دوفصلنامه دانشنامه حقوق اقتصادی دوره جدید، سال بیست و ششم، شمارۀ۱۵، بهار و تابستان ۱۳۹۸

تحلیل اقتصادی حریم خصوصی در سیستم حقوقی ایالات‌متحده آمریکا

محمدتقی رفیعی[۱]
دانشیار گروه حقوق دانشگاه تهران، پردیس فارابی
مرضیه زوکی نژاد[۲]
دانشجوی دکتری حقوق خصوصی دانشگاه تهران، پردیس فارابی

تاریخ دریافت : ۱۳۹۷/۰۶/۲۰ تاریخ پذیرش: ۱۳۹۸/۰۳/۲۷

چکیده

فنّاوری، تأثیرات اخلاقی و اجتماعی دارد که موجب بحث‌ها و نگرانی‌های زیادی شده است. یکی از مسائل خاص فنّاوری، حریم خصوصی است. باوجود تعاریف متفاوت از حریم خصوصی، تمامی آن‌ها، به مرزهای بین خود و دیگران یا درواقع مرزهای بین خصوصی و عمومی مربوط هستند. در این مقاله، به‌منظور تعیین حدود بهینه مداخله دولت و ارزیابی اقتصادی قطعی از اینکه آیا حمایت قانونی کمتر یا بیشتری از حریم خصوصی موردنیاز است، به مقایسه ارزش کلی حفاظت از حریم خصوصی و افشای داده شخصی(عدم حفاظت از حریم خصوصی) و پیامدهای اقتصادی آن‌ها از طریق تجزیه‌وتحلیل جریان‌های متنوع نظری در مورد اقتصاد حریم خصوصی و همچنین بده بستان‌های حریم خصوصی برای دارندگان داده، موضوعات داده و اشخاص ثالث، پرداخته‌ایم. با توجه به تجزیه‌وتحلیل‌هایی که ارائه گردید، این نتیجه حاصل شد که معنا و گستره حریم خصوصی، بده بستان‌های مربوط به آن و ارزش‌گذاری‌های مصرف‌کنندگان از داده شخصی، بسیار متنوع است. بعلاوه، منافع و هزینه‌های حفاظت از حریم خصوصی و به اشتراک‌گذاری داده شخصی نیز در موقعیت‌ها، شرایط و فروض مختلف متفاوت می‌شود. درنهایت

۱- نویسنده مسئول E-mail: rafiei@ut.ac.ir

2- E-mail: zookinejad@ut.ac.ir

DOI: 10.22067/le.v26i15.75337

تئوری اقتصاد نیز نشان می‌دهد که در اوضاع‌واحوال مختلف، به همان اندازه که توقف جریانات داده می‌تواند رفاه کل را کاهش دهد، حفاظت از حریم خصوصی می‌تواند آن را افزایش دهد؛ لذا مقایسه ارزش کلی حفاظت از حریم خصوصی و داده شخصی و برآورد اقتصادی نهایی و قطعی در مورد اینکه نیاز به حفاظت بیشتر یا کمتری از حریم خصوصی است، دشوار است. بنابراین به نظر می‌رسد حل مسئله حریم خصوصی، به معنای یافتن تعادلی میان حریم خصوصی و به اشتراک‌گذاری اطلاعات در جهت منافع موضوعات داده و جامعه خواهد بود. ارزیابی حریم خصوصی از دیدگاه اقتصادی می‌تواند در یافتن این تعادل به ما کمک کند. روش ایجاد چنین تعادلی به تحقیق دیگری در این زمینه نیاز دارد.

واژگان کلیدی: تحلیل اقتصادی حقوق، حفاظت از حریم خصوصی (اطلاعات)، افشای داده شخصی.
طبقه‌بندی JEL: K13،K39،K

مقدمه

حقوق برای ایجاد نظم اجتماعی و تعادل در روابط به‌ویژه روابط اقتصادی، ناچار است از علوم مختلفی چون علم اقتصاد، جامعه‌شناسی، روانشناسی، آمار، حسابداری، ریاضیات، برنامه‌ریزی و مانند این‌ها نیز بهره‌گیری نماید. یکی از نظریه‌های مهم که در خصوص روابط حقوق و اقتصاد در نیمه دوم قرن بیستم نخست در آمریکا و سپس در کشورهای دیگر مطرح شده، نظریه تحلیل اقتصادی حقوق[1] است که گاهی از آن به نظریه حقوق و اقتصاد تعبیر می‌کنند. در تحلیل اقتصادی حقوق، تأمین عدالت مطرح نیست؛ بلکه کارایی اقتصادی قواعد حقوقی مطرح است. در نظریه تحلیل اقتصادی حقوق، یک پیش‌فرض در نحوه رفتار افراد پذیرفته شده و آن رفتار انسان معقول در حداکثر کردن سود و حداقل ساختن هزینه است. درواقع فرض بر این است که افراد برای منافع خود عمل می‌کنند و در پی افزایش حداکثری دارایی و ثروت خود و کم کردن هرچه بیشتر هزینه‌ها هستند و در هر مورد با سنجش سود و زیان، انتخاب خود را انجام می‌دهند. در نظریه تحلیل اقتصادی حقوق، افزایش کارایی اقتصادی و حداکثر کردن ثروت، به‌عنوان مبنای ارزیابی و

