(مقاله مروری)

نانوفنّاوری و حریم خصوصی: نگاه اخلاقی و حقوقی

دکتر محمّد راسخ[1*]، فاطمه دومانلو[2]

1. **گروه حقوق عمومی، دانشکده حقوق، دانشگاه شهید بهشتی**

2. **گروه حقوق و اخلاق زیستی، مرکز تحقیقات بیوتکنولوژی تولیدمثل، پژوهشکده فنّاوری‌های نوین علوم پزشکی جهاددانشگاهی ـ ابن‌سینا، تهران**

(تاریخ دریافت: 93/12/5 تاریخ پذیرش:94/3/30)

چکیده

زمینه: یکی از مهم‌ترین چالش های اخلاقی و حقوقی که در مورد پیشرفت و به‌کارگیری نانوفناوری مطرح شده، مسئلهٔ حریم خصوصی است. هستهٔ اصلی این چالش «فناوری تشخیص هویت از طریق امواج رادیویی» (آرفید) است. تراشه‌های آرفید با استفاده از فناوری نانو، بسیار کارآمدتر، کوچک‌تر و ارزان‌تر از گذشته تولید می‌شوند. این برچسب‌ها امروزه برای ردیابی، صورت‌برداری و جلوگیری از سرقت کالاها در فروشگاه‌های بزرگ مورد استفاده قرار می‌گیرند. اطلاعاتِ ذخیره‌شده روی تراشهٔ آرفید، حتی پس از فروش و خروج کالای حاملِ آن از فروشگاه، به‌آسانی با یک دستگاه خوانندهٔ الکترونیکی قابل دسترسی و بنابراین فردی که آن کالا را به همراه دارد، بی آنکه بداند، قابل ردیابی است. فراگیریِ برچسب‌های آرفید و استفاده از آنها به شکل کنونی، یعنی بدون هر گونه تدبیر امنیتی، حریم خصوصیِ افراد را به‌شدت تهدید می‌کند. پژوهش حاضر ضمنِ مطالعهٔ چگونگیِ نقض حریم خصوصیِ افراد در اثر استفادهٔ نادرست از نانوفناوری و نیز پرداختن به اهمیتِ حریم خصوصی در زندگیِ اخلاقیِ افراد و توجه به جایگاهِ آن در نظام‌های حقوقیِ بین‌المللی و کشورهای مختلف، از جمله ایران، می‌کوشد جامعه را از این خطراتِ بالقوه و راه‌های مقابله با آن آگاه سازد.

نتیجه‌گیری: از آنجا که نقض حریم خصوصی ارزش‌هایی مثل «کرامت انسانی»، «خودآیینی» و «صمیمیت» و بدین‌ترتیب بنیانِ زندگیِ اخلاقیِ افراد را به خطر می‌اندازد، لازم است ضمن رعایت اصول اخلاقی، راهکارهایی حقوقی اندیشیده شوند تا ضمن بهره‌مندی از مزایای فناوری آرفید امکان سوءاستفاده از آن برای تهدید امنیّت و نقض حقوق شهروندان مرتفع شود.

کلیدواژگان: *اخلاق، آرفید، حریم خصوصی، نانوفنّاوری*

سرآغاز

گذشت نیم‌قرن برای فراگیر شدن یک فنّاوری زمانی اندک به نظر می‌رسد، با این حال، نانوفنّاوری از سال 1959، که ایدهٔ اولیهٔ آن، یعنی «ساختن اتم به اتم مواد»، مطرح شد، تاکنون پیشرفت‌هایی چشمگیر در حوزه‌های گوناگون داشته است. در واقع، شاید بتوان نانوفنّاوری را نه یک فنّاوری نوین که رویکردی جدید در همهٔ رشته‌های علمی و مهندسی دانست. شاهد این مدعا کارکرد این شاخه از فنّاوری در حوزه‌های مختلف و متفاوت ـ از جمله در علوم زیستی، پزشکی و دارویی، کشاورزی، صنایع غذایی، الکترونیک و فنّاوری اطلاعات، صنایع نظامی و امنیتی، مهندسی عمران، معماری و نساجی ـ است. البته گسترش نانوفنّاوری در همهٔ حوزه‌های یادشده یکسان نبوده است. این کاربرد گسترده بر ابعاد گوناگون زندگی روزمرهٔ انسان

* نویسنده مسؤول: نشانی الکترونیکی: m_rasekh @ sbu.ac.ir

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

نیز تأثیر داشته است؛ از غذایی که افراد می خورند و لباسی که می‌پوشند تا خانه‌ای که در آن زندگی می‌کنند همه در اثر استفاده از نانوفنّاوری کیفیتی متفاوت یافته‌اند. در سطح اجتماعی نیز نانوفنّاوری نوع زندگی انسان‌ها، توانایی‌هایشان، روابط آنان با یکدیگر و محیط پیرامون‌شان را تغییر داده است(1).

این فنّاوری هر چه بیشتر با زندگی انسان‌ها تنیده می‌شود، مسائل و ملاحظات اخلاقیِ بیشتر و پیچیده‌تری را نیز پیرامون خود شکل می‌دهد که به نوبهٔ خود نیاز به قانونگذاری و رسیدگی قضائی را نیز به میان می‌آورد. نانوفنّاوری، همانند هر فنّاوری دیگری، به خودی خود، نه خوب است و نه بد و مسائل اخلاقی همگی از چگونگی به‌کاربردنِ آن برمی‌خیزند. فنّاوری‌های جدید اغلب با اهداف مثبت شکل گرفته‌اند، اما بعدها وجوه منفیِ آنها نیز آشکار شده‌اند. بنابراین، برای بیان ملاحظات اخلاقی یک فنّاوری جدید بهتر است بر کاربردهای بالقوه زیان‌بار و پیامدهای منفی آن تمرکز نمود، به این امید که تمهیداتی برای رفع و پیشگیری از آنها اندیشیده شود(1). اما، در مواجهه با فنّاوری‌های جدید همواره یک تنگنا وجود دارد. از یک سو، در مراحل آغازین پیشرفت آنها اطلاعات اندکی دربارهٔ پیامدهای احتمالی‌شان در دسترس است. از دیگر سو، وقتی آن فنّاوری‌ها گسترش می‌یابند، پیامدهای‌شان آشکار می‌شوند، حال آنکه مجال اندکی برای تغییر مسیر پیشرفت آنها باقی می‌ماند(2). به هر روی، هیچ گاه، نه پیش و نه پس از پیشرفت یک فنّاوری، نباید نسبت به مسائل اخلاقی برخاسته از آن بی‌تفاوت بود.

در این خصوص و برای نمونه، می‌توان به اصل احتیاط، به مانند یک اصل اخلاقی عام، اشاره کرد. این اصل هنگام تصمیم گیری دربارهٔ خطرات احتمالی تحقیق و توسعهٔ علمی و فنی به کار می‌آید. اصل احتیاط به نوبهٔ خود به اصول اخلاقی دیگر متکی است که مهم‌ترین آنها اصل ضررنرسانی است. بنابر اصل احتیاط، عقل سلیم بر فنّاوری‌های جدید اِعمال می‌شود، بدین معنا که ضرر آنها نباید بیش از سودشان باشد(3). به دیگر سخن، در پیشرفت علم و فنّاوری باید میان ممکن، دست‌یافتنی و مطلوب تمایز نهاد. اما باید تعیین کرد که «چه چیز مطلوب است؟» و در تعیین مطلوبیت امور، بسته به نظرگاه، سنجه‌هایی چون ایمنی، منافع عمومی، دیدگاه‌های اخلاقی، حقوق شهروندان، کرامت انسانی و دین برای داوری به کار گرفته می‌شوند(1).

بر این اساس، رشد پرشتاب نانوفنّاوری نیز نباید سبب مغفول ماندن مسائل اخلاقی و حقوقی مربوط به آن شود(4و5). یکی از مهم‌ترین چالش های اخلاقی و نیز حقوقی که در خصوص پیشرفت و به‌کارگیری نانوفنّاوری مطرح شده، مسئلهٔ حریم خصوصی است(6). هستهٔ اصلی این دغدغه فنّاوری «آرفید» (فنّاوری تشخیص هویت از طریق امواج رادیویی) است(7). «آرفید» در اصل نیازمند فنّاوری نانو نیست، اما نانوفنّاوری آن را بازتعریف کرده و زمینهٔ نقض حریم خصوصی را بدان وسیله فراهم آورده است(7). این نوشتار در پی بررسی اخلاقی و حقوقی تأثیر توسعهٔ نانوفنّاوری بر حریم خصوصی است. به این منظور، ابتدا به تشریح فنّاوری «آرفید» و چگونگی امکان نقض حریم خصوصی افراد، بدین وسیله، می‌پردازد و سپس بحث حریم خصوصی و دلالت‌های اخلاقی آن را بررسی می‌کند. پس از آن به مطالعهٔ نمونه‌های قانون‌گذاری در سطح ملی و راه‌کارهای ارائه شدهٔ منطقه‌ای در ارتباط با این موضوع می‌پردازد.

«آرفید» چیست؟

فنّاوری «آرفید[1]»، همانند دیگر فنّاوری‌ها، در واقع در پاسخ به یک نیاز به وجود آمد: شناسایی اشیا از راه دور. در جنگ جهانی دوم، انگلیسی‌ها برای تشخیص هواپیماهای متفقین از هواپیماهای دشمن از فرستنده‌های رادیویی استفاده کردند. در دههٔ 1960 نخستین تراشه‌ها[2] در آزمایشگاه‌های تحقیقاتی ساخته شدند و در دههٔ بعد دولت آمریکا از آنها استفاده کرد. در دههٔ 1980، با استفاده از تراشه‌ها، برچسب‌های آرفید[3] برای ردیابی اموالی که مدیریت آنها دشوار بود، مانند حیوانات مزرعه و واگن‌های راه‌آهن، به کار گرفته شدند. در چند سال گذشته، بازار آرفید به سبب پیشرفت‌هایی که در پایگاه‌های دادهٔ کامپیوتری صورت گرفته و نیز کاهش قیمت تراشه‌ها بسیار رونق پیدا کرده است. اکنون نیز شرکت‌های بسیاری مانند موتورولا، فیلیپس و تگزاس اینسترومنتس به تولید تراشه‌ها مشغولند(8).

یک برچسب آرفید دست‌کم دو جزء دارد: یک مدار مجتمع[4] برای ذخیره و پردازش اطلاعات و تنظیم فرکانس رادیویی و

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

مانند آنها و یک آنتن برای گرفتن و فرستادن پیام(6). هر برچسب یک شمارهٔ شناسایی منحصر به فرد دارد که از طریق آنتن برای داده‌خوان ارسال می‌شود. داده‌خوان نیز امواج رادیویی آنالوگ را برای استفادهٔ کامپیوتر به داده‌های دیجیتال تبدیل می‌کند. برچسب‌های «آرفید» دو نوعند: فعال و منفعل. برچسب‌های منفعل هیچ منبع انرژی درونی‌ای ندارند و انرژی مورد نیاز خود را از سیگنالی رادیویی که از داده‌خوان دریافت می‌دارند تأمین می‌کنند. برچسب‌های فعال با باتری کار می‌کنند و، از این رو، از برچسب‌های منفعل بزرگ‌تر و البته گران‌ترند. برچسب‌های فعال بر خلاف نوع دیگر که عمر نامحدود دارند، به سبب محدودیت عمر باتری، حدود 10 سال کار می‌کنند. دامنهٔ پوشش برچسب‌های منفعل به‌طور معمول از چند سانتی‌متر تا چند متر است، ولی دامنهٔ پوشش برچسب‌های فعال به حدود 1500 متر هم می‌رسد. برچسب‌های منفعل فقط قابلیت خواندن (یعنی برداشت اطلاعات ذخیره شده در حافظه) دارند، درحالی‌که برچسب‌های فعال هم قابلیت خواندن و هم قابلیت نوشتن (یعنی ذخیرهٔ اطلاعات جدید در حافظه) دارند.

برچسب‌های آرفید از لحاظ طیف فرکانسی که استفاده می‌کنند نیز متفاوتند. برچسب‌های فرکانس بالا نسبت به برچسب‌های فرکانس پایین دامنه و سرعت بیشتری دارند(9 و 7).

کاربردهای «آرفید»

ابتدایی‌ترین و بیشترین کاربرد فنّاوری «آرفید» در صورت‌برداریِ اموال است. بارکُدها، اگر چه مدت‌هاست به بازار راه یافته‌اند و هزینهٔ تولید آنها بسیار پایین است، رفته‌رفته جای خود را به برچسب‌های آرفید می‌دهند. بزرگترین محدودیت بارکُد این است که برای خواندن آن باید کالا به طور مستقیم مقابل بارکدخوان قرار بگیرد، در نتیجه، به طور مثال برای صورت‌برداری از دفترهای موجود در یک فروشگاه، لازم است آنها یک به یک در مقابل بارکدخوان قرار بگیرند. همچنین، با فروش دفترها یا به سرقت رفتن آنها دیگر نمی‌توان شمار و تعداد آنها را مشخص کرد. ولی با استفاده از برچسب‌های آرفید اطلاعات کالاها به آسانی و دقیق ثبت شده و به‌روز خواهد بود. کافی است یک داده‌خوان در فاصلهٔ مناسبی از کالاها قرار داده شود تا به محض جابه‌جایی یک کالا اطلاعات مربوط در کامپیوتر به‌روز و ذخیره شود. افزون بر این، بارکُدها فقط نوع کالا را مشخص می‌کنند و هیچ اطلاعات دیگری دربارهٔ کالا به دست نمی‌دهند، درحالی‌که یک برچسب آرفید می‌تواند اطلاعاتی مانند اندازه، وزن، تاریخ انقضا، محل تولید و جزئیات حمل کالا را در بر داشته باشد(7).

کاربرد آرفید اما به مورد یادشده محدود نمی‌شود. دیگر کاربردهای این فنّاوری عبارتند از: پرداخت خودکار عوارض، کارت شناسایی، دستگاه‌های دزدگیر، مدیریت بایگانی، نظام‌های پرداخت، مبارزه با کالاهای تقلبی، شناسایی خودرو، امنیت ساختمان، شناسایی کالاهای مرجوعی، نظام‌های کتابخانه‌ای، شناسایی حیوانات خانگی و دام‌ها و مانند آنها(7 و 9).

گفتنی است کاربرد آرفید به کالاها و حیوانات محدود نمی‌شود. از سال 2001 میلادی به این سو، با تولید ریزتراشهٔ[5] یا ریزتراشهٔ آرفید، امکان کاشت ریزتراشه در درون بدن انسان نیز فراهم شده است. ریزتراشه‌ها در شیشه‌هایی به اندازهٔ تقریبی یک دانهٔ برنج جاسازی و درون بافت چربی زیر ماهیچهٔ سه‌سر تزریق می‌شوند. این تراشه حاوی یک شمارهٔ شناسایی است که داده‌خوان می‌تواند آن را بخواند. برخی از شرکت‌ها از این روش برای نظارت بر ورود و خروج کارکنان خود و نیز دسترسی آنها به محدوده‌های امنیتی استفاده می‌کنند. همچنین، پیشنهاد شده است ریزتراشه‌ها برای ثبت سابقهٔ پزشکی افراد به‌کار گرفته شوند. بدین سان، هنگامی که فرد بیهوش است یا در شرایطی نیست که بتواند اطلاعات لازم را در اختیار گروه پزشکی بگذارد، سابقهٔ پزشکی او در دسترس خواهد بود(7).

با رواج استفاده از فنّاوری آرفید تلاش برای تولید برچسب‌های کوچک‌تر و ارزان‌تر نیز آغاز شده است که گسترده شدن کاربرد آن را در پی خواهد داشت.

«آرفید» و امکان نقض حریم خصوصی

از آنجا که تراشه‌های آرفید از فرکانس رادیویی استفاده می‌کنند، اطلاعات آنها می‌تواند به‌آسانی در دسترس هر کسی قرار بگیرد. مشکلات زیر در ارتباط با برچسب‌های آرفید و داده‌خوان‌ها گزارش شده‌اند:

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

اطلاعات یک برچسب آرفید بعد از خروج کالای حاوی آن از فروشگاه همچنان می‌تواند خوانده شود. برچسب «آرفید» تفاوت داده‌خوان‌ها را تشخیص نمی‌دهد و هر داده‌خوانی می‌تواند به اطلاعات آن دست یابد.

کندن برچسب‌های آرفید دشوار است. برخی از برچسب‌های آرفید بسیار کوچکند و برخی چنان داخل کالا جاسازی شده‌اند که خریدار نمی‌تواند آنها را ببیند یا جدا کند. البته، یکی از مزایای اصلی برچسب‌های آرفید، یعنی جلوگیری از سرقت، به همین ویژگی جدانشدنی بودن برچسب‌ها باز می‌گردد.

برچسب‌های آرفید بدون اطلاع شخص قابل ردیابی‌اند. هر کس، به وسیلهٔ یک داده‌خوان، می‌تواند برچسب‌های جاسازی شده در لباس یا دیگر لوازم همراه فرد را، بی‌آنکه او بداند، بخواند. برای مثال، هنگام ورود به یک فروشگاه داده‌خوان‌ها فرد را برای ردیابی تراشه‌های آرفید همراه او اسکن می‌کنند. به این ترتیب، کارمند فروشگاه با اطلاع از محتویات کیف مشتری می‌تواند پیشنهادهایی مناسب برای خرید به او ارائه کند.

برچسب‌های آرفید را می‌توان با استفاده از آنتن‌های بسیار قوی از فاصله‌های دورتر ردیابی کرد و به اطلاعات آنها دست یافت.

برچسب‌های آرفید با یک شماره سریال منحصر به فرد می‌توانند به شمارهٔ کارت اعتباری مشتری متصل شوند. در حال حاضر، کُد جهانی محصولات[6] به هر محصولی که در یک فروشگاه فروخته می‌شود شماره‌ای منحصر به فرد اختصاص می‌دهد که آن محصول را شناسایی می‌کند. هنگام خرید یک کالا اگر بهای آن به‌وسیلهٔ کارت اعتباری پرداخت شود، شمارهٔ برچسب آرفید می‌تواند به شمارهٔ کارت اعتباری، و در نتیجه به هویت خریدار، متصل شود(8).

در واقع، مهم‌ترین مسئله این است که برچسب‌های آرفید روی کالا، حتی پس از خرید و خروج آنها از فروشگاه، فعال باقی می‌مانند و می‌توانند برای نظارت یا اهدافی دیگر، غیر از آنچه برای آن ساخته شده‌اند (مانند صورت‌برداری و نظارت بر اموال)، به کار گرفته شوند(8).

چنانکه از شواهد برمی‌آید، فنّاوری آرفید هرچه پیشتر می‌رود و هرچه بیشتر استفاده می‌شود، خطراتش برای حریم خصوصی افراد ابعادی جدی‌تر پیدا می‌کند.

اهمیت ارزشی حریم خصوصی

به تعبیر یکی از نویسندگان، البته در زمینه‌ای متفاوت، به نظر می‌رسد حریم خصوصی[7] مفهومی بسیار مبهم نزد همگان است(10). مراجعه به ادبیات موجود در این زمینه درستی این تعبیر را آشکار می‌کند، زیرا تعاریفی بسیار متفاوت از حریم خصوصی وجود دارند که هیچ یک از تیغ نقدِ اندیشمندان در امان نمانده است. با این حال، به نظر می‌رسد مهم‌ترین تعریف‌های حریم خصوصی پیرامون دو محور کلی شکل گرفته‌اند: 1- تسلط و نظارت بر اطلاعات شخصی، و 2- محدودیت دسترسی.

یکی از قدیمی‌ترین تلاش‌ها برای تعریف حریم خصوصی بر اساس تسلط و نظارت بر اطلاعات شخصی به نوشته‌ای معروف، در قرن نوزدهم میلادی زیر عنوان «حق بر حریم خصوصی» باز می‌گردد(11). در واقع، بحث مکتوب و نظام‌مند معاصر دربارهٔ مفهوم حریم خصوصی در اساس با نوشتهٔ یادشده آغاز شد. نویسندگان حریم خصوصی را به شرح زیر تعریف می‌کنند: توانایی فرد به تعیین زمان، چگونگی و میزان انتقال اطلاعات او به دیگران(12). پاره‌ای نویسندگان نیز حریم خصوصی را وضعیتی می‌دانند که در آن هیچ یک از اطلاعات شخصی غیرمستند فرد در اختیار دیگران نباشد(13). همچنین، گفته شده است که گرایش به حریم خصوصی از نگرانی از در دسترسِ دیگران بودن بر می‌خیزد؛ این نگرانی که دیگران چقدر دربارهٔ فرد می‌دانند، به چه میزان دسترسی فیزیکی به وی دارند و افراد چقدر مورد توجه دیگران هستند(14). به تعبیر برخی از نویسندگان، حریم خصوصی از فرد در برابر دسترسی دیگران محافظت می‌کند، البته در صورتی که به میل خود نخواهد در دسترس باشد(12).

تعریف حریم خصوصی در میان صاحب‌نظران بسیار مناقشه برانگیخته است، اما همگی دربارهٔ اهمیت آن توافق دارند. حریم خصوصی چه دارای ارزشی ذاتی و غایتی در خود در نظر گرفته شود، چه وسیله و ابزاری برای تضمین ارزش‌های دیگر مانند عشق و خلاقیت، اغلب نظریه‌پردازان آن را امری ارزشمند می‌دانند(15). به گونه‌ای که این اهمیت ارزشی راه خود را به اسناد سیاسی و حقوقی باز کرده است. برای نمونه، در مادهٔ 12

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

اعلامیهٔ جهانی حقوق بشر آمده است: «احدی در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود نباید مورد مداخله‌های خودسرانه واقع شود و شرافت و اسم و رسمش نباید مورد حمله قرار گیرد. هر کس حق دارد که در مقابل این‌گونه حملات مورد حمایت قانون قرار گیرد.»(16)

در توجیه اهمیت ارزشی حریم خصوصی می‌توان به سه ارزش «کرامت انسانی[8]»، «خودآیینی[9]» و «صمیمیت[10]» استناد کرد که نقض حریم خصوصی آنها را تهدید می‌کند. البته برشمردنِ صمیمیت در کنار کرامت انسانی و خودآیینی، برای تبیین اهمیت حریم خصوصی، به معنای هم‌ارز دانستن این مفاهیم نیست. این مفاهیم، گرچه با قوّتی نابرابر، به دفاع از حریم خصوصی برخاسته‌اند و تنها از این رو کنار هم نشسته‌اند.

هر انسانی از آن جهت که انسان است و نه به هیچ دلیل دیگر، شایستهٔ احترام است. ضرورت احترام به کرامت انسانی بر هیچ بنیانی استوار نگشته است، بلکه خود بنیان همهٔ ادعاها و استحقاق‌های منتسب به انسان است(17). حریم خصوصی نیز بر همین اساس توجیه‌شدنی است که نبود آن به تضعیف ارزش غایی انسان می‌انجامد. به دیگر سخن، حریم خصوصی ضامن شخصیت غیر قابل تجاوز انسان انگاشته شده است(11). فردی که مجبور است هر لحظه از زندگی‌اش را در میان دیگران بگذراند و همهٔ نیازها، اندیشه‌ها، آرزوها و خیال‌هایش در معرض نگاهِ دیگران باشد، از فردیت و کرامت انسانی‌اش محروم شده و با توده درآمیخته است. عقاید و دیدگاه‌هایش هیچ‌گاه متفاوت نخواهند بود، چون زیر نفوذ دیگرانند، آرمان‌هایش همیشه مطابق عرف خواهند بود، چون همه از آنها آگاهند و احساساتش یکتایی و اصالتشان را از دست می‌دهند، چون در برابر همگان به نمایش در می‌آیند. چنین موجودی دیگر فرد نیست، چون یگانه نیست، چون جایگزین‌پذیر است. بی‌تردید، تجاوز به خلوت انسان‌ها نادیده گرفتن کرامت آنان است(18).

در بسیاری از نظام‌های اخلاقی، احترام به خودآیینیِ افراد، از جمله مهم‌ترین اصول ارزشی برشمرده شده است. خودآیینی هنگامی به فرد نسبت داده می‌شود که وی دست به انتخاب‌های اصیل بزند و سرنوشت زندگی‌اش را خود تعیین کند. فرد خودآیین آرمان‌ها و برنامه‌هایش را طبق تصوری که از خیر دارد انتخاب و آنها را پی می‌گیرد. بنابراین، انتخاب پیش‌شرطِ زندگیِ اصیل، شکوفا و موفقی است که مطابق دیدگاه اخلاقیِ فرد زیسته می‌شود. بر خلاف آزادی که ارزشی سلبی و، در تعریفی دقیق، عبارت از نبود موانع است، خودآیینی ارزشی ایجابی و مستلزمِ شکل دادن و پی‌گیریِ فعالِ مفهومی از خیر است(19 و 20). پس آرمانِ خودآیینی بر ظرفیت انسان برای انتخاب خودجوش، مختارانه و مسئول متمرکز است(20). هدف این است که جامعه دیدگاه‌های عمومی و داوری‌های اخلاقی خود را به افراد تحمیل نکند و فرد زندگی‌ای مبتنی بر خیر، از دیدگاه خود، بنا کند(2). می‌توان گفت حریم خصوصی مشروعیت خود را از خودآیینی کسب می‌کند و حتی به ادعای برخی از نویسندگان به همین واسطه بهتر فهمیده می‌شود(2).

افزون بر این، انسان‌ها روابط بین فردیِ مختلفی را تجربه می‌کنند، از روابط رسمی و سطحی گرفته تا روابط صمیمانه، دوستانه و عاشقانه. آنچه نوع رابطه را تعیین می‌کند، میزان دسترسیِ طرفین رابطه به یکدیگر و نیز میزان اطلاعاتی است که دربارهٔ یکدیگر در اختیار دارند(7 و 21). حریم خصوصی امکانِ تسلط و نظارت بر شخص و بدین‌ترتیب تنظیم و مدیریت روابط بین‌الانسانی را برای فرد فراهم می‌آورد. صمیمیت در میان گذاشتن اندیشه‌ها، احساسات و تجربه‌هایمان با تعداد اندکی افراد خاص است، اندیشه‌ها، احساس‌ها و تجربه‌هایی که حق داریم از دیگران پوشیده نگه داریم. حریم خصوصی بدین وسیله سرمایهٔ اخلاقی لازم را برای صمیمیت فراهم می‌آورد(22). از دیگر سو، اعتماد که عنصر ضروریِ روابط صمیمانه است، بدون حریم خصوصی معنای خود را از دست می‌دهد. اعتماد یعنی انتظار داشتن از دیگری برای این‌که مطابق حدود اخلاق رفتار کند و این امر بدون وجود خلوت و حریم خصوصی شدنی نیست(22). صمیمیت و اعتماد به نوبهٔ خود زمینهٔ یک زندگی معنادار را برای انسان‌ها فراهم می‌آورند و ضرورت ارزشی حریم خصوصی را بیشتر آشکار می‌کنند(7).

بر این اساس، حریم خصوصی حس فردیت آمیخته با شخص‌بودن[11] را در فرد تقویت می‌کند و مجال ابرازِ وجود، آرامش و تفکر را برای او فراهم می‌آورد. حریم خصوصی رشد و

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

شکوفایی فردی و تمرین داوری اخلاقی را ممکن می‌سازد و تعیین سرنوشت افراد را به دست خودشان می‌سپارد(23).

ابعاد حقوقی «آرفید»

با گسترش استفاده از آرفید، به مثابه پدیده‌ای نوظهور در حوزه‌های مختلف و شناخت چالش‌هایی که می‌تواند برای حریم خصوصی افراد به همراه داشته باشد، این پرسش به میان می‌آید که چه راه‌کارهای حقوقی در دنیا اتخاذ شده که هم‌زمان امکان بهره‌گیری از این فنّاوری را فراهم و حفظ حریم خصوصی افراد را تضمین می‌کنند. برای پاسخ به این پرسش، بررسی قانون‌گذاری در برخی کشورها بصیرت‌زا به نظر می‌رسد.

ایالات متحدهٔ امریکا

در ایالات متحدهٔ امریکا، قانونی جامع در مورد بهره‌گیری از آرفید در سطح فدرال وجود ندارد و در این خصوص به قوانین مسئولیت مدنی12 استناد می‌شود که البته کافی و وافی به مقصود نیستند. از این رو، هر یک از ایالات قوانینی در خصوص نحوهٔ استفاده از آرفید و ارتباط آن با حریم خصوصی وضع کرده‌اند. برای نمونه، در واشنگتن، به موجب قانونی که از ماه ژوئیهٔ سال 2008 لازم الاجرا شده، «خواندن» اطلاعات شخصی افراد به دلایل غیرقانونی از روی اقلامی چون پوشاک و کالاهایی که در آن برچسب آرفید به کار رفته جرم‌انگاری شده است؛ همچنین است اطلاعات شخصی مندرج در مدارکی چون گواهینامهٔ رانندگی و کارت اعتباری. منظور از «خواندن» در اینجا هرگونه استفادهٔ مخفیانه از آرفید برای جمع‌آوری اطلاعات است(24). ایالت کالیفرنیا نیز، به تبع واشنگتن، خواندن اطلاعات هویتی اشخاص از راه دور و بدون آگاهی و رضایت قبلی آنها را، با استفاده از فنّاوری «آرفید»، ممنوع اعلام کرد(25). در بسیاری از ایالات نیز استفاده از برچسب «آرفید» در گواهینامه‌های رانندگی و کارت‌های شناسایی مشمول قواعد و مقررات خاصی شده‌اند. همچنین، به موجب قوانین و مقررات وضع‌شده در ایالت میشیگان، مرجع صادرکنندهٔ کارت‌های شناسایی و گواهینامهٔ رانندگی باید از امنیت «آرفید»های استفاده شده اطمینان حاصل نماید و عدم دسترسی افراد و مقامات غیرصالح به اطلاعات بازیابی شده از آن را تضمین کند. همچنین متقاضی صدور کارت یا گواهینامه باید اعلام نماید که از به کار رفتن فنّاوری آرفید در کارت خود اطلاع دارد(26). در سایر ایالات نیز قوانینی مشابه وضع شده‌اند.

استرالیا

به موجب قوانین و مقررات حاکم بر حریم خصوصی در استرالیا، فروشگاه‌هایی که کالاهای آنها مجهز به آرفید هستند، باید موارد زیر را رعایت نموده و اطمینان یابند که حریم خصوصی مصرف‌کنندگان نقض نمی‌شود:

اطلاع‌رسانی به مشتری در مورد وجود برچسب آرفید در کالا.

ثبت جزئیات مربوط به چگونگی استفاده و حفظ اطلاعاتی که در کالای خریداری‌شده به وسیلهٔ فنّاوری آرفید جمع‌آوری می‌شود.

آموزش به مصرف‌کنندگان در خصوص این فنّاوری و قابلیت‌های آن.

امکان تصمیم‌گیری مشتری، در حین خرید یا پس از آن، در مورد حذف، برداشتن یا از کار انداختن تراشهٔ آرفید به کار رفته در کالا(27).

انگلستان

در انگلستان، مهم‌ترین قانونی که در خصوص استفاده از آرفید وضع شده، «قانون حفاظت از اطلاعات» (1998) است(28). فنّاوری آرفید در دو صورت می‌تواند اطلاعات شخصی را پردازش کند. نخست، وقتی برچسب آرفید حاوی اطلاعات شخصی فرد باشد یا اینکه برچسب به پایگاهی اطلاعاتی متصل باشد که اطلاعات شخصی فرد در آن ثبت شده است. دوم زمانی است که برچسب‌های به کاررفته در دارایی‌های شخصی افراد می‌توانند برای شناسایی هویت یا اطلاعات شخصی دارندهٔ آن مورد استفاده قرار گیرند. بر این اساس، «قانون حفاظت از اطلاعات» بر هر یک از این صورت‌ها قابل اِعمال است. همهٔ افراد یا نهادهایی که به شکلی از این فنّاوری استفاده می‌کنند (مانند فروشندگان کالاهای دارای آرفید یا صادرکنندگان انواع کارت‌های دارای برچسب آرفید) مؤظف به رعایت اصول حفاظت

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

از اطلاعات مندرج در این قانون، پیش از به کارگیری آن فنّاوری، هستند. این اصول عبارتند از:

1. پردازش منصفانهٔ اطلاعات[13]: همهٔ نهادها و کسانی که به کمک فنّاوری آرفید اقدام به جمع‌آوری اطلاعات شخصی می‌کنند، موظفند افراد را از وجود برچسب آرفید در کالاها و همهٔ پیامدهای آن مطلع سازند. همچنین، لازم است به طور مشخص توضیح دهند چه اطلاعاتی از سوی چه کسی و به چه منظوری جمع‌آوری می‌شوند. آموزش چگونگی از کار انداختن یا برداشتن برچسب آرفید به مشتریان از دیگر تکالیف مندرج در آن قانون است.

2. رعایت حدود قانونی در استفاده از آرفید: گردآوری اطلاعات شخصی افراد باید جهتی مشخص و قانونی داشته باشد. بنابراین، همهٔ شرکت‌ها و بنگاه‌ها باید از این فنّاوری به شکل مقید و مشروط استفاده کنند.

3. کیفیت اطلاعات: استفاده‌کنندگان از اطلاعات به دست آمده به وسیلهٔ آرفید باید اطمینان حاصل کنند که این اطلاعات دقیق و مطابق آخرین تغییرات است.

4. حفظ اطلاعات[14]: اطلاعات شخصی افراد را نباید بیش از زمان لازم و جز برای هدف مشخص نگهداری کرد.

5. امنیت: استفاده‌کنندگان از آرفید باید از امنیت اطلاعات ذخیره شده یا به دست آمده از آن اطلاعات اطمینان یابند.

اسناد منطقه‌ای

افزون بر قوانین داخلیِ هر کشور در خصوص استفاده از فنّاوری آرفید، در سطح منطقه‌ای نیز می‌توان اسنادی را یافت. برای نمونه، در اروپا، می‌توان به دو سند، یکی عام و دیگری خاص، اشاره کرد. «دستورالعمل حفاظت از اطلاعات اتحادیهٔ اروپا» سندی کلی در حوزهٔ پردازش اطلاعات شخصی است که در سال 1995 به‌طور مشترک از سوی پارلمان و شورای اروپا صادر شد(29). این سند به‌طور مشخص به آرفید نمی‌پردازد، اما قواعد پردازش اطلاعات، که در این دستورالعمل آمده، بر پردازش اطلاعات به دست آمده از آرفید قابل اِعمال است(30). به موجب این دستورالعمل، هرگونه پردازش اطلاعات بیش از حدِ متعارف و نیاز، با اهداف غیرقانونی، ممنوع است و اطلاعات جمع‌آوری شدهٔ قانونی نیز نباید بیش از زمان مورد نیاز نگهداری شود.

دستورالعمل «حریم خصوصی در ارتباطات الکترونیکی»(31) سند دیگری است که در سال 2002 از سوی پارلمان و شورای اروپا صادر شد و به طور خاص به این فنّاوری می‌پردازد. موضوع این دستورالعمل که در سال 2009، به موجب دستورالعمل Directive 2009/136/EC اصلاح شده، پردازش آن دسته از اطلاعات شخصی است که در شبکهٔ ارتباطات جمعی الکترونیکی ثبت می‌شود. آنچه در این دستورالعمل مورد تأکید قرار گرفته ضرورت اخذ رضایت از صاحبان اطلاعات برای گردآوری اطلاعات یا دسترسی به اطلاعات ذخیره شده در آرفید است. از آنجا که آرفید می‌تواند به منزلهٔ مکان‌یاب جغرافیایی مورد استفاده قرار گیرد، بند (c) مادهٔ 2 این دستورالعمل اطلاعات مکانی را تعریف کرده است. در مادهٔ 9 نیز مقرر شده نه تنها رضایت صاحبان اطلاعات ضروری است، بلکه آنان، پیش از اخذ رضایت، باید در جریان جزئیات پردازش اطلاعات قرار گیرند.

نتیجه‌گیری

حریم خصوصی جایگاهی مهم در زندگی اخلاقی آدمیان دارد که چشم پوشیدن از آن یا بی‌توجهی به آن پیامدهایی ناگوار برای جامعه در پی خواهد داشت. از دیگر سو، دست کشیدن از فنّاوری «آرفید» نیز، با توجه به کارایی و مزایای آن، نه مطلوب و نه حتی ممکن است. راه چاره برگزیدن راهی میانه است که نه ما را از فواید فنّاوری محروم کند و نه زندگی اخلاقی را ناممکن. جست‌وجو برای یافتن چنین راهی هنوز در مراحل آغازین است. متخصصان دست به کار طرح و آزمایش راه‌حل‌هایی مختلف شده‌اند تا از نقض حریم خصوصی به‌وسیلهٔ فنّاوری آرفید جلوگیری کنند. برای نمونه، می‌توان به استفاده از برچسب‌های مسدودکننده[15]، برچسب‌های بازنوشتنی[16] و برچسب‌های هوشمند[17]، از بین بردن برچسب‌ها[18] یا رمزگذاری اطلاعات برچسب‌ها اشاره کرد(32 و 2 و 8). با این حال، هر کدام از این راه‌حل‌ها نیز مشکلاتی را در پی دارند. در بعضی موارد، مثل رمزگذاری اطلاعات، استفاده از این راه‌حل‌ها به دلیل هزینهٔ بالا مقرون به صرفه نیست. در برخی موارد، راه‌حل‌های پیشنهادی،

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

مانند از بین بردن برچسب‌ها، مانع از انتفاع از برخی کاربردهای مثبت آرفید می‌شوند(33). برای نمونه، پیشنهاد لوازم فرعی متناسب با محصول خریداری شده، ارسال پیام‌های تبلیغاتی متناسب با سلیقهٔ خریدار، کاهش احتمال خرید کالای تقلبی، نظارت بر امنیت کالا (جلوگیری از سرقت)، مرجوع کردن یا تعویض کالا و انقضای تاریخ مصرف مواد غذایی همگی با غیرفعال یا نابود کردن برچسب‌های «آرفید» دشوار یا ناممکن می‌شوند(9).

با این همه، چنانکه در موارد مشابه دیده شده، می‌توان امیدوار بود که فنّاوری سرانجام به نتیجهٔ مطلوب دست یابد و با ارائهٔ محصولات جدیدتر و کارآمدتر مشکلات پیش رو را از میان بردارد. اما این روند در هر صورت نیازمند زمان است و این هزینه‌ای است که برای رسیدن به غایت مطلوب باید پرداخت. آنچه در این بین اهمیت دارد رعایت اخلاق و نیز حقوق شهروندان و احترام به کرامت و جلب رضایت آنان است. آگاه کردنِ مردم از برچسب‌های «آرفید» و خطراتی که برای حریم خصوصی آنها در پی دارد، می‌تواند نخستین گام باشد. لازم است افراد در مورد فنّاوری آرفید و کارآیی آن آگاه شوند. این آگاهی دست کم موارد زیر را در بر می‌گیرد: توضیح دقیق اطلاعات قابل دسترسی به‌وسیلهٔ فنّاوری آرفید، هدف از جمع‌آوری اطلاعات، چگونگی جمع‌آوری و حفظ اطلاعات، چگونگی استفاده از اطلاعات جمع‌آوری شده و چگونگی و میزان دسترسی اشخاص ثالث به اطلاعات جمع‌آوری شده(9). خرید از فروشگاهی که از فنّاوری آرفید استفاده می‌کند، با علم به این موضوع، هر چند نه بالضروره، می‌تواند نشان‌دهندهٔ رضایت خریدار و ترجیح او بر استفاده از مزایای آرفید در مقابل از دست دادنِ بخشی از حریم خصوصی‌اش باشد و بدین‌ترتیب تا حدی از مسئولیت اخلاقی-حقوقی متصدیان این امر بکاهد. آگاهی از وجود برچسب‌های آرفید در محصولات برخی فروشگاه‌ها به شهروندان قدرت انتخاب می‌دهد تا، در صورت نارضایتی از نقض حریم خصوصی‌شان، تدابیر لازم را به کار گیرند و یا از فروشگاه دیگری خرید کنند.

افزون بر این، یکی از مصادیق نقض حریم خصوصی، انتقال اطلاعات از حوزهٔ مربوط به حوزهٔ نامربوط است. کمتر کسی به استفاده از اطلاعات پزشکی‌اش برای مقاصد اخلاقی در پزشکی (برای نمونه در مواردی که به‌طور مستقیم به سلامت خودش مربوط است یا به سلامت خانواده و یا جامعه‌اش) اعتراض می‌کند. اما اگر از اطلاعات پزشکی افراد برای تبعیض در محل کار، ارائه ندادن خدمات تجاری، منع بهره‌گیری از مزایای اجتماعی و مانند آنها استفاده شود، بی‌گمان زبان به اعتراض خواهد گشود. شاید کسی به استفاده از اطلاعات جستجوهای کتابخانه‌ای‌اش برای ارائهٔ بهتر خدمات کتابخانه‌ای به او یا دیگران اهمیت ندهد. اما اگر سلیقه و شخصیت او بر مبنای این اطلاعات نقد شوند، اعتراض خواهد کرد. به‌طور قطع، هیچ‌کس دوست ندارد کتابدار کتابخانه، بر اساس اطلاعات پزشکی او، برای نمونه، کتابی در زمینهٔ رژیم‌های کم چربی به وی پیشنهاد دهد یا پزشک وی، با اطلاع از کتابی که او دربارهٔ بیماری‌ای خاص (مانند ایدز) از کتابخانه به امانت گرفته، سوالاتی در این زمینه از او بپرسد(2). بنابراین، نکتهٔ دیگری که در مورد اطلاعات جمع‌آوری شده به‌وسیلهٔ برچسب‌های «آرفید» اهمیت دارد، لزوم انحصار استفاده از این اطلاعات در حوزهٔ مربوط است. همچنین اطلاعات جمع‌آوری شده نباید بیش از مدتی که ضروری است، نگهداری شود. اطلاعات باید در جریان باشند و با سر رسیدن تاریخ آن پاک شوند(33).

با رعایت اصول پیش‌گفته و آگاهی دادن به افراد دربارهٔ فنّاوری «آرفید» می‌توان ضمن احترام به ارزش غایی و خودآیینیِ آنان، تا رفع کامل مشکلات این فنّاوری، از مزایای فراوان آن بهره برد. این امر به نوبهٔ خود نشانگر آن است که کاربرد نانوفنّاوری، که در این نوشتار از یکی از دستاوردهای آن (آرفید) و ارتباطش با یکی از وجوه ارزشی زندگی انسان (حریم خصوصی) بحث شد، تنها با رعایت «حدود اخلاقی» مجاز و موجه است(34). بیشترِ مقررات «حقوقی» برای جلوگیری از سوءاستفاده از این فنّاوری شکل می‌گیرند یا وضع می‌شوند. پا به پای رشد و گسترش نانوفنّاوری در عرصه‌های گوناگون باید به شکل جزئی و مصداقی به تأثیرات آن بر وجوه گوناگون حیات ارزشی انسان پرداخت و راه‌حل‌های مناسب برای مشکلات پدیدآمده فراهم کرد. بی‌تردید، کاربردهای نانوفنّاوری، همانند همهٔ انواع فنّاوری، همواره باید درون مرزهای اخلاقی باقی بمانند.

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

حمایت حقوقی از حریم خصوصی بسیار مهم است. علم و فنّاوری اغلب پیشاپیش قانون حرکت می‌کنند، چنانکه امروزه کشورهای اندکی هستند که راه‌های نقض حریم خصوصی با استفاده از فنّاوری «آرفید» را شناسایی و ضمانت اجراهای قانونی برای آن تعریف کرده باشند. در بیشتر کشورها، در صورت مواجهه با نقض حریم خصوصی به‌وسیلهٔ فنّاوری یادشده، به قوانین و مقررات کلی از پیش موجود استناد می‌شود که ممکن است برای این منظور کافی نباشند و حتی موجب ترویج نقض و سوءاستفاده از حریم خصوصی نیز بشوند.

آنچه امروزه اهمیت دارد تمشیت حقوقی این گونه فنّاوری‌ها برای بهبود سطح کیفی حیات اجتماعی است، چرا که، در غیر این صورت، فنّاوری‌های نوین تنها بر دشواری و پیچیدگی زندگی اجتماعی خواهند افزود. از این رو، لازم است نظام حقوقی پاسخی درخور و متناسب با هر یک از فنّاوری‌ها، اعم از وضع قوانین جدید، اصلاح قوانین موجود یا پرورش رویهٔ قضائی متناسب، پیش نهد. در پایان، باید افزود که در نظام حقوقی جمهوری اسلامی ایران نیز قوانین و مقررات کافی در این خصوص وجود ندارد و لازم می‌نماید قوانین جدیدی در حوزهٔ حمایت از حریم خصوصی، با تکیه بر فنّاوری خاص آرفید تدوین و وضع شوند.

ملاحظه‌های اخلاقی

در مقالهٔ حاضر، با معرفی منابع مورد استفاده، اصل اخلاقی امانت‌داری علمی رعایت و حق معنوی مؤلفین آثار محترم شمرده شده است.

سپاسگزاری

نویسندگان بر خود فرض می‌دانند از خانم شیرین برومند برای همکاری خالصانه و فعال در بخش تحقیق حقوقی و سرکار خانم فائزه عامری برای مطالعه، نقد و تکمیل کل مقاله صمیمانه تشکر کنند. بدیهی است کلیهٔ اشکالات و معایب بر عهدهٔ نویسندگان است.

واژه‌نامه

1. RFID: Radio Frequency Identification	آرفید: فنّاوری تشخیص هویت از طریق امواج رادیویی
2. Chip	تراشه
3. RFID tags	برچسب‌های «آرفید»
4. Integrated circuit	مدار مجتمع
5. VeriChip	ریزتراشه
6. Universal Product Code (UPC)	کُد جهانی محصولات
7. Privacy	حریم خصوصی
8. Human Dignity	کرامت انسانی
9. Autonomy	خودآیینی
10. Intimacy	صمیمیت
11. Personhood	شخص‌بودن
12. Tort Law	قوانین مسئولیت مدنی
13. Fair Processing	پردازش منصفانهٔ اطلاعات
14. Data Retention	حفظ اطلاعات
15. Blocker tags	برچسب‌های مسدودکننده
16. Rewritable tags	برچسب‌های بازنوشتنی
17. Smart tags	برچسب‌های هوشمند
18. Tag killing	از بین بردن برچسب‌ها

منابع

1. Choi K. (2003). Ethical issues of nanotechnology development in the Asia-Pacific Region, UNESCO. Regional unit for social & human sciences in Asia and Pacific. The Regional Meeting on Ethics of Science and Technology; (5, 7): 332.
2. Van den Hoven J. (2007). Nanotechnology and privacy: instructive case of RFID. In: Fritz A. (ed.). Nanoethics: the ethical and social implications of nanotechnology. New Jersey: John Wiley & Sons. p. 253.
3. O'Mathúna Dónal P. (2009). Nanoethics: big ethical issues with small technologies. London: Continuum. p.75 - 81.
4. Seyed Hosseini M, Eqbali M, Bonyadi Naeeni A, Qazi Noori S. (2014). Relation between science & ethics in nanotechnology. Ethics in Science and Technology; 9(3). (In Persian).
5. Heidari AE. (1386).ethical consideration in nanothechnology. Ethics in Science and Technology; 2(3,4): 23-30. (In Persian).

[DOR: 20.1001.1.22517634.1395.11.1.3.1]

6. Van Den Hoven J, Vermaas PE. (2007). Nanotechnology and privacy: On continuous surveillance outside the panopticon. Journal of Medicine and Philosophy; 32(3): 283–297.

7. Allhoff F, Lin P, Moore D. (2010). What is nanotechnology and why does it matter? from science to ethics. Singapore: Wiley-Blackwell. p. 199.

8. Ahson S, Ilyas M. (2008). RFID handbook: applications, technology, security and privacy. New York: Taylor & Francis Group. p. 470.

9. Peslak Alan R. (2005). An ethical exploration of privacy and radio frequency identification. Journal of Business Ethics; 59: 327–345.

10. Thomson J J. (1975). The right to privacy. Philosophy and Public Affairs; 4(4):295-314.

11. Warren S, Brandeis L. (1890). The right to privacy. Harvard Law Review; 4(5).

12. DeCew J. (2008). Privacy. The Stanford Encyclopedia of Philosophy. In: Edward Zalta N. (ed.). Available at: http:// plato. stanford. edu/ archives/ fall2008/ entries/ privacy. Accessed: July 2013.

13. Parent WA. (1983). Privacy, morality and the lew. Philosophy & Public Affairs; 12(4): 269-288.

14. Gavison R. (1980). Privacy and the limits of law. The Yale Law Journal; 89(3):421-471.

15. Wacks R. (2010). Privacy: a very short introduction. New York: Oxford. p. 49-50.

16. UNESCO. (2007). International conference of right humans. Tehran: Shahid Beheshti Universtiy Publications. P. 74. (In Persian).

17. Rasekh M, Zamani G. (2013). Definition of human munificence: international society & law in 21 century. Tehran: Khane Andishmandan. p. 265-268. (In Persian).

18. Bloustein E J. (1964). Privacy as an aspect of human dignity: an answer to dean prosser. New York University Law Review; 39: 962-1007.

19. Rasekh M. (2014). Freedom as value: Right and responsibility. Tehran: Nashre Nai. p. 266. (in Persian).

20. Roberts P. (2001). Privacy, autonomy and criminal justice rights: philosophical preliminaries. In: Alldridge P, Brants C (ed). Personal autonomy, the private sphere and the criminal law: a comparative study. Portland: Oregon Hart Publishing. p. 59.

21. Rachels J. (1975). Why privacy is important. Philosophy & Public Affairs; 4(4):323-333.

22. Fried C. (1984). Privacy [a moral analysis]. In: Schoeman Ferdinand D. (Ed.). Philosophical dimensions of privacy: an anthology. New York: Cambridge University Press. p. 211.

23. Staples WG. (2007). Encyclopedia of privacy. London: Greenwood Press. p. 395-396.

24. Washington Criminal Code. (2008). possessing or reading or capturing information contained on another person's identification document.

25. California Civil Code, 52.7 (S.B. 31) (2008). Available at: https:// www. leginfo. ca.gov/ pub/ 07-08/bill/sen/sb_0001-0050 /sb_31_bill_ 20080930 _chaptered.html. Accessed: May 2015.

26. Michigan comp laws 28.304 (2008). Available at: https:// www. legislature. mi. gov/ documents/ 2007-2008/ publicact/ htm/ 2008- PA-0023. htm, Accessed: May 2015.

27. Radio Frequency Identification (RFID) in Retail Consumer's Privacy Code of Practice (2007). Available at: https:// www. gs1au. org. Accessed: May 2015.

28. Data Protection Act. (1998). Available at: http://www. legislation. gov.uk/ ukpga/ 1998/29/ contents. Accessed: May 2015.

29. EU Data Protection Directive (1995). Available at: eur-lex.europa.eu. Accessed: May 2015.

30. Iglezakis I. (2011). Regulation models addressing data protection issues in the EU concerning RFID technology. USA: 4th Conference on Information Law and Ethics.

31. Directive 2002/58/EC. (2002). Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

32. Henrici D. (2008). RFID security and privacy: concepts, protocols and architectures. Berlin: Springer.

33. Wasieleski DM, Gal-Or M. (2008). An enquiry into the ethical efficacy of the use of radio frequency identification technology. Ethics and Information Technology; 10: 27-40.

34. Taheri Damneh M, Zare Ahmad Abadi H. (2009). Framework of ethical policy in nanotechnology. Ethics in Science and Technolgoy; 4(3, 4): 102-115. (In Persian).

[DOR: 20.1001.1.22517634.1395.11.1.3.1]