فصلنامه مطالعات حقوق خصوصی، دورهٔ ۵۱، شمارهٔ ۴، زمستان ۱۴۰۰، صفحات ۷۱۵- ۶۹۵ (مقاله علمی پژوهشی)

بررسی خطرهای تهدیدکنندهٔ حریم خصوصی و الزامات حقوقی حمایت از آن در استفاده از وسایل نقلیهٔ خودران

سبحان دهقان‌پور فراشاه
دانش‌آموختهٔ کارشناسی ارشد حقوق تجارت بین‌الملل، دانشکدهٔ حقوق دانشگاه شهید بهشتی تهران
نوید رهبر*
استادیار حقوق تجارت بین‌الملل و مالکیت فکری، دانشکدهٔ حقوق، دانشگاه شهید بهشتی، تهران

چکیده

وسایل نقلیهٔ خودران، فناوری‌هایی هستند که توسط هوش مصنوعی از قدرت تصمیم‌گیری و تجربه‌آموزی بهره‌مند شده‌اند. این وسایل نقلیه که با حسگرهای متعدد اطلاعات فراوانی را جمع‌آوری می‌کنند، از طریق اینترنت اشیا با یکدیگر و با همه چیز در ارتباط‌اند و اطلاعات را در شبکه‌هایی منتقل می‌کنند که در دسترس تأسیسات شهری و جاده‌ای قرار می‌گیرد؛ اطلاعاتی که می‌تواند منتسب به شخصی باشد و ذیل حریم خصوصی وی بیاید. در چنین شبکه‌هایی، حریم خصوصی اشخاص با خطرهایی مواجه می‌شوند که قانونگذار باید آنها را به‌منظور پیشگیری از نقض حریم خصوصی بشناسد. تحقیق حاضر تعابیر حریم خصوصی در قوانین کشورهای اروپایی و ایالات متحدهٔ آمریکا، و اندیشه‌ها تا تعبیر مناسب را بیابد، و از رهگذر ویژگی‌های وسایل نقلیهٔ خودران، مربوط به نحوهٔ جمع‌آوری و به‌کارگیری اطلاعات در مراحل چرخهٔ حیات اطلاعات، و مطالعهٔ پرونده‌ها، محققان و قانونگذار را با خطرهایی آشنا می‌سازد که در استفاده از این فناوری متوجه حریم خصوصی می‌شود و به فراخور هر مرحله الزاماتی حقوقی را برای پوشش این خطرها معرفی می‌کند.

واژگان کلیدی

اطلاعات شخصی، چرخهٔ حیات اطلاعات، داده‌های شخصی، فناوری خودکار، هوش مصنوعی.

* نویسندهٔ مسئول Email: n_rahbar@sbu.ac.ir

تاریخ دریافت: ۲ خرداد ۱۴۰۰، تاریخ تصویب: ۱۳ آذر ۱۴۰۰
DOI:10.22059/JLQ.2021.323088.1007535

۱. مقدمه

استفاده از اینترنت اشیا و نسل پنجم که همه چیز را در شهرهای هوشمند به یکدیگر متصل می‌کند، از چشم‌اندازهای نه‌چندان دور جوامع پیشرفته است. در این شهرها، اشخاص، ماشین‌ها، تأسیسات و همه چیز با شبکه‌هایی به‌هم متصل‌اند. وسایل نقلیهٔ خودران (خودران‌ها) به‌عنوان یکی از این ماشین‌ها و نمودی از هوش مصنوعی، با استفاده از حسگرهای متعدد خود، اطلاعات فراوانی را جمع‌آوری، پردازش و استفاده می‌کنند، و از طریق اینترنت اشیا این اطلاعات را میان یکدیگر منتقل می‌سازند (Wang *et al.*, 2021: 1-3). اطلاعات بی‌شمار مورد استفادهٔ میلیون‌ها خودران، همگی می‌توانند دست‌کم در حریم خصوصی[1] یک شخص حقیقی یا حقوقی جای بگیرند. این جریان اطلاعات، هرچند لازمهٔ عملکرد خودران‌هاست، ولی این اطلاعات می‌توانند مورد دستیابی و دستیازی حکومت‌ها و کسب‌وکارها قرار بگیرند؛ کما اینکه در فناوری‌های مشابه و فعلی، حریم خصوصی اشخاص، توسط آنها نقض می‌شوند (قاسم‌زاده لیاسی و رئیسی دزکی، ۱۳۹۹: ۵۹۸).

این تحقیق درصدد است تا با تبیین مفهوم حریم خصوصی در عصر جدید، قانونگذار را با خطرهای خودران‌ها، هوش مصنوعی و اینترنت اشیا، برای حریم خصوصی و ابزارهای حقوقی لازم برای پوشش این خطرها آشنا سازد. بخش نخست به بیان مفهوم حریم خصوصی و مشخصات آن از نگاه این تحقیق پرداخته و سعی شده است تا ماهیت حریم خصوصی به‌درستی شناسانده شود؛ سپس خودران‌ها و چرخهٔ حیات اطلاعات، و در نهایت در پی شناسایی خطرهایی که اطلاعات را در این چرخه تهدید می‌کنند، الزامات حقوقی برای حمایت از آن معرفی شده‌اند.

۲.از حریم خصوصی تا صیانت از داده

محققان بسیاری در تعریف مفهوم حریم خصوصی کوشیده‌اند، اما بر ارائهٔ تعریفی جامع و مانع فائق نیامده‌اند (مقامی و عطاران، ۱۳۹۸: ۳۱۲). در این بخش تلاش‌هایی برای استفاده از واژهٔ حریم خصوصی، در سه دورهٔ زمانی بررسی می‌شوند، که این تعابیر در هر دوره با توجه به فناوری‌های ارتباطی آن زمان، ویژگی‌های خاصی دارند؛ در انتها تعبیر موردنظر این تحقیق بیان می‌شود.

تلاش‌های نخستین برای حمایت از حریم خصوصی در دوران جنگ انقلاب در ایالات متحدهٔ آمریکا (آمریکا) صورت گرفت، که به تصویب متمم‌های سوم، چهارم و پنجم قانون اساسی آمریکا انجامید (Smith, 2000: 50). البته تا پیش از این نیز می‌توان قائل به فرض حریمی

1. Privacy

برای اشخاص از جانب قوانین، قضات و مذاهب، با ممنوعیت استراق سمع و ورود به خانه‌ها بود (Backstone, 2016: 111). احترام به حریم خصوصی را می‌توان در ادیان مختلف، از جمله اسلام، مشاهده کرد (بادینی، ۱۳۹۱: ۹۹)؛ اما در سده‌های نوزدهم و بیستم میلادی، ظهور فناوری‌های نو، آبستنی برای توجه به حریم خصوصی بود. اولین قانون حامی حریم خصوصی در یک فناوری، با ظهور فناوری تلگراف در نیمهٔ دوم سدهٔ نوزدهم برای حمایت از حریم تلگراف‌ها در آمریکا تصویب شد (Seipp, 1981: 65). در این دوره بنابر رویهٔ قضایی، حمایت از حریم خصوصی، در واقع حمایت از امنیت و آزادی شخصی است و از حق مالکیت نشأت می‌گیرد (Boyd v. United States, 1886: para. 616).

با ظهور دوربین‌های عکاسی قابل حمل در دهه‌های پایانی سدهٔ نوزدهم، و شوق عکاسانی که شیفتهٔ ثبت لحظات بودند، و در واکنش به کنجکاوی روزنامه‌نگاران در زندگی خصوصی اشخاص، مسئلهٔ حریم خصوصی به تعبیر «حق بر تنها بودن»[1] بیان شد (مقامی و عطاران، ۱۳۹۸: ۳۱۴)؛ حقی که عمومی‌تر از حق مالکیت و مربوط به حق تسلط بر میزان آگاهی دیگران از افکار، تمایلات و احساسات بود (Warren & Brandies, 1890: 198). در پرونده‌ای در ابتدای سدهٔ بیستم، حق بر تنها بودن از حقوق طبیعی شناخته شد؛ بدین‌منظور که افراد در زندگی دو انتخاب دارند، که در ارتباط با دیگران زندگی کنند، یا عزلت گزینند؛ چراکه انسان حق دارد زمان، مکان و شیوهٔ حضور خود در جامعه را تعیین کند. هر گاه برخلاف میل شخصی، زندگی وی (و در آن پرونده، بدن وی) در جامعه نمایش داده شود، حق مذکور نقض شده است (Pavesich v. New England Life Ins. Co., 1905: para. 70). بنابراین می‌توان معتقد بود که تعبیر از حریم خصوصی، تا این دوره، برای حمایت از حریم خلوت انسان است.

در پی نقض حریم خصوصی در دوران جنگ جهانی دوم و نیمهٔ دوم سدهٔ بیستم با اهداف سیاسی که چنین رویکردی با توجه به ملاحظات سیاسی توسط قضات نیز تأیید و قانونی شناخته می‌شد (Barenblatt v. United States, 1959: para. 109)، در اعلامیهٔ جهانی حقوق بشر[2] و کنوانسیون اروپایی برای حقوق بشر[3] در میانهٔ سدهٔ بیستم میلادی، حریم خصوصی به‌عنوان «یک حق بشری بر احترام به زندگی شخصی و خانوادگی و ارتباطاتش» بیان شد.[4] با بیان مفهوم حقوق بشر، حریم خصوصی دیگر صرفاً امری شخصی در نظر گرفته نمی‌شد، بلکه مسئله‌ای اجتماعی و ابزاری برای حمایت از اشخاص در برابر حکومت‌ها و محدود کردن صلاحیت حاکمان بود (Henkin, 1974: 1419). در این دوره استفاده از اطلاعات شخصی اصولاً

1. The Right to Be Let Alone
2. Universal Declaration of Human Rights 1948 (UDHR)
3. European Convention on Human Rights 1950 (ECHR)
4. Article 8 of ECHR, Article 12 of UDHR

غیرمجاز شمرده می‌شد، مگر آنکه قانون در شرایطی این رفتار را تجویز کند (Henkin, 1974: 1420). در اصول ۲۲، ۲۳، و ۲۵ قانون اساسی جمهوری اسلامی ایران، مادهٔ ۲۴ قانون آیین دادرسی کیفری (شهبازی، ۱۳۹۵: ۴۲۰) و در فرامین ششم، هفتم و هشتم رهبر وقت ایران در سال ۱۳۶۱، مراد از حریم خصوصی، تعبیر مشابهی بوده است. چنین برداشتی از حریم خصوصی اکنون نیز مورد پذیرش است؛ ضرورت حفظ حریم خصوصی در دادرسی کیفری نیز از همین منظر مورد توجه حقوقدانان ایرانی بوده است (آقابابایی و موسوی، ۱۳۹۲: ۲۶-۲۷). با وجود این، دولت‌ها به بهانه‌های متعدد (صرف‌نظر از مشروعیت آن)، از جمله امنیت ملی و مبارزه با تروریسم دست به نقض حریم خصوصی زده‌اند؛ مثل دسترسی به اطلاعات و ایمیل‌های شخصی از جانب آمریکا (قاسم‌زاده لیاسی و رئیسی دزکی، ۱۳۹۹: ۶۰۲).

در اواخر سدهٔ بیستم و اوایل هزارهٔ سوم، زمانی‌که در آمریکا منافع سیاسی و اقتصادی به نقض حریم خصوصی گره خورده بود، کشورهای اروپایی برای حمایت از حریم خصوصی شهروندان، قوانینی را وضع کردند تا اطلاعات شخصی حاصل سرشماری‌ها محفوظ بمانند. با پیشرفت چشمگیر فناوری‌های جمع‌آوری و پردازش اطلاعات مثل رایانه‌ها و بانک‌های داده، دغدغهٔ حمایت از حریم خصوصی شهروندان پررنگ‌تر شد. در آن دوران، از اصطلاح صیانت از داده[1] برای حمایت از حریم خصوصی اشخاص استفاده شد و نشانی از عبارات حریم خصوصی[2] یا اطلاعات[3] نبود؛ اصطلاحی که به عقیدهٔ بسیاری موجب اشتباه در موضوع حمایت قانونی بود؛ چراکه داده به صیانت نیازی ندارد و موضوع حمایت قانونی باید شخصی باشد که داده به او مرتبط می‌شود (شخص موضوع داده). عبارت صیانت از داده، از پی نگرشی طرح شد که رایانه و پردازش اطلاعات را مشکل اصلی می‌دانست، و در جهت رفع این مشکل، مقرراتی به‌منظور تنظیم استفاده از رایانه و کنترل پردازش اطلاعات در راستای منافع جامعه تصویب شد (Mayer-Schönberger, 1998 :223-224). نگاه کنونی قوانین به داده‌ها توجه دارد تا حریم خصوصی که مقررات عمومی صیانت از داده در اروپا[4]، و قانون حریم خصوصی مصرف‌کننده[5] و قانون حریم خصوصی در ایالت کالیفرنیا[6] (قانون اخیر از سال ۲۰۲۳ میلادی لازم‌الاجرا می‌شود)، از جملهٔ این مواردند. این در حالی است که استفاده از مفهوم صیانت از داده موجب حمایت ناقص از حریم خصوصی می‌شود (Mayer-Schönberger, 1998 :219). ماهیت داده‌های شخصی و حریم خصوصی متفاوت است؛ حریم خصوصی، مجموعه‌ای از

1. Data Protection
2. Privacy
3. Information
4. General Data Protection Regulation
5. California Consumer Privacy Act
6. California Privacy Act

عناوین است که اطلاعات اشخاص ذیل آن طبقه‌بندی می‌شود. درحالی‌که داده‌ها، اطلاعاتی هستند که شخص موضوع آن می‌تواند معین نباشد. به‌عبارت دیگر، نمی‌توان داده را به شخص معینی مرتبط ساخت. زمانی‌که آن اطلاعات به شخصی مرتبط شد، می‌توان از آن به‌عنوان داده‌های شخصی یاد کرد و ذیل حریم خصوصی آورد (قاسم‌زاده لیاسی و رئیسی دزکی، ۱۳۹۹: ۵۹۹). ازاین‌رو در این پژوهش نیز از اصطلاحات حریم خصوصی و اطلاعات استفاده شده است.

تعابیر حریم خصوصی دورهٔ حاضر، به‌منظور شناسایی اختیار اشخاص بر تبادل، و کیفیت و کمیت تبادل اطلاعاتشان با دیگران است، به‌نحوی که بتوان از منافعی که در گرو اطلاعات اشخاص است نیز بهره‌مند شد. این تعبیر راهکاری است که به ایجاد توازن میان حمایت از حریم خصوصی در برابر فناوری اطلاعات از یک سو و از سوی دیگر کمک به رشد فناوری و نوآوری منجر می‌شود. با چنین دیدگاهی، اشخاص می‌توانند از محتوای حساس حریم خصوصی خود حفاظت کنند و باقی اطلاعات شخصی خود را با رضایت و ارائهٔ مجوز خاص در اختیار دیگران قرار دهند (Nissenbaum, 2010: 231).

۳. اتصال خودران‌ها و حریم خصوصی

حسگرهای خودران جمع‌آوری اطلاعات فراوانی را، که شامل همهٔ ابعاد حریم خصوصی[۱] می‌شوند، ممکن می‌سازند (Zepf *et al.*, 2020: 3). برای نمونه، خودران‌ها برای شناسایی اجسام در حال حرکت از سه نوع حسگر استفاده می‌کنند؛ رادار، دوربین و لیدار[۲]. رادار با تشخیص هدف، دوربین با فراهم آوردن تصویر، و لیدار با موقعیت‌یابی و نقشه‌برداری مداومْ اجسام در حال حرکت را تشخیص می‌دهند (Kocić *et al.*, 2018: 424).[۳]

خودران‌ها به مرور از استقلال کامل به سمت اتصال پیش می‌روند. به‌عبارت دیگر، به‌جای اینکه خودران‌ها اطلاعات مورد نیاز خود را صرفاً از حسگرهای خود جمع‌آوری کنند و آنها را در خود ذخیره سازند، اطلاعات دریافتی از حسگرها را در فضایی ابری میان خود و دیگر خودران‌ها و تأسیسات به اشتراک می‌گذارند تا بتوانند با دسترسی به اطلاعاتی جامع در خصوص محیط پیرامون، تصمیمات بهتری اتخاذ کنند (Xiong *et al.*, 2020: 24). در خودران‌های مستقل، به‌طور کلی اطلاعات در سه مرحلهٔ دریافت، پردازش و مبنای تصمیم واقع می‌شود. این اطلاعات در فضای خارجی مبادله نمی‌شود و از تأسیسات و خودران‌های

---

۱. حریم خصوصی طبق نظر اندیشمندان به ابعاد مختلفی تقسیم شده است که این ابعاد در یک تقسیم‌بندی «موقعیت مکانی»، «وضعیت جسمی و روانی»، «رفتار و اعمال»، «زندگی اجتماعی» و «رسانه» بیان شده‌اند.

2. Lidar

۳. نحوهٔ کار چنین حسگرهایی و امکان تشخیص چهره و احساسات توسط خودران‌ها را می‌توان در منابع ارجاع‌شده مشاهده کرد.

دیگر نیز اطلاعاتی وارد نمی‌شود (Chang *et al*., 2020: 357-358)؛ بنابراین با توجه به عدم دخالت عوامل خارجی در مراحل مذکور، دغدغه‌های مربوط به حریم خصوصی و صیانت از داده نیز هرچند از بین نخواهد رفت، سطح پایینی خواهد داشت.

خودران‌های متصل در محیط خود، اطلاعات را در شبکه‌های بین خودران‌ها، خودران–تأسیسات، خودران–عابر پیاده، و خودران–همه چیز مبادله می‌کنند (Misra *et al*., 2017: 78). اتصال خودران‌ها می‌تواند خطرهای متعددی را برای حریم خصوصی ایجاد کند. اطلاعات در این فضا به خودران‌ها و تأسیسات بسیاری منتقل می‌شوند و در دسترس اشخاص قرار می‌گیرند و حتی اطلاعات ممکن است در مسیر این انتقالات سرقت شوند، ازاین‌رو چه دسترسی با مجوز و چه بدون مجوز به اطلاعات می‌تواند منشأ خطرهایی برای حریم خصوصی باشد. نهادهایی همچون شرکت‌های صوری، می‌تواند با در دست داشتن و سوء استفاده از اطلاعات شناسایی بسیاری از اشخاص تشکیل شوند. با اتصال خودران‌ها و دیگر وسایل، می‌توان موقعیت مکانی و اطلاعات شخصی افراد را پیگیری کرد (Bansal *et al*., 2021:203). اطلاعات موقعیت مکانی که توسط مکان‌یاب‌های خودران یا مخابرهٔ اطلاعات با تأسیسات مربوط جمع‌آوری می‌شوند، می‌توانند علیه شخص موضوع آن مورد استناد در دادگاه قرار بگیرند؛ برای نمونه اف بی آی در پرونده‌ای از طریق جمع‌آوری بیش از ۱۲ هزار نقطهٔ مکانی متهم طی ۱۲۷ روز و پردازش آن اطلاعات، دریافت که وی به‌هنگام وقوع چهار فقره سرقت مقرون به آزار و اذیت[1] در نزدیکی آن محل‌ها بوده است (Carpenter v. US, 2018: para. 2206). همچنین این اطلاعات می‌تواند کسب‌وکارهایی را به طرق متعدد منتفع سازد. برای مثال در پرونده‌ای علیه گوگل[2]، ادعا شد که این شرکت از جمع‌آوری اطلاعات مکانی پردازش آن با دیگر اطلاعاتی مربوط به سلامتی که توسط مرکزی درمانی برای وی افشا شده است، می‌تواند به هویت بیماران دست یابد (Dinerstein v. Google, para. 2020). اطلاعات مربوط به وضعیت جسمانی و روانی نیز می‌توانند در معرض خطر باشند. چنین اطلاعاتی توسط حسگرهای داخل خودران، مربوط به بررسی وضعیت هوشیاری سرنشینان یا حسگرهای خارجی مربوط به وضعیت هوشیاری عابران پیاده می‌توانند جمع‌آوری شوند (Mangal & Nooteboom, 2021). دسترسی به اطلاعات مربوط به علایق اشخاص توسط نتفلیکس[3] و فروش یا استفاده از آن برای اهداف تبلیغاتی (Mollett v. Netflix, 2015: para. 1062) که ذیل حریم خصوصی اعمال و رفتار قرار می‌گیرد و مشابه آن را می‌توان در خودران‌ها با یافتن الگوهای رفتاری کاربران آن یافت. همچنین حسگرهای صوتی و تصویری داخل یا خارج خودران در کنار یافتن الگوهای

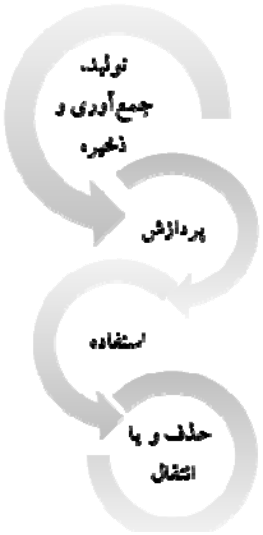
1. Robbery
2. Google
3. Netflix

رفتاری می‌تواند اطلاعاتی در خصوص روابط اجتماعی اشخاص به‌دست دهد. چنین تصاویر و صداهایی اطلاعاتی را در دسترس خودران و با انتقال آن داده‌ها در شبکه‌های متصل، در دسترس بی‌شمار تأسیسات و وسیله قرار می‌دهد که امکان شناسایی کاربران را به‌دست می‌دهد و ذیل حریم خصوصی رسانه می‌آیند.

بررسی جریان اطلاعات در خودران‌های متصل و اتفاقاتی که در این خودران‌ها می‌تواند برای حریم خصوصی رخ دهد، ملاکی برای بررسی خودران‌های مستقل نیز به‌دست می‌دهد، چراکه مستقل‌ها اخص مطلق خودران‌های متصل‌اند.

۴. خطرهای تهدیدکنندهٔ حریم خصوصی در خودران‌ها

چرخهٔ حیات اطلاعات[۱] مفهومی است که می‌تواند جریان اطلاعات را به‌خوبی نمایش دهد (Floridi, 2014: 5-6)؛ چرخه‌ای که در آن اطلاعاتْ تولید، جمع‌آوری، ذخیره و تحلیل می‌شود و سپس مورد استفاده، حذف یا انتقال قرار می‌گیرد و مجدداً اطلاعات منتقل یا تولیدشده وارد چرخه می‌شود (شکل ۱). با بررسی وضعیت اطلاعات تشکیل‌دهندهٔ حریم خصوصی در چرخهٔ حیات، در ارتباط با خودران‌های متصل (خودران‌ها)، می‌توان تهدیداتی را که متوجه حریم خصوصی می‌شوند، شناسایی کرد.



شکل ۱. چرخهٔ حیات اطلاعات

منظور از خطرهای تهدیدکنندهٔ حریم خصوصی، رفتارهایی است که نقض حریم خصوصی را سبب می‌شوند. این رفتارها را انواع تعرض به حریم خصوصی می‌نامد (Kaspar, 2005: 76). این خطرها ذیل چهار عنوان رفتار جمع‌آوری اطلاعات[۲]، پردازش اطلاعات[۳]، انتشار اطلاعات[۴]

۱. الهام گرفته‌شده از چرخهٔ حیات اطلاعات (The Life Cycle of Information) ارائه‌شده توسط:
Floridi Luciano, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality*, 1st Edition, United Kingdom: Oxford University Press, 2014, pp. 5-6.

2. Information Collection
3. Information Processing
4. Information Dissemination

و تجاوز[1] قرار می‌گیرند (Solove, 2006: 490). این خطرها را می‌توان در هریک از مراحل چرخهٔ حیات اطلاعات متوجه حریم خصوصی دانست؛ خطرهایی که از طرف هر دو فناوری هوش مصنوعی و اینترنت اشیا خودران را تهدید می‌کنند. هرچند پیشتر خطرهای اینترنت اشیاءبرای حریم خصوصی بیان شد، اما این فناوری با همراهی هوش مصنوعی دغدغه‌های مضاعفی برای محافظت از اطلاعات ایجاد می‌کند.

بسیاری از اقدام‌های لازم برای محافظت از حریم خصوصی و پوشش این خطرها باید در زمان طراحی محصول مورد توجه واقع شوند، با وجود این اقدام‌های حقوقی نقش مهمی در پیشگیری از نقض حریم خصوصی ایفا می‌کنند. لزوم تأمین امنیت اطلاعات و شفافیت از جمله اقداماتی هستند که در تمامی مراحل چرخهٔ حیات مورد نیاز است. اقدام‌های تأمین امنیت باید با رصد کردن مداوم محیط حیات اطلاعات همراه باشد تا اقدام‌های مناسبی با توجه پیشرفت روزانهٔ فناوری‌ها انجام گیرند. این اقدام‌ها در مادهٔ ۲۴.۱ مقررات اروپایی و بند الف۱- مادهٔ ۱۷۹۸.۱۵۰ قانون کالیفرنیا لازم دانسته شده‌اند. استفاده از فرایندهایی برای حفظ محرمانگی و شناسایی کاربر برای دسترسی به اطلاعات و رمزگذاری داده از جمله مواردی هستند که شرکت‌های فناوری هم‌اکنون برای حفظ امنیت اطلاعات از آن بهره می‌برند (Tamò-Larrieux, 2018 :105). آگاهی شخص موضوع اطلاعات از کیفیت و کمیت اطلاعات جمع‌آوری‌شده و دسترسی به آنها، و هدف پردازش اطلاعات و استفاده از آنها از الزامات شفافیت است. لزوم شفافیت از مشتقات حق بر ایفای نقش[2] شخص موضوع داده است، که باید در طراحی محصول مورد توجه قرار گیرد. به‌منظور تضمین حقوق شخص موضوع اطلاعات، که معمولاً در موقعیت ضعیف‌تری نسبت به کنترل‌کننده قرار دارد، لازم است که اقدام‌های قانونی به‌نحوی باشد که محافظت از حریم خصوصی را با افزایش شفافیت تضمین کند. قانونگذار می‌تواند با در نظر گرفتن جریمه یا محرومیت‌هایی، منافع اقتصادی و اجتماعی اشخاص نقض‌کنندهٔ حریم خصوصی را مورد هدف قرار دهد. همچنین لازم است تا با تأسیس نهادهایی قانونی، برخورد حریم خصوصی شهروندان با این فناوری و شرکت‌های ارائه‌دهندهٔ آن به‌نحو مستمر رصد شود تا ضمن پیشگیری از وقوع نقض حریم خصوصی با بررسی فنی طراحی فناوری از لحاظ تضمین حق بر حریم خصوصی، در صورت وقوع تصمیمات فوری و متناسب اخذ شود (Tamò-Larrieux, 2018:108,109).

1. Invasion
2. Participation Right

۴.۱. جمع‌آوری اطلاعات

اینکه به چه اطلاعاتی نیاز است، چه استفاده‌ای از آن می‌شود، از کجا می‌آید و کجا ذخیره می‌شود، پرسش‌هایی است که برای جمع‌آوری اطلاعات پاسخ داده می‌شود. این مرحله از چرخه را می‌توان شامل تولید و بازتولید داده توسط خودران یا ورود دستی متصدی، دریافت داده از خودران، زیرساخت‌ها یا هر چیز دیگر، جمع‌آوری و ذخیره آن دانست. یک خودران از نظر فضا، دو نوع آگاهی دارد؛ آگاهی خارجی و داخلی. اطلاعاتی مانند مشخصات متصدی و سرنشینان، وضعیت جسمی و روحی، رفتارها و احساسات آنها از یک طرف و مشخصات فنی، وضعیت صحت عملکرد وسیلهٔ نقلیه، و میزان سوخت یا انرژی از طرف دیگر، آگاهی‌هایی هستند که خودران نسبت به فضای داخلی خود کسب می‌کند (Rangesh *et al*., 2018: 190-193). آگاهی‌هایی که خودران از فضای خارجی کسب می‌کند، اطلاعاتی است از موقعیت جغرافیایی خود، وضعیت دیگر وسایل نقلیه، عابران و هر چیز دیگر و موقعیت آنها نسبت به خود، که توسط حسگرهای خودران، فضاهای ابری شبکه‌های موقت یا فناوری‌های کنار جاده‌ای می‌شود (Endsley, 2019: 303-306).

جمع‌آوری اطلاعات را ابتدایی‌ترین رفتاری می‌دانند که خطر نقض حریم خصوصی را در پی دارد. تمامی خودران‌ها و تأسیسات شهری، اطلاعات را برای تصمیم‌گیری‌های مختلفی جمع‌آوری می‌کنند (Han *et al*., 2020: 1-2). این رفتار از نگاه سولو با پرسش[1] و نظارت[2] صورت می‌گیرد؛ در کلام وی، مراد از پرسش، کسب اطلاعات فراوان و طی مدتی طولانی است که می‌تواند با پرسش‌های ابتدایی و جمع‌آوری اطلاعات در طول مدت استفاده از خودران صورت گیرد. نظارت و پرسش از نگاه وی، به‌عنوان یکی از ابزارهای قدرت، اسباب کنترل رفتارهای اشخاص را فراهم می‌آورد، چراکه نتیجهٔ آن به جمع‌آوری اطلاعات محدود نمی‌شود و می‌تواند به تحدید و تغییر رفتارهای اشخاص، خودسانسوری و بازداری از بروز تفکرات و احساسات بینجامد (Solove, 2006: 491-505)؛ به‌خصوص زمانی‌که اطلاعات در اختیار نهادهای دولتی، رسانه و اهل آن قرار گیرد.

از جمله مهم‌ترین الزامات حقوقی برای محافظت از حریم خصوصی در مرحلهٔ جمع‌آوری اطلاعات می‌توان به لزوم اخذ رضایت و تحصیل حداقلی اطلاعات اشاره کرد. شخص موضوع اطلاعات باید پیش از جمع‌آوری اطلاعاتش نسبت به آن رضایت بدهد؛ رضایتی که باید با آگاهی از نوع اطلاعات و هدف پردازش آنها اخذ شود. چنین تکلیفی بر پردازش‌کنندهٔ اطلاعات است، و آزادی انتخاب و اختیار اعمال حق شخص موضوع اطلاعات را تضمین

1. Interrogation
2. Surveillance

می‌کند. نمونهٔ شناسایی چنین حقی در مادهٔ ۲ قانون حریم خصوصی مصرف‌کننده در کالیفرنیا (قانون کالیفرنیا) و بند ۲ مادهٔ ۷ مقررات عمومی صیانت از داده در اروپا (مقررات اروپایی) آمده است. از طرف دیگر، میزان و نوع اطلاعات جمع‌آوری‌شده باید همانی باشد که برای هدف پردازش کاربرد دارد، تا با جمع‌آوری اطلاعات فراوان خطر نقض حریم خصوصی افزایش پیدا نکند. در مقررات اروپایی (بند «پ» مادهٔ ۱.۵) برخلاف قانون کالیفرنیا چنین تکلیفی شناسایی شده، البته قانون جدید حریم خصوصی کالیفرنیا[1] چنین حقی را شناسایی کرده است. در نظر گرفتن این مسئله به‌هنگام طراحی خودران اهمیت بسزایی دارد، چراکه باید طراحی سیستم‌ها به‌گونه‌ای باشد تا اطلاعات را با نیاز حداقلی و در موارد معین دریافت کنند، در غیر این صورت اطلاعات بی‌شماری توسط حسگرهای خودران جمع‌آوری می‌شوند که ذیل حریم خصوصی بسیاری اشخاص قرار می‌گیرند. از دیگر موارد طراحی به نفع حریم خصوصی، جمع‌آوری اطلاعات به‌طور ناشناس است، به‌نحوی که اطلاعات بدون امکان شناسایی شخص موضوع آن جمع‌آوری و مبادله شود. با چنین طراحی‌ای، اطلاعات جمع‌آوری‌شده صرفِ داده هستند و به شخص خاصی تعلق ندارند، ازاین‌رو خطر نقض حریم خصوصی کاهش می‌یابد (Deng *et al*., 2021: 151). چنین داده‌های ناشناسی مشمول هیچ‌یک از دو مقررهٔ بیان‌شده نمی‌شوند.

۴.۲. پردازش اطلاعات

تجمیع و طبقه‌بندی ورودی‌ها، امکان استخراج اطلاعات مفید و یافتن الگوهای رفتاری را به‌دست می‌دهد. چنین پردازشی قدرت پیش‌بینی رفتارهای اشخاص و وسایل نقلیه را به‌دست می‌دهد که از جمله مهم‌ترین عملکردهای هوش مصنوعی خودران است (Anderson *et al*., 2020: 6892-6893). خودران با شناسایی جسم، عنوانی (عابر پیاده، خودرو، کشتی و...) را برای آن در نظر می‌گیرد و با توجه به سابقهٔ رفتارهای آن، اقدام به تصمیم‌گیری مقتضی می‌کند؛ سابقه‌ای که از اطلاعات پیشتر به‌دست‌آمده در اختیار دارد. سپس از تصمیمات و نتیجهٔ آن کسب تجربه کرده و اطلاعات را اصلاح و به‌روز می‌کند (Xu *et al*., 2020: 9523-9524). این رفتار را می‌توان تشخیص موضوع اطلاعات نامید؛ رفتاری که در پی آن اطلاعات به اشخاص مرتبط می‌شود (Solove, 2006: 491-551).

پردازش اطلاعات از نگاه سولوْ حریم خصوصی را با تجمیع و طبقه‌بندی[2]، تشخیص موضوع[3]، آسیب‌پذیری[1]، استفادهٔ ثانویه[2] و محروم‌سازی[3] متوجه خطرهایی می‌کند. تجمیع و

۱. مادهٔ پیشنهادی ۱۷۹۸.۱۰۰

2. Data Aggregation
3. Identification

دسته‌بندی رفتاری است که به گردآوری اطلاعات و دستیابی به گستره‌ای از اطلاعات یک شخص منجر می‌شود؛ چنانچه وی انتظار یا رضایت از چنین پردازشی را نداشته باشد یا اطلاعاتی که در کنار هم گذاشته شده‌اند به تشکیل مجموعه اطلاعاتی غیرواقعی یا تبعیض‌آمیز منجر شود (Danks & London, 2017: 4691, 4693)، حریم خصوصی وی به خطر می‌افتد. تشخیص موضوع، فرایندی است که طی آن اطلاعات جمع‌آوری‌شده که لزوماً به موجود خاصی منسوب نیستند، به یک شخص یا موجود فیزیکی نسبت داده می‌شود؛ این رفتار می‌تواند موجب جلب توجه، نظارت، برچسب زدن و سوگیری، تحدید فعالیت، خودسانسوری و بازداری شود (Ntoutsi *et al*., 2020: 2-3). آسیب‌پذیری رفتارهای بسیاری را شامل می‌شود، مثل سرقت هویت، سوء استفاده از اطلاعات و اخاذی. به‌طور کلی می‌توان احساس عدم امنیت ناشی از دو مرحلهٔ جمع‌آوری و تشخیص موضوع دانست؛ زمانی‌که اطلاعات در اختیار اشخاصی با سوء نیت قرار می‌گیرد (Kim & Shrestha, 2020: 44). استفادهٔ ثانویه رفتاری است که طی آن از اطلاعاتی که ابتدائاً برای هدف خاصی جمع‌آوری شده و مورد رضایت شخص موضوع آن بوده است، برای هدف دیگری استفاده می‌شود (Bloom *et al*., 2017: 357-358). خودران اطلاعاتی را که جمع‌آوری می‌کند، ابتدائاً از آنها برای تصمیم‌گیری استفاده می‌کند. چنانچه این اطلاعات برای اهدافی مانند تشخیص چهره و شناسایی اشخاص به‌کار رود، می‌توان آن را استفادهٔ ثانویه دانست. ثانویه یا اولیه بودن رفتار به نحوهٔ عملکرد دستگاه و رضایت موضوع آن بستگی دارد. برای مثال ممکن است اطلاعات جمع‌آوری‌شده در همان مرحلهٔ ابتدایی عملکرد دستگاه مورد فرایندی قرار بگیرد که موضوع آن اطلاعات (شخصی که اطلاعات مربوط به آن است) نسبت به آن فرایند رضایت نداشته باشد (Bloom *et al*., 2017: 366-367). حال این فرایند می‌تواند در خودران رخ دهد، همچنین فرایندی باشد که توسط شرکت ارائه‌دهندهٔ خدمات، دولت یا هر شخص دیگری انجام گیرد. در هریک از این حالت‌ها چنانچه دسترسی مجاز یا رضایت نباشد، حریم خصوصی نقض شده است. محروم‌سازی شامل اطلاع ندادن به اشخاص برای جمع‌آوری و استفاده از اطلاعاتشان، و محدود ساختن دسترسی ایشان به اطلاعات جمع‌آوری‌شده می‌شود (Solove, 2006: 505-525). در حالتی که اطلاعات جمع‌آوری‌شده از کاربر صحیح نباشد، به اتخاذ تصمیم نامناسب از سوی خودران منجر می‌شود. برای مثال یک تاکسی خودران، شخصی را به‌دلیل تشخیص چهرهٔ اشتباه، یک مشتری بدحساب تشخیص می‌دهد و از سوار کردن وی خودداری می‌کند (Such, 2017: 4762). ازاین‌رو لازم است، شخص بتواند به اطلاعات دسترسی پیدا کند.

1. Insecurity
2. Secondary Use
3. Exclusion

در این مرحله از چرخهٔ حیات اطلاعات نیز الزاماتی حقوقی و فنی را می‌توان در نظر گرفت تا این خطرها را پوشش دهد؛ از جملهٔ این الزامات، محدودیت هدف پردازش، محدودیت افشا و استفاده از اطلاعات و امکان اصلاح اطلاعات است. اینکه اطلاعات جمع‌آوری‌شده برای همان هدفی که نسبت به آن رضایت داده شده (یا اهدافی که در راستای رسیدن به آن هدف هستند) پردازش شوند، دغدغه‌ای است که باید با ابزارهای حقوقی آن را پاسخ داد؛ هرچند به‌طور معمول در فرم‌های اخذ رضایت موارد وسیعی را ذکر می‌کنند تا از نقض احتمالی حریم خصوصی در پردازش اطلاعات برای اهداف مختلف جلوگیری شود. این دغدغه که به‌طور مستقیم به رضایت شخص موضوع داده و حق تمامیت وی بازمی‌گردد، در بند «ب» ماده ۱.۵ مقررات اروپایی و بند «ب» مادهٔ ۱ قانون کالیفرنیا پوشش داده شده است. دیگر مشتقات این حق را می‌توان با ایجاد محدودیت‌هایی برای افشا و استفاده از اطلاعات تضمین کرد، به‌نحوی که اطلاعات جمع‌آوری یا پردازش شده، به‌جز کنترل‌کننده و برای استفاده در موارد موضوع رضایت مأخوذه، به شخص یا استفادهٔ دیگری نرسد. همچنین از آنجا که اطلاعات جمع‌آوری‌شده توسط حسگرها یا دیگر درگاه‌های ورودی می‌تواند غیرواقعی باشد، لازم است تا امکان اصلاح اطلاعات برای شخص موضوع اطلاعات فراهم باشد. این امکان نیز از حق بر ایفای نقش و تمامیت شخص موضوع اطلاعات بازمی‌گردد که علاوه‌بر ابزارهای حقوقی، از لحاظ فنی نیز باید در مرحلهٔ طراحی محصول مورد توجه واقع شود (Coelho *et al*., 2021: 747). چنین حقوقی در مواد ۱۶ و ۱۸ مقررات اروپایی شناسایی شده‌اند، ولی در قانون کالیفرنیا مقرره‌ای در این خصوص نیست؛ با وجود این حقی کلی مبتنی بر امکان رد فروش اطلاعات شخصی در مادهٔ ۱۲۰.۱۷۹۸ این قانون وجود دارد.

۴.۳. استفاده از اطلاعات

اطلاعاتی که در مراحل پیشین جمع‌آوری و پردازش شده‌اند، برای استفاده در اختیار خودران قرار می‌گیرد. هوش مصنوعی برای تمامی عملکردهای خودران تصمیم‌گیری می‌کند؛ از زمانی‌که خودران را روشن، مقصد را انتخاب و حرکت می‌کند، تا زمانی‌که خودران به پارکینگ می‌رسد و پارک می‌شود (رهبر و دهقان‌پور فراشاه، ۱۴۰۰؛ ۵۲۶). تصمیم‌گیری‌های هوش مصنوعی با یادگیری از تجربیات همراه است. این فرایند هرچند لازمهٔ عملکرد مفید خودران، ولی منشأ احتمالی مشکلاتی از جمله سوگیری و تبعیض، تعرض و دخالت در تصمیم‌گیری است.

هوش مصنوعی، حتی با اطلاعات منطبق بر واقعیت، می‌تواند یادگیری‌هایی خلاف واقع یا تبعیض‌آمیز داشته باشد. چنین فرایندی می‌تواند در زمان آموزش اولیه یا هنگام عملکرد و در طول زمان استفاده صورت گیرد (DARPA, 2016: 10-13). فرضاً اگر در یک موتور

جست‌وجوی شغل، مردان بیشتری مشاغل یدی را دنبال کنند، موتور جست‌وجو چنین درک می‌کند که این مشاغل را برای زنان کمتر پیشنهاد دهد. چنین اتفاقی را می‌توان در استفاده از خودران‌ها نیز متصور شد. زمانی‌که خودران از محله‌ای با رانندگان کم‌احتیاط می‌گذرد، آن منطقه را ناامن تشخیص می‌دهد. چنین تجربه‌ای با دیگر خودران‌ها نیز به اشتراک گذاشته می‌شود و در نهایت (با دسترسی اشخاص خصوصی و عمومی به این اطلاعات) می‌تواند تأثیرات نامطلوبی برای آن منطقه داشته باشد. هرچند چنین رفتاری برای مطابقت عملکرد خودران با واقع، نزدیکی به رفتار انسان و پذیرش آن در اجتماع لازم است (Falco, 2019: 155)، ولی کنترل ورودی‌ها و اصلاح اطلاعات برای جلوگیری از سوگیری و تبعیض ناروا ضروری به‌نظر می‌رسد (Borgesius, 2020: 403-406).

از نگاه سولو، با استفاده از اطلاعات و دسترسی به آنها، حریم خصوصی در معرض تجاوز قرار می‌گیرد. تجاوز، که بالاترین سطح خطر برای حریم خصوصی است، به دو شکل می‌تواند صورت گیرد؛ تعرض[1] و دخالت در تصمیم‌گیری[2]. تعرض زمانی است که با افشای اطلاعات در روند زندگی شخص مزاحمت ایجاد شود (Solove, 2006: 553)، مثل تعقیب یک بازیگر توسط خبرنگاران، که به‌طور معمول چنین تعرضی در پی نظارت الگوهای رفتاری اتفاق می‌افتد. در استفاده از خودران، تعرض را می‌توان زمانی متصور شد که با دستیابی به آموخته‌های خودران، الگوهای رفتاری یک شخص یا اجتماع به‌نحو غیرمجاز در دسترس اشخاص خصوصی و عمومی قرار گیرد؛ چنین تعرضی می‌تواند منافع اقتصادی و سیاسی در پی داشته باشد (Oham *et al*., 2018: 4). دخالت در تصمیم‌گیری زمانی رخ می‌دهد که عوامل خارجی تأثیرات نامطلوبی بر زندگی شخص و تصمیم‌گیری‌های شخص بگذارند. همان اشخاص خصوصی و عمومی که به الگوهای رفتاری افراد و اجتماع دست یافته‌اند، با ایجاد موانع یا دستکاری شرایط، رفتارها را به سمت دلخواه خود هدایت می‌کنند (Federal Trade Commission, 2015). دخالت در تصمیم‌گیری، مثل هدایت ترافیک، نقض آزادی ارادهٔ انسان‌ها و خطری مسلم برای حریم خصوصی محسوب می‌شود (Solove, 2006: 552-562).

علاوه‌بر ابزارهای محدودیت هدف پردازش و محدودیت افشا و استفاده از اطلاعات، که به شخص موضوع اطلاعات این اختیار را می‌دهد که بر اطلاعات خود کنترل داشته باشد و کنترل‌کنندهٔ اطلاعات را از استفاده از اطلاعات برای اهداف و استفاده‌هایی غیر از استفادهٔ اولیه (که برای آن رضایت اخذ شده است) بازمی‌دارد، ابزار حقوقی دیگری که می‌تواند در راستای شناسایی حق بر تمامیت و اختیار بر اطلاعات به‌کار رود، شناسایی حق پذیرش و رد در این

1. Intrusion
2. Decisional Interference

مرحله است. شخص موضوع اطلاعات باید بتواند در این مرحله از چرخهٔ حیات اطلاعات، در خصوص استفاده از اطلاعاتش تصمیم‌گیری کند. شناسایی چنین حقی در مادهٔ ۲۱ مقررات اروپایی اتفاق افتاده است، ولی در قانون کالیفرنیا صرفاً با حق رد فروش اطلاعات شخصی می‌توان چنین حقی را اعمال کرد. اعمال این حق در هر حال مستلزم وجود شفافیت در طراحی سیستم است تا شخص موضوع اطلاعات بداند اطلاعات پردازش‌شده برای چه هدفی و توسط چه شخصی به‌کار می‌رود تا بتواند در خصوص استفاده از اطلاعاتش به‌طور کلی یا جزئی اعلام عدم رضایت یا درخواست حذف اطلاعات کند (Coelho *et al*., 2021: 744).

۴.۴. حذف یا انتقال اطلاعات

اطلاعاتی که طی فرایندهای مختلف در خودران، جمع‌آوری، طبقه‌بندی و پردازش و استفاده شود، سرانجام حذف یا انتقال خواهد یافت. حذف و ذخیرهٔ اطلاعاتی که مورد نیاز هوش مصنوعی نیست و انتقال اطلاعات به شبکه‌های متعدد خارجی، همگی موجد خطرهایی هستند که متوجه حریم خصوصی می‌شود. حذف اطلاعات از خودران، چنانچه با رضایت کاربر نباشد، دسترسی ایشان را از اطلاعات مورد استفاده و یادگیری قطع می‌کند و کاربر امکان تغییر آنها را ندارد. انتقال اطلاعات خطرهایی را در پی دارد که می‌توان ذیل خطر انتشار اطلاعات بیان کرد. انتشار اطلاعات از نگاه سولو رفتاری است که به موجب آن اطلاعات پردازش‌شده افشا می‌شوند، یا توافقات محرمانگی نقض می‌شوند. نقض محرمانگی[1] زمانی است که توافقی قبلی مبنی بر عدم افشای اطلاعات خاصی میان اشخاص صورت می‌گیرد و از جانب آنان رعایت نمی‌شود؛ چنین رفتاری به‌سبب وجود قرارداد میان طرفین و نقض آن، با افشای اطلاعات متفاوت است، هرچند نتیجتاً اطلاعات شخص در پی این رفتار افشا می‌شوند. افشاگری[2] به‌طور معمول برای اطلاعاتی رخ می‌دهد که شخص انتظار یا رضایت افشای آن را ندارد و در پی این رفتار، به منافع وی آسیب می‌رسد (Solove, 2006: 525-552). این اطلاعات می‌تواند منطبق بر واقع باشد یا نباشد؛ در هر صورت نتیجهٔ امر نقض حریم خصوصی شخص موضوع اطلاعات و یا کاربر خودران است (Solove, 2006: 526). انتقال اطلاعات از خودران‌ها از یک طرف و از طرف دیگر ذخیرهٔ آنها درون خودران، خطر دسترسی و در نهایت انتشار آنها را در پی خواهد داشت.

حق بر حذف اطلاعات که برآمده از حق بر فراموشی است، در مادهٔ ۱۷ مقررات اروپایی و مادهٔ ۱۰۵.۱۷۹۸ قانون کالیفرنیا شناسایی شده است. اهمیت شفافیت در این مرحله پرواضح است، چراکه لازم است تا شخص موضوع اطلاعات بتواند اطلاعاتش را حذف کند، بداند

1. Breach of Confidentiality
2. Disclosure

اطلاعاتش حذف شده‌اند، بداند به چه اشخاصی منتقل شده‌اند یا به چه هدف و تا چه مدتی ذخیره می‌شوند. اینکه اطلاعات با چه هدفی ذخیره و مجدداً استفاده می‌شوند، باید در محدودهٔ هدف ابتدایی جمع‌آوری اطلاعات باشد و میزان و نوع اطلاعات ذخیره‌شده باید محدود به مورد استفادهٔ آتی باشد. علاوه‌بر شفافیت در این مرحله به‌نظر می‌رسد که لازم است تا شخص موضوع اطلاعات رضایت مضاعفی برای ذخیره و استفادهٔ مجدد اطلاعاتش داده باشد (Coelho *et al*., 2021: 744).

۵. نتیجه

در عصر حاضر، به تعبیری از حریم خصوصی روی آورده شد که اختیار اشخاص بر تبادل، کیفیت و کمیت تبادل اطلاعاتشان با دیگران را تضمین می‌کند، به‌نحوی که بتوان از منافعی که در گرو اطلاعات اشخاص است نیز بهره‌مند شد. زمانی‌که اطلاعات مختلف از طریق فناوری خودران جمع‌آوری، ذخیره، پردازش، استفاده، حذف و در شبکه‌های به‌هم متصل منتقل می‌شوند، در معرض خطرهایی قرار می‌گیرند.

هرچند استفاده از چنین اطلاعاتی برای پیشرفت فناوری‌ها، تطابق هرچه بیشتر خودران‌ها با رفتار یک انسان راننده و در نهایت پذیرش آن در جامعه ضروری است و با اینکه نمی‌توان گفت دسترسی به اطلاعات شخصی همواره متضمن ضرر برای شخص موضوع اطلاعات یا جامعه است، باید پذیرفت که تمامی این رفتارها خطرهایی هستند که حریم خصوصی را تهدید می‌کنند و لازم است تا با شناخت بیشتر حریم خصوصی و این خطرها، و لذا اشراف بر مقتضیات حمایت از این حریم، در جهت وضع مقرراتی برای نظام‌مند ساختن چرخهٔ حیات اطلاعات شخصی در فناوری‌ها گامی مناسب برداشت. اطلاعات شخصی در هریک از مراحل چرخهٔ حیات با خطرهایی مواجه می‌شوند که برای پوشش آنها الزاماتی از لحاظ حقوقی یا در مرحلهٔ طراحی اهمیت دارد؛ برخی از این الزامات مثل تأمین امنیت و شفافیت باید در تمامی مراحل مدنظر باشند. الزام بر اخذ رضایت و تحصیل حداقلی اطلاعات در مرحلهٔ جمع‌آوری، محدودیت هدف پردازش، محدودیت افشا و استفاده از اطلاعات و امکان اصلاح اطلاعات در مرحلهٔ پردازش، و به‌همراه شناسایی حق پذیرش و رد در مرحلهٔ استفاده، از دیگر الزاماتی هستند که از لحاظ حقوقی می‌توانند خطرهایی را که در چرخهٔ حیات متوجه حریم خصوصی می‌شوند، پوشش دهند.

بیانیه نبود تعارض منافع

نویسندگان اعلام می‌کنند که تعارض منافع وجود ندارد و تمام مسائل اخلاق در پژوهش را شامل پرهیز از دزدی ادبی، انتشار و یا ارسال بیش از یک بار مقاله، تکرار پژوهش دیگران، داده‌سازی یا جعل داده‌ها، منبع‌سازی و جعل منابع، رضایت ناآگاهانه سوژه یا پژوهش‌شونده، سوءرفتار و غیره ، به‌طور کامل رعایت کرده‌اند.

منابع

الف) فارسی

۱. آقابابایی، حسین؛ موسوی، ریحانه (۱۳۹۲).«حریم خصوصی، اجرای قانون و ادلهٔ اثبات دعوی کیفری در حقوق اسلامی»، *فصلنامهٔ مطالعات حقوق خصوصی دانشگاه تهران*، ش ۴، ص ۳۵-۱۹.