۱- نگرش اقتصادی به حقوق دارای دو شاخه اثباتی و هنجاری است: در نگرش اثباتی حقوق، تنها چیستی حقوق و قواعد آن مورد تحلیل قرار می‌گیرد و اثر حقوق بر متغیرهای قابل‌اندازه‌گیری به‌صورت کمی درمی‌آید؛ نگرش هنجاری نیز در پی انطباق قواعد حقوقی با اصول کارایی اقتصادی است.(Badini, 2004, pp. 91-92)

هدف حقوق معرفی شده است و تحلیل تأثیر قواعد حقوقی بر میزان کارایی در جامعه بر اساس میزان افزایش ثروت، صورت می‌گیرد.(Safai, 2015)

یکی از جذاب‌ترین حوزه‌های تحقیقات اقتصادی از زمان مقاله هایک در سال ۱۹۴۵[۱] در مورد استفاده از دانش در جامعه، ارزش و تنظیم دارایی‌های اطلاعاتی است. مؤثرترین و جذاب‌ترین موضوع اطلاعات، اقتصاد اطلاعات است. در اقتصاد اطلاعات، مطالعات متنوعی چون نقش قیمت در اقتصاد بازار،(Stigler, 1961) ایجاد دانش و انگیزه برای نوآوری،(Arrow, 1962) شیوع اطلاعات نامتقارن و انتخاب نامساعد،[۲](Akerlof, 1978) انتقال اطلاعات خصوصی از طریق فعالیت علامت‌دهی[۳](Spence, 1978) و افشای داوطلبانه اطلاعات(Grossman, 1981) بررسی

۱- فریدریش آگوست فون هایک به آلمانی Friedrich August von Hayek اقتصاددان نئو لیبرال اتریشی تبار در مقاله‌ای با عنوان استفاده از دانش در جامعه (به انگلیسی The Use of Knowledge in Society)، با تأکید بر ماهیت پویا و ارگانیک قیمت و مزایای این پدیده، علیه ایجاد یک انجمن مرکزی قیمت‌گذاری استدلال کرده است. او اظهار می‌کند بازاری که به‌طور متمرکز برنامه‌ریزی شده باشد، هرگز به کارایی یک بازار باز نخواهد رسید؛ زیرا هر فرد تنها بخش کوچکی از همه آنچه را که به‌طور جمعی شناخته‌شده، می‌داند. یک اقتصاد نامتمرکز به این دلیل ماهیت پراکنده نشر اطلاعات در سراسر جامعه را تکمیل می‌کند. برای اطلاعات بیشتر رجوع شود به (Ostovar, 2009, p. 78) (Hayek, 2010)

۲- رفتار خریداران برای کسب اطلاعات بیشتر از ویژگی‌های کالا و مخفی کردن اطلاعات توسط فروشندگان، سبب ایجاد نوعی عدم تقارن و توازن در سطح اطلاعات دو طرف می‌شود؛ لذا خریدار تنها به یک آگاهی نسبی از کالا دست می‌یابد. در این شرایط خریداران سعی می‌کنند قیمت متوسطی را به فروشندگان پیشنهاد کنند. این متوسط قیمت می‌تواند کمتر از حداقل قیمت درخواستی فروشندگان کالای با کیفیت خوب و بالاتر از حداقل قیمت درخواستی فروشندگان کالای با کیفیت بد باشد؛ درنتیجه، قیمت پیشنهادی برای کالای با کیفیت پایین موردتوافق طرفین خواهد بود و صرفاً این‌گونه کالاها مبادله می‌شوند. در این صورت فروشندگان کالای با کیفیت خوب رفته‌رفته بازار را ترک می‌کنند؛ تا آنجا که می‌توان گفت کالای بد، کالای خوب را از بازار خارج می‌کند. این مسئله که در حوزه اقتصاد اطلاعات مطرح می‌شود، به شیوع اطلاعات نامتقارن و انتخاب نامساعد (عکس) The prevalence of asymmetric information and adverse selection معروف است. (Mahdavi & Rajaei, 2016, p. 26)

۳- منظور از علامت‌دهی، بیان این دیدگاه است که علامت دادن در شرکت‌ها، انگیزه ایجاد می‌کند که اطلاعات را افشا نمایند. بر اساس نظریه علامت‌دهی، شرکت‌ها از طریق ارائه اطلاعات بیشتر و بهتری به بