Resilience: Why Things Bounce Back 7 (2012).

Articles:

[3] Akbarian, M. & jafarzad, M. (2026). Protection of Internet of Things (IoT) Data as Intellectual Property: A Comparative Study of the Intellectual Property Laws of the European Union and Iran. Research and development in technology law and Intellectual property, 1(1), 24-62. https://doi.org/10.22034/jtlip.2026.736034. (in Persian)

[4] Al-Faruque, Ferdous. Are Smartphones the Best Medicine? The Hill (June 17, 2014, 6:01 AM), http://thehill.com/policy/technology/209534-are-smartphones-thebest-medicine, archived at http://perma.cc/7A76-DLP9.

[5] Barth-Jones, Daniel C. Does De-identification Work or Not? Fierce Big Data (June 23, 2014), http://www.fiercebigdata.com/node/35502156, archived at http://perma.cc/AC68-2PXE; see also Arvind Narayanan & Edward W. Felten, No Silver Bullet: De-identification Still Doesn't Work 8 (July 9, 2014) (unpublished manuscript), available at http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf, archived at http://perma.cc/82Y8-MQW7.

[6] Beales, Howard, Richard Craswell & Steven C. Salop. The Efficient Regulation of Consumer Information, 24 J.L. & Econ. 491, 531 (1981).

[7] Beales, J. Howard, III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. Chi. L. Rev. 109, 109 (2008).

ویراستاری | در انتظار انتشار | Awaiting Publication | Draft Version | Unedited

[8] Bennett, Brian. Wearable Tech Multiplies and Goes Mainstream at MWC 2014. CNET (Feb. 27, 2014, 10:49 AM), http://reviews.cnet.com/8301-13970_7-57619658-78/wearable-tech-multiplies-and-goes-mainstream-at-mwc-2014, archived at http://perma.cc/LMK6-UJU5; Health and Appiness, ECONOMIST (Feb. 1, 2014), http://www.economist.com/news/business/21595461-those-pouring-money-healthrelated-mobile-gadgets-and-apps-believe-they-can-work, archived at http://perma.cc/ZLY2-YKA8.

[9] Bilton, Nick. Tech, Meet Fashion. N.Y. Times, Sept. 4, 2014, at E2, http://www.nytimes.com/2014/09/04/fashion/intel-and-opening-ceremony-collaborateon-mica-a-stylish-tech-bracelet.html, archived at http://perma.cc/97C3-QAHN.

[10] Bracy, Jedidiah. Will Industry Self-Regulation Be Privacy's Way Forward? Int'l Ass'n Privacy Profs. (June 24, 2014), https://www.privacyassociation.org/publications/will_industry_self_regulation_be_privacys_way_forward, archived at https://perma.cc/RK7R-43AE.

[11] Bryant Walker Smith, Proximity-Driven Liability, 102 Geo. L.J. 1777, 1779 (2014).

[12] Calo, Ryan, The Boundaries of Privacy Harm, 86 Ind. L.J. 1131, 1133 (2011).

[13] Carter, Jamie. Wearable Cameras Are All the Rage but Should We All Become Lifeloggers? Tech Radar (June 4, 2014), http://www.techradar.com/us/news/world-of-tech/life-through-a-lens-trials-and-tribulations-of-a-life-logger-1251717?src=rss&attr=all, archived at http://perma.cc/82EW-F74Q.

[14] Castelao, Leandro. The Quantified Self: Counting Every Moment. Economist, Mar. 3, 2012, at Q1, http://www.economist.com/node/21548493, archived at http://perma.cc/822H-8CJ2; see also Lupton, Deborah. Understanding the Human Machine. IEEE TECH. & SOC'Y MAG. (Dec. 9, 2013), at 25, https://www.academia.edu/5392119/Understanding_the_human_machine, archived at https://perma.cc/C7FA-EUCS.

[15] Cervantes, Edgar. CA7CH Lightbox: The Next Wearable Camera to Compete Against the GoPro. Android Authority (June 18, 2014), http://www.androidauthority.com/ca7ch-lightbox-wearable-camera-394812, archived at http://perma.cc/QA7Q-DNBG.

[16] Collier, Anne. From Users to Citizens: How to Make Digital Citizenship Relevant, NetFamilyNews (Nov. 16, 2009), http://www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html, archived at http://perma.cc/V52V-FBZY.

[17] Dickson, E. J. Google Glass Livestream Brings Your Privacy Nightmares to Life. Daily Dot (Apr. 8, 2014), http://www.dailydot.com/technology/google-glass-livestream, archived at http://perma.cc/P33X-UZD9.

[18] Fornasier, M. D. O. (2019). The Applicability of the Internet of Things (IoT) between Fundamental Rights to Health and to Privacy. Revista de Investigacoes Constitucionais, 6(2), 298-299.

[19] Gitlin, Jonathan M. How Can Cars Keep up With Gadget Innovation? Ars Technica (June 3, 2014, 7:00 AM), http://arstechnica.com/cars/2014/06/industries-collide-howautomakers-are-adapting-to-consumer-tech-life-cycles/, archived at http://perma.cc/8ZRN-XCEQ.

[20] Gilbert, Ben. Google Fit Is Android's Answer to Exercise and Health Tracking. Engadget (June 25, 2014, 2:30 PM), http://www.engadget.com/2014/06/25/google-fit, archived at http://perma.cc/FJM6-K55X.

[21] Gellman, Robert, Fair Information Practices: A Basic History 1, 12–14, 16–26 (Aug. 3, 2014) (unpublished manuscript), available at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf, archived at http://perma.cc/NL6V-5CEZ.

[22] Guglielmo, Connie & Parmy Olson. The Case Against Wearables, or Why We Won't All Look Like the Borg This Year. Forbes (Mar. 3, 2014), http://www.forbes.com/sites/connieguglielmo/2014/02/12/the-case-against-wearables, archived at http://perma.cc/H4F9-JFZ4; Warnock, Nick. Wearable Tech: Fashion Will Rule. InformationWeek (June 18, 2014, 9:06 AM), http://www.informationweek.com.

[23] Havenstein, Heather. "Baked-In Security." *Computerworld* (Mar. 21, 2005), https://www.computerworld.com/article/1713821/baked-in-security.html, archived at: https://perma.cc/ZF58-6URF.Cavoukian, Ann & Daniel Castro. *Big Data and Innovation, Setting the Record Straight: De-identification Does Work* 1 (June 16, 2014), available at http://www2.itif.org/2014-big-data-deidentification.pdf, archived at http://perma.cc/7TBK-KGPX.

[24] Holmes, Elizabeth. Tech Companies and Fashion Designers Try to Put the 'Wear' in 'Wearables'. Wall St. J., Sept. 9, 2014, http://online.wsj.com/articles/tech-companiesand-fashion-designers-try-to-put-the-wear-in-wearables-1410305929, archived at http://perma.cc/HMH6-KLU5.

[25] Howard, Alex. The "Right to Record" Is Not a Question of Technology, but Rather Power and Policy. Tech Republic (May 22, 2014, 8:03 AM PST), http://www.techrepublic.com/article/the-right-to-record-is-not-a-question-of-technologybut-rather-power-and-policy/#, archived at http://perma.cc/3SED-M5PF.

[26] Helm, Anne Marie & Daniel Georgatos. Privacy and Mhealth: How Mobile Health "Apps" Fit into a Privacy Framework Not Limited to HIPAA, 64 Syracuse L. Rev. 131, 156 (2014).

[27] Kelly, Heather. Google Glass Users Fight Privacy Fears. CNN (Dec. 12, 2013, 2:47 PM), http://www.cnn.com/2013/12/10/tech/mobile/negative-google-glass-reactions, archived at http://perma.cc/YN3Z-N7DB.

[28] Kennedy, Charles H., An ECPA for the 21st Century: The Present Reform Efforts and Beyond, 20 CommLaw Conspectus 129, 129–30, 154 (2011).

[29] Klosowski, Thorin. Lots of Health Apps Are Selling Your Data: Here's Why, Lifehacker (May 9, 2014, 10:00 AM), http://lifehacker.com/lots-of-health-apps-are-selling-your-data-heres-why-1574001899, archived at http://perma.cc/N7Y5-RGFB.

[30] Langley, Hugh. Autographer Boss: Google Glass Privacy Fears Have Been Exaggerated by the Media. Tech Radar (June 18, 2014), http://www.techradar.com/news/photography-video-capture/google-glass-privacy-fears-have-been-exaggerated-by-the-media-says-autographer-creator-1253837, archived at http://perma.cc/AZ3N-39FR; An Intelligent, Sneaky, Wireless Camera for the Ultra-Connected Home, CNET (May 21, 2014, 5:00 AM), http://www.cnet.com/products/butterfleye, archived at http://perma.cc/6S8P-4XD4.

[31] Lohr, Steve. A Messenger for the Internet of Things. N.Y. Times (Apr. 25, 2013, 12:15 AM), http://bits.blogs.nytimes.com/2013/04/25/a-messenger-for-the-internet-of-things, archived at http://perma.cc/649A-PQAY.

[32] Mann, Steve. Eye Am a Camera: Surveillance and Sousveillance in the Glassage. TIME (Nov. 2, 2012), http://techland.time.com/2012/11/02/eye-am-a-camera-surveillance-and-sousveillance-in-the-glassage, archived at http://perma.cc/GP6F-N3JR.

[33] Magid, Larry. “We Need to Rethink Online Safety.” *The Huffington Post* (Jan. 22, 2010). Available at: http://www.huffingtonpost.com/larry-magid/we-need-to-rethink-online_b_433421.html. Archived at: https://perma.cc/T3N4-6A5X.

[34] Mallozzi, Vincent M. On Train, a Fight Between Silent and Merely Quiet, N.Y. Times, Jan. 10, 2011, at A17, available at http://www.nytimes.com/2011/01/10/nyregion/10quiet.html, archived at http://perma.cc/3G59-3RQW.

[35] McLellan, Charles. M2M and the Internet of Things: A Guide. ZDNet (Jan. 10, 2013, 1:27 PM), http://www.zdnet.com/m2m-and-the-internet-of-things-7000008219, archived at http://perma.cc/XNK7-GJEY.

[36] Mead, Derek. Google Glass Is Already Being Used in the Operating Room. Motherboard (June 24, 2013, 1:30 PM), http://motherboard.vice.com/blog/googleglass-is-already-being-used-in-the-operating-room, archived at http://perma.cc/NH4S-2DSB.

[37] Mershon, Erin. Apple Dives into “Internet of Things.” Politico (June 2, 2014, 6:01 PM), http://www.politico.com/story/2014/06/apple-wwdc-2014-internet-of-things-107336.html#ixzz33hMxZTIN, archived at http://perma.cc/5PQU-TBVY.

[38] Metz, Rachel. The Internet of You. MIT Tech. Rev. (May 20, 2014), http://www.technologyreview.com/news/527386/the-internet-of-you, archived at http://perma.cc/FV4T-YUPH.

[39] Miller, Claire Cain. At Google, Bid to Put Its Glasses to Work. N.Y. Times, Apr. 7, 2014, at B1, http://www.nytimes.com/2014/04/08/technology/google-begins-a-push-to-take-glass-to-work.html?_r=0, archived at http://perma.cc/J2Z7-WLLW.

[40] Mundie, Craig, Privacy Pragmatism: Focus on Data Use, Not Data Collection, 93 Foreign Aff., Mar./Apr. 2014, at 28, 29.

[41] Newman, Jared. The Real Privacy Implications of Google Glass, TIME (May 2, 2013), http://techland.time.com/2013/05/02/the-real-privacy-implications-of-google-glass, archived at http://perma.cc/RR93-TWWA.

[42] Olivarez-Giles, Nathan. WebMD Relaunches iPhone App as a Hub for Fitness Data. Wall St. J. (June 16, 2014, 1:22 AM), http://blogs.wsj.com/personaltechnology/2014/06/16/webmd-relaunches-iphone-app-as-a-hub-for-fitness-data, archived at http://perma.cc/N2P9-4636.

[43] Olson, Parmy. Wearable Tech Is Plugging into Health Insurance. Forbes (June 19, 2014, 1:26 PM), http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance, archived at http://perma.cc/VG5W-6YUB.

[44] Panzarino, Matthew. Disney Gets into Wearable Tech with the MagicBand. Next Web (May 29, 2013, 7:24 PM), http://thenextweb.com/insider/2013/05/29/disney-goes-into-wearable-tech-with-the-magic-band, archived at http://perma.cc/HD8S-XWBU.

[45] Plyler, Katrina. What Is Everybody Wearing? Fitness Tech Gadgets! U.S. News (Apr. 11, 2014, 8:00 AM), http://health.usnews.com/health-news/blogs/eat-run/2014/04/11/what-is-everybody-wearing-fitness-tech-gadgets?int=9a5208, archived at http://perma.cc/2TN8-ARGM.

[46] Regan, Maria K. Saving Lives: Ambulances Get Connected to the IoT. PTC (July 25, 2014), http://blogs.ptc.com/2014/07/25/saving-lives-ambulances-get-connected-to-the-iot, archived at http://perma.cc/SD58-FH7P.

[47] Rojahn, Susan Young. An Activity Tracker for Seniors. MIT Tech. Rev. (Feb. 27, 2014), http://www.technologyreview.com/news/525016/an-activity-tracker-for-seniors, archived at http://perma.cc/NL4P-7EQY.
[48] Rojahn, Susan Young. Why Some Doctors Like Google Glass So Much. MIT Tech. Rev. (May 6, 2014), http://www.technologyreview.com/news/526836/why-some-doctors-like-google-glass-so-much, archived at http://perma.cc/8MVU-LF7J.
[49] Sadeghi, M. & Javadi Parsa, K. (2025). Comparative Study of Legal Policymaking in the Field of AI in European Union; Suitable Model for Iranian Law. Journal of Research and Development in Comparative Law, 9(31), 198-246. https://doi.org/10.22034/law.2025.2065565.1673. (in Persian)
[50] Schofield, Jack. Microsoft's Wearable Alice Band Is Not a Rival to Google Glass. ZDNet (July 14, 2014, 11:03 AM), http://www.zdnet.com/microsofts-wearable-aliceband-is-not-a-rival-to-google-glass-7000031563, archived at http://perma.cc/P4NN-KY89.
[51] Singleton, Micah, Defining Privacy in the Age of Wearable Cameras, Kernel (Sept. 14, 2014), http://kernelmag.dailydot.com/issue-sections/features-iss-sections/10248/glass-wearable-cameras-legal-privacy, archived at http://perma.cc/2UD7-WJ2S.
[52] Sunstein, Cass. Social Norms and Social Roles, 96 Colum. L. Rev. 903, 914 (1996).
[53] Thomson, Judith Jarvis. The Right to Privacy, 4 Phil. & Pub. Aff. 295, 310 (1975).
[54] Thierer, Adam. A Framework for Benefit-Cost Analysis in Digital Privacy Debates, 20 Geo. Mason L. Rev. 1055, 1066–69 (2013) [hereinafter A Framework], available at http://mercatus.org/publication/framework-benefit-cost-analysis-digital-privacy-debates, archived at http://perma.cc/6UA4-7PUS.
[55] Thierer, Adam. Can We Adapt to the Internet of Things? Int'l Ass'n Privacy Profs. (June 19, 2013), https://www.privacyassociation.org/privacy_perspectives/post/can_we_adapt_to_the_internet_of_things, archived at https://perma.cc/V3Q9-2QET.
[56] Thierer, Adam. Do We Need a Constitutional Amendment Restricting Private-Sector Data Collection? Int'l Ass'n of Privacy Prof'l (Jan. 23, 2014), https://privacyassociation.org/news/a/do-we-need-a-constitutional-amendment-restricting-private-sector-data-colle/, archived at https://perma.cc/8H66-6Z5S.
[57] Thierer, Adam. Muddling Through: How We Learn to Cope with Technological Change. Tech. Liberation Front (June 17, 2014), http://techliberation.com/2014/06/17/muddling-through-how-we-learn-to-cope-with-technological-change, archived at http://perma.cc/WD4U-KZRN.
[58] Thierer, Adam. Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle, 14 Minn. J.L. Sci. & Tech. 309, 311 (2013).
[59] Thierer, Adam. Privacy Law's Precautionary Principle Problem, 66 Me. L. Rev. 467, 473–77 (2014) [hereinafter Precautionary Principle].
[60] Trew, James. Pavlok Is a Habit-Forming Wearable That Will Shock You. Engadget (July 4, 2014, 10:40 AM), http://www.engadget.com/2014/07/04/pavlok-wearable, archived at http://perma.cc/MPW6-LP4B.
[61] Tummarello, Kate, Obama's "Big Data" Report Calls for New Privacy Laws, The Hill (May 1, 2014, 2:28 PM), http://thehill.com/policy/technology/204961-white-house-big-data-report-calls-for-new-privacy-laws, archived at http://perma.cc/MK6K-AETX.
[62] Valenstein, Jill, Will Individual Notice and Consent Become a Relic of the Past? The White House Report on Big Data Suggests Privacy Regulation Should Focus on Data

Use, Rather Than Data Collection, Privacy & Sec. L. Blog (May 20, 2014), http://www.privsecblog.
[63] Villasenor, John, Who Is at Fault When a Driverless Car Gets in an Accident? Atlantic (Apr. 25, 2014, 4:15 PM), http://www.theatlantic.com/business/archive/2014/04/who-is-at-fault-when-a-driverless-car-gets-in-an-accident/361250, archived at http://perma.cc/NWV9-2RWR.
[64] Warren, Samuel D. & Louis D. Brandeis. The Right to Privacy, 4 Harv. L. Rev. 193, 195 (1890).
[65] Warren, Tom. Samsung's Free Galaxy S5 "Gifts" Focus on Fitness. Verge (Mar. 10, 2014, 6:40 AM), http://www.theverge.com/2014/3/10/5490078/freesamsung-galaxy-s5-apps-health-fitness, archived at http://perma.cc/7G6P-AFD4.
[66] Weaver, John Frank. We Need to Pass Legislation on Artificial Intelligence Early and Often, Future Tense (Sept. 12, 2014, 3:53 PM), http://www.slate.com/blogs/future_tense/2014/09/12/we_need_to_pass_artificial_intelligence_laws_early_and_often.html, archived at http://perma.cc/RH82-JJRM.
[67] Wilson, H. James. Wearables in the Workplace. Harv. Bus. Rev., Sept. 2013, http://hbr.org/2013/09/wearables-in-the-workplace/ar/1, archived at http://perma.cc/4BLQ-7MG4.

Documents:

[1] About Us, OnGuard Online, http://www.onguardonline.gov/about-us, archived at http://perma.cc/DJJ8-DKRH (last visited Jan. 29, 2015).
[2] ACLU v. Alvarez, 679 F.3d 583, 595–96 (7th Cir. 2012).
[3] FDA. Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff (Sept. 25, 2013), available at http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/default.htm, archived at http://perma.cc/G7YH-PBBN.
[4] Fair Information Practice Principles (FIPPs).
[5] Federal Trade Commission (FTC). Strategic Plan for Fiscal Years 2009 to 2014 4 (Sept. 2009), available at http://www.ftc.gov/opp/gpra/spfy09fy14.
[6] pdf, archived at http://perma.cc/L4VV-MEUB.
[7] FOOD & DRUG ADMIN., U.S. DEP'T HEALTH & HUM. SERVS., Guidance for Industry: Internet/Social Media Platforms with Character Space Limitations – Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices 7 (June 2014), available at http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM401087.pdf, archived at http://perma.cc/A69N-8Z6V.
[8] Harper, Jim, Consumer Online Privacy, Cato Institute (July 27, 2010), available at http://www.cato.org/publications/congressional-testimony/consumer-online-privacy, archived at http://perma.cc/7GVT-ZR4D.
[9] Shapiro, Gary & Laura Knapp Chadwick. Comments of the CEA in re Privacy and Security Implications of the Internet of Things [to the FTC] 7 (June 10, 2013), http://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00027861 93.pdf.
[10] Ohlhausen, Maureen K., Comm'r, U.S. Fed. Trade Comm'n. Success in Self-Regulation: Strategies to Bring to the Mobile and Global Era, Address to the Better

Business Bureau Self-Regulation Conference 3 (June 24, 2014), available at http://www.ftc.gov/system/files/documents/public_statements/410391/140624bbbself-regulation.pdf, archived at http://perma.cc/957C-ZU67.

[11] Julie Brill, Comm'r, U.S. Fed. Trade Comm'n. Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data, Address Before the European Data Protection Supervisor's Workshop on Privacy, Consumer Protection and Competition in the Digital Age 9 (June 2, 2014), available at http://www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf, archived at http://perma.cc/D9S7-URR4.

[12] Ramirez, Edith. Chairwoman, Fed. Trade Comm'n. Protecting Consumer Privacy in a Big Data Age, Speech at the Media Institute, Washington, D.C. 12 (May 8, 2014), available at http://www.ftc.gov/system/files/documents/public_statements/308421/140508mediainstitute.pdf, archived at http://perma.cc/L282-DQPA.

[13] Ramirez, Edith, Chairwoman, U.S. Fed. Trade Comm'n, The Internet of Things and the FTC: Does Innovation Require Intervention**?** Remarks Before the U.S. Chamber of Commerce 3 (Oct. 18, 2013), available at http://www.ftc.gov/public-statements/2013/10/internet-things-ftc-does-innovation-require-intervention-0, archived at http://perma.cc/K3NW-N8S9.

[14] Ramirez, Edith, Chairwoman, U.S. Fed. Trade Comm'n, The Internet of Things: Privacy and Security in a Connected World 4 (Nov. 19, 2013), available at http://www.ftc.gov/public-statements/2013/11/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission, archived at http://perma.cc/68H2-YW8H.

[15] RESTATEMENT (SECOND) OF TORTS § 652B (Am. L. Inst. 1977).

[16] Thierer, Adam D., Testimony Before the Senate Comm. on Commerce, Sci. & Transp.: A Status Update on the Development of Voluntary Do-Not-Track Standards 2–3 (Apr. 24, 2013).

[17] FED. TRADE COMM'N, PROJECT NO. P135405, Comments of the Future of Privacy Forum 13 (2014), available at http://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00013-88250.pdf, archived at http://perma.cc/FBX3-9H93 [hereinafter Future of Privacy Forum].

[18] Va. Code Ann. § 18.2-130 (2014) (Peeping or spying into dwelling or enclosure).

Reports:

[1] Cate, Fred H., Peter Cullen & Viktor Mayer-Schönberger. *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* 8 (Dec. 2013), available at http://op.bna.com/pl.nsf/id/dapn-9gyjvw/$File/Data-Protection-Principles-for-the-21st-Century.pdf, archived at http://perma.cc/258D-44NQ.

[2] Cavoukian, Ann. *Privacy by Design and the Emerging Personal Data Ecosystem* 4 (Privacy by Design Oct. 2012), available at http://www.ipc.on.ca/images/Resources/pbd-pde.pdf, archived at http://permacc/K6QJ-2ND3

[3] Caprio, Daniel W., Jr., Senior Strategic Advisor, Transatlantic Computing Continuum Policy Alliance, Letter to Donald S. Clark, Secretary, U.S. Federal Trade Commission,

Accepted | Awaiting Publication | Under Peer Review | Unedited

3 (Jan. 10, 2014), available at: http://cppionline.org/docs/Letter-to-Secretary_Clark_final.pdf, archived at: https://perma.cc/5JL6-23K3.

[4] Common Sense Media. *Digital Literacy and Citizenship in the 21st Century: Educating, Empowering, and Protecting America's Kids* 1 (June 2009), available at https://www.itu.int/council/groups/wg-cop/second-meeting-june-2010/CommonSenseDigitalLiteracy-CitizenshipWhitePaper.pdf, archived at https://perma.cc/YTX4-YL73.

[5] Fordham Center on Law & Information Policy (FORDHAM CLIP). *Volunteer Privacy Educators Program* (2013), available at http://law.fordham.edu/assets/CLIP/2013_CLIP_VPE_Complete.pdf, archived at http://perma.cc/65EC-3B.

[6] Lenard, Thomas M. & Paul H. Rubin**.** *The Big Data Revolution: Privacy Considerations* 24 (Dec. 2013) (unpublished manuscript), available at http://www.techpolicyinstitute.org/files/lenard_rubin_thebigdatarevolutionprivacyconsiderations.pdf.

[7] Maughan, Alistair & Ferdous Al-Faruque. *The Internet of Things Part 2: The Old Problem Squared.* Morrison Foerster 6 (Mar. 20, 2014), http://media.mofo.com/files/Uploads/Images/140320-The-Internet-of-the-Things-Part-2.pdf, archived at http://perma.cc/YAG8-LB8Q.

[8] Pfeifle, Sam. *How Big Data Discriminates*, Int'l Ass'n Privacy Profs. (June 24, 2014), https://www.privacyassociation.org/publications/how_big_data_discriminates, archived at https://perma.cc/2UED-U2VK.

[9] PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE & TECHNOLOGY (PCAST). *Big Data and Privacy: A Technological Perspective* 38 (May 2014), available at http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_an_privacy_may_2014.pdf, archived at http://perma.cc/BK4F-RS8A.

[10] Solove, Daniel. *Privacy and Data Security Violations: What's the Harm?* LinkedIn (June 25, 2014), ttps://www.linkedin.com/today/post/article/20140625045136-2259773-privacy-and-data-security-violations-what-s-the-harm, archived at https://perma.cc/5X89-RD6A.

[11] Thierer, Adam. *Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer*, 16 *Progress on Point*, July 2009, at 1–2, available at http://www.pff.org/issues-pubs/pops/2009/pop16.13-five-online-safety-task-forces-agree.pdf, archived at http://perma.cc/P5R6-8GNR; *Online Safety & Tech. Working Group, Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group* 1–2 (June 4, 2010), available at http://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_060410.pdf, archived at http://perma.cc/YG8W-NTSF.

[12] Valenstein, Jill. *Will Individual Notice and Consent Become a Relic of the Past? The White House Report on Big Data Suggests Privacy Regulation Should Focus on Data Use, Rather Than Data Collection*, Privacy & Sec. L. Blog (May 20, 2014), http://www.privsecblog.com/2014/05/articles/main-topics/marketing-consumer-privacy/will-individual-notice-and-consent-become-a-relic-of-the-past-the-white-house-report-on-big-data-suggests-privacy-regulation-should-focus-on-data-use-rather-than-data-collection, archived at http://perma.cc/7Q94-XM98.

[13] Villasenor, John. *Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation* 7–14 (2014), available at http://www.brookings.edu/research/papers/2014/04/products-liability-driverless-cars-villasenor, archived at http://perma.cc/UH34-9C4R.

پذیرفته‌شده | در انتظار انتشار | نسخه‌ی اولیه | ویراستاری‌نشده
Accepted | Awaiting Publication | Draft Version | Unedited

Legal Dimensions of Privacy Violations by AI-Powered Wearable Technologies: Legal Analysis and a Comparative Assessment of Policy Approaches

Abstract

The rapid proliferation of artificial intelligence-powered wearable technologies has opened up new horizons for human–machine interaction while giving rise to profound challenges concerning privacy and personal data protection. These challenges have received limited attention in Persian-language scholarship, and the present article seeks to serve as a starting point for further Persian-language research in this emerging field. The central research question is: To what extent can different policy approaches protect privacy against the risks posed by these technologies while maintaining a balance between such protection and the freedom to innovate?

This study aims to elucidate the legal dimensions of these risks, comparatively evaluate different policy approaches, and identify an optimal regulatory model for these technologies. It adopts a descriptive-analytical method, drawing on a comparative analysis of policy approaches and a documentary and library-based review of relevant legal and scholarly sources. The study also identifies and presents the regulatory approach considered most appropriate by the authors. The findings indicate that concerns arising from the long-term storage of data, third-party access, government intervention, and the sensitivity of collected information underscore the need to review existing legal and regulatory frameworks in order to enhance the effectiveness of privacy protection and ensure that regulatory interventions are proportionate to the level of risk.. The analysis identifies two categories of privacy-protection strategies: first, non-legal approaches such as enhancing digital literacy, user self-regulation, and social-normative pressure; and second, legal approaches grounded in flexible, incremental, and risk-responsive policy measures. Within the policy domain, two primary approaches are examined: (1) ex-ante or ex-post rule-making that balances the precautionary principle with the freedom to innovate; and (2) data-minimization approaches that shift responsibility from data collection to data use. Additionally, evolving standards of civil liability and constraints on governmental access to private data constitute further key axes of this analysis. The study ultimately emphasizes the necessity of adopting a multilayered and participatory policy model—one that preserves the balance between data security and innovation freedom, and that is anchored in institutional transparency, developer accountability, and continuous oversight of privacy-related obligations.

Keywords: Internet of Things (IoT), wearable technologies, artificial intelligence, privacy

پذیرفته‌شده | در انتظار انتشار | نسخه‌ی اولیه | ویراستاری‌نشده
Accepted | Awaiting Publication | Draft Version | Unedited