DOI: 10.22059/JLQ.2014.50103

۲. بادینی، حسن (۱۳۹۱). «مسئولیت مدنی ناشی از نقض حقوق معنوی مربوط به شخصیت و حقوق بشر»، *فصلنامهٔ مطالعات حقوق خصوصی دانشگاه تهران*، ش ۱، ص ۱۰۷-۸۹.

DOI: 10.22059/JLQ.2012.29818

۳. رهبر، نوید؛ دهقان‌پور فراشاه، سبحان (۱۴۰۰). «بررسی تطبیقی مبنای مسئولیت مدنی در تصادفات وسایل نقلیهٔ خودران»، *فصلنامهٔ مطالعات حقوق تطبیقی دانشگاه تهران*، ش ۲، ص ۵۴۳-۵۲۳.

DOI: 10.22059/JCL.2021.320449.634169

۴. شهبازی، آرامش (۱۳۹۵). «لزوم رعایت حریم خصوصی – درمانی قربانیان کاربرد سلاح‌های شیمیایی جنگ عراق علیه ایران»، *فصلنامهٔ مطالعات حقوق عمومی دانشگاه تهران*، ش ۲، ص ۴۱۷-۴۴۰.

DOI: 10.22059/JPLSQ.2016.58204

۵. مقامی، امیر؛ عطاران، نادیا (۱۳۹۸). «موازنهٔ افشای حریم خصوصی خانوادگی چهره‌های مشهور در رسانه‌ها و آزادی بیان در رویهٔ نهادهای قضایی»، *فصلنامهٔ مطالعات حقوق عمومی دانشگاه تهران*، ش ۲، ص ۳۱۱-۳۳۱.

DOI: 10.22059/JPLSQ.2018.219954.1390

۶. قاسم‌زاده لیاسی، فلور؛ رئیسی دزکی، لیلا (۱۳۹۹). «کاربست قوانین و مقررات ارتباطی در صیانت از حریم خصوصی شهروندان در فضای سایبر»، *فصلنامهٔ مطالعات حقوق عمومی دانشگاه تهران*، ش ۲، ص ۶۱۶-۵۹۷.

DOI: 10.22059/JPLSQ.2018.261128.1778

ب) خارجی

7. Anderson Cyrus., Ram Vasudevan, Matthew Johnson-Roberson (2020). "Off the Beaten Sidewalk: Pedestrian Prediction in Shared Spaces for Autonomous Vehicles", *IEEE Robotics and Automation Letters*, Vol. 5, Iss. 4, pp.6892-6899. DOI: 10.1109/LRA.2020.3023713
8. Malti Bansal, Marshal Nanda, & Husain Md. Nazir (2021). "Security and Privacy Aspects for Internet of Things (IoT)" *In 2021 6th International Conference on Inventive Computation Technologies (ICICT). IEEE*, pp. 199-204. DOI: 10.1109/ICICT50816.2021.9358665
9. Bloom Cara, Tan Joshua, Javed Ramjohn, Lujo Bauer (2017). "Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles*", USENIX Association Thirteenth Symposium on Usable Privacy and Security*, pp.357- 375. Available at: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bloom (Last visited December 26, 2021)
10. Borgesius Frederik Zuiderveen (2020). "Price Discrimination, Algorithmic Decision-Making, and European Non-Discrimination Law", *European Business Law Review*, Vol. 31, Iss. 3, pp.401-422. Available at SSRN: https://ssrn.com/abstract=3413556 (Last visited December 26, 2021)
11. Chang Wanli, Simon Burton, Chung-Wei Lin, Qi Zhu, Lydia Gauerhof, John McDermid (2020). "Intelligent and Connected Cyber-Physical Systems: A Perspective from Connected Autonomous Vehicles", In: Firouzi Farshad, Chakrabarty Krishnendu, Nassif Sani,

Intelligent Internet of Things, Cham: Springer, pp.357-392. DOI: 10.1007/978-3-030-30367-9_7

12. Coelho Maria Dias, Andre Vasconcelos, Pedro Sousa (2021). "Privacy by Design Enterprise Architecture Patterns", *ICEIS 2021 – 23rd International Conference on Enterprise Information Systems*, pp.743-750. Available at: https://www.scitepress.org/Papers/2021/104735/104735.pdf (Last visited December 26, 2021)
13. Defense Advanced Research Project Agency (2016). "Explainable Artificial Intelligence", *DARPA: Broad Agency Announcement*, pp.1-52. Available at: https://www.darpa.mil/program/explainable-artificial-intelligence (Last visited December 26, 2021)
14. Deng Han, Zhechon Wang, & Yazhen Zhang (2021). "Overview of Privacy Protection Data Release Anonymity Technology", *2021 7th IEEE Intl Conference on Big Data Security on Cloud (Big Data Security), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp.151-156. DOI: 10.1109/BigDataSecurityHPSCIDS52275.2021.00037
15. Endsley Mica R. (2019). "Situation Awareness in Future Autonomous Vehicles: Beware of the Unexpected", In: Bagnara, S., Tartaglia, R., Albolino, S., Alexander, T., Fujita, Y., *Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018) Advances in Intelligent Systems and Computing*, Vol. 824, Cham: Springer, pp.303-309. DOI: 10.1007/978-3-319-96071-5_32.
16. Falco Gregory (2019). "Participatory A.I.: Reducing AI Bias and Developing Socially Responsible A.I. in Smart Cities", *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, New York, NY, USA, pp.154-158. DOI: 10.1109/CSE/EUC.2019.00038
17. Federal Trade Commission (2015). "FTC Report in Internet of Things Urges Companies to Adopt Best Practice to Address Consumer Privacy and Security Risks", *Federal Trade Commission: Protecting America's Consumers* (January 2015) available at https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices (Last visited December 26, 2021)
18. Floridi Luciano (2014). *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality*, 1st Edition, United Kingdom: Oxford University Press.
19. Han Songyang, Fei Miao (2020). "Behavior Planning for Connected Autonomous Vehicles Using Feedback Deep Reinforcement Learning", *Cornell University arXiv Labs*, 1-9. ArXiv: arXiv:2003.04371 (Last visited December 26, 2021)
20. Henkin Louis (1974). "Privacy and Autonomy", *Columbia Law Review*, Vol. 74, Iss. 8, 1410-1433. DOI: 10.2307/1121541
21. Kaspar Debbie V.S. (2005). "The Evolution (or Devolution) of Privacy", *Sociological Forum*, Vol. 20, Iss. 1, pp.69-92. DOI: 10.1007/s11206-005-1898-z
22. Kim, Shiho, Rakesh Shrestha (2020). *Automotive Cyber Security*, Singapore: Springer.
23. Kocić Jelena, Nenad Jovičić, Vujo Drndarević (2018). "Sensors and Sensor Fusion in Autonomous Vehicles", *2018 26th Telecommunications Forum (TELFOR)*, 420-425. DOI: 10.1109/TELFOR.2018.8612054
24. Mayer-Schönberger Viktor (1998). "Generational Development of Data Protection in Europe", in Agre P.E. and Rotenberg M. (eds.), *Technology and Privacy: The New Landscape*, London, MIT Press.
25. Misra Sridipa, Muthucumaru Maheswaran, Salman Hashmi (2017). *Security Challenges and Approaches in Internet of Things*, Cham: Springer International Publishing.
26. NHTSA, "Automated Driving Systems", *National Highway Traffic Safety Administration*, available at https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems#automated-driving-systems-av-20. (Last visited December 26, 2021)
27. Nissenbaum Helen (2010). *Privacy in Context Technology, Policy, and the Integrity of Social Life*, Stanford, California: Stanford University Press.
28. Ntoutsi Eirini, Pavlos Fafalios, Ujwal Gadiraju (2020) "Bias in Data‐Driven Artificial Intelligence Systems—An Introductory Survey", *Wires Data Mining and Knowledge Discovery*, 1-14. DOI: 10.1002/widm.1356
29. Oham Chuka (2018) "A blockchain based liability attribution framework for autonomous vehicles", *arXiv preprint*, arXiv:1802.05050, 1-13. Available at: https://arxiv.org/abs/1802.05050 (Last visited December 26, 2021)

30.Rangesh Akshay, Nachiket Deo, Kevan Yuen, Kirill Pirozhenko (2018). "Exploring the Situational Awareness of Humans inside Autonomous Vehicles", *2018 21st International Conference on Intelligent Transportation Systems (ITSC),* Maui, HI, USA, 190-197. DOI: 10.1109/ITSC.2018.8570001
31.Regan Priscilla M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill: University of North Carolina Press.
32.Seipp David J. (1981). *The Right to Privacy in American History*, Harvard University, Program on Information Resources Policy.
33.Smith Robert Ellis (2000). *Ben Franklin's web site: Privacy and curiosity from Plymouth Rock to the Internet*, Privacy Journal.
34.Solove Daniel J. (2002). "Conceptualizing Privacy", *California Law Review*, Vol. 90, Iss. 4, pp.1087-1156. DOI: 10.2307/3481326
35.Solove Daniel J. (2002). "Digital Dossiers and the Dissipation of Fourth Amendment Privacy", *South California Law Review*, Vol. 75, pp. 1083-1169. Available at: http://ssrn.com/abstract=313301 (Last visited December 26, 2021)
36.Solove Daniel J. (2006). "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol. 154, Iss. 3, 477-564. DOI: 10.2307/40041279
37. Such Jose M. (2017). "Privacy and Autonomous Systems", *IJCAI*, pp.4761-4767. DOI: 10.5555/3171837.3171953
38. Tamò-Larrieux Aurielia (2018). "Technical Tools and Designs for Data Protection. In: Designing for Privacy and its Legal Framework", *Law, Governance and Technology Series*, Springer, Cham, Vol. 40, pp.101-148. DOI: 10.1007/978-3-319-98624-1_6
39. Wang Jianxin, Ming K. Lim, Chao Wang, Ming-Lang Tseng (2021). "The Evolution of the Internet of Things (IoT) over the Past 20 Years", *Computers & Industrial Engineering,* Vol. 155, Iss. 1, 107-174. DOI: 10.1016/j.cie.2021.107174
40. Warren Samuel and Louis Brandeis (1890). "The Right to Privacy", *Harvard Law Review*, Vol. 4, Iss. 5, pp.193–220. DOI: 10.2307/1321160
41. Xiong Jinbo, Renwan Bi, Mingfeng Zhao, Jinga Guo, Qing Yang (2020). "Edge-Assisted Privacy-Preserving Raw Data Sharing Framework for Connected Autonomous Vehicles", *IEEE Wireless Communications*, Vol. 27, Iss. 3, pp.24-30. DOI: 10.1109/MWC.001.1900463
42. Xu Yiran, Xiaoyin Yang, Lihang Gong, Hsuan-Chu Lin, Tz-Ying Wu, Yunsheng Li, Nuno Vasconcelos (2020). "Explainable Object-Induced Action Decision for Autonomous Vehicles", *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 9523-9532. Available at: https://arxiv.org/abs/2003.09405 (Last visited December 26, 2021)
43. Zepf Sebastian, Javier Hernandez, Alexander Schmitt, Wolfgang Minker, Rosalind W. Picard (2020) "Driver Emotion Recognition for Intelligent Vehicles: A Survey", *ACM Computing Surveys*, Vol. 53 Iss. 3, pp.1-30. DOI: 10.1145/3388790

Case Law

44. *Barenblatt v. United States*, 360 U.S. 109, 79 S. Ct. 1081, 3 L. Ed. 2d 1115 (1959).
45. *Boyd v. United States*, 116 U.S. 616, 6 S. Ct. 524, 29 L. Ed. 746 (1886).
46. *Carpenter v. U.S.*, 138 S. Ct. 2206, 585 U.S. 2018, 201 L. Ed. 2d 507 (2018).
47. *Dinerstein v. GOOGLE, LLC*, No. 19 C 4311 (N.D. Ill. Sept. 4, 2020).
48. *Mollett v. Netflix, Inc.*, 795 F.3d 1062 (9th Cir. 2015).
49. *Pavesich Case*, 50 S.E. 68, 122 Ga. 190, 122 Georgia 190 (1905).

Presentations

50. Mangal Nandita, Leslie Nooteboom (2021). "Understanding AI Bias and How It Could Affect A.V.s", *Pave Virtual Panel*. Available at: https://www.youtube.com/watch?v=g1m1XLcd1NQ (Last visited December 26, 2021)

Private Law Studies Quarterly, 2022
51(4): 695-715, DOI:10.22059/JLQ.2021.323088.1007535

Research Paper

Privacy Implication in Autonomous Vehicles: A Comparative Study of Threats and Legal Requirements

Sobhan Dehghanpour Farashah
MA. Graduate in International Trade Law, Shahid Beheshti University, Tehran, Iran.
Navid Rahbar*
Assistant Professor of Faculty of Law, Shahid Beheshti University, Tehran, Tehran, Iran.

Abstract
The idea of a smart city conveys devices highly equipped with novel technologies performing in place of human beings. For a city to be smart, information flow plays an underpinning role. Devices in smart cities collect enormous amounts of information, enabling their embodied systems to run either as computers tackling ordinary tasks or as intelligent agents making decisions and gaining experiences. Artificial intelligence (AI) and other algorithmic systems in both learning and performing stages rely on learning from information entered by a programmer and transmitted from an external source. AI, in particular, benefits from information to predict the future, make decisions, and use feedback on prior ones for decisions on similar occasions. Therefore, the more information at hand, the more efficient AI performs and the smarter the city is. The growing communication technologies such as 5G internet and the internet of things (IoT) let AI systems access transmitted information at higher rates. Autonomous vehicle (AV) is one of the features by which smart cities are known. Along with IoT and the 5G internet, which make information transfer from other devices and infrastructures faster, AVs benefit from numerous embodied sensors collecting various sets of information from the environment for AI to participate in the vehicles' functions. In a city where people use AVs alongside other smart devices, collecting and transmitting information raises privacy concerns. This study deals with the growing concern over the

* Corresponding Author Email: n_rahbar@sbu.ac.ir
Received: 23 May 2021, Accepted:4 December 2021

privacy of the information on which AVs rely to operate. The study's primary purpose is to detect the potential privacy threats by describing the underlying features of AVs in the implementation of which information plays an essential role. Then, considering the potential threats, the research introduces and criticizes the current privacy protections in principle and practice, associable with AV's inherence.

The study dedicates Section I to the concept of privacy to illustrate the evolution of its definition, dimensions, and legal protections as technologies grew over time. Dividing the process into three courses in which privacy relates different meanings, the study suggests that privacy within the current course is falsely comprehended through data and data protection regulations when instead of information itself, the aim of protection must be the subject person whose information is collected. Not considering different dimensions, the current interpretation provides narrow protection for privacy, although it empowers data transactions where data is not sensitive and the subject person consents. Some recent regulations in the EU and the USA, namely General Data Protection Regulation (GDPR) and California Privacy Act (CPA), deal with privacy in this sense by protecting data in the collection, transmission, storage, and usage stages against unconsented processes in the technology sector and technological systems, one of which being AVs. Section II provides details on how information flow and IoT enable inter-connected AVs to operate, then elucidates how the usage of such inter-connection has threatened different dimensions of privacy in actual technology cases similar to AVs. There are cases in which different sets of information on people's location, state of body and mind, behavior and action, social life, and media are collected and transmitted in vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-everything networks unconsented or illegally processed. Outlining the four stages of the life cycle of information (collection and storage, processing, usage, and transmission), Section III demonstrates whether AVs impose the risk of breach of privacy by four types of behavior (collection, processing, dissemination, and invasion) and how the current regulations protect privacy in the said types of behavior. Primarily, privacy protection in AVs entails considering legal principles in the design stage as well as the stages of the life cycle of information to guarantee the security and transparency of information flow. Confidentiality and encryption to improve security and inform the data subject of the purpose of processing and implementing data to increase transparency are the legal principles envisaged by current regulations, GDPR and CPA.

Equipped with sensors facing the external and internal environments, AVs collect and store information about the bodily and mentally status of people in and around the vehicle, information about the vehicle itself, namely estimating energy consumption, locating the vehicle and other objects around it, and other information necessary for AI to operate the vehicle. Regulations protecting privacy should require prior consent for the collection and that the technologies associated with the collection phase minimize the

amount of data collected. The processing phase provides AI categorized, tagged, and patterned sets of information to enable the usage phase. A standard regulation contains provisions on the limitation of the purpose of the processing of data, as well as the ability to modify data for the data subject; therefore, the regulation preserves privacy from threats such as data aggregation, identification, insecurity, secondary use, and exclusion. The collected and processed data enables AVs to anticipate incidents, make decisions, and improve upon them in the usage phase of the life cycle of information. To prevent AI from being biased, intrusive, and decisionally interfering, the regulation must grant the right to reject data usage to the data subject in addition to the purpose limitation requirements. In the last stage of the cycle, AV systems transmit data in networks or delete unnecessary data. The standard regulation grants data subject the right to control over the deletion of their collected data as well as requiring its consent for data dissemination to both maintain transparency and protect privacy against unconsented disclosures and breach of confidentiality.

Keywords: Artificial Intelligence, Automated Technology, The Life Cycle of Information, Personal Data, Personal Information.

Declaration of conflicting interests
The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs: https:/orcid.org/ 0000-0002-6993-0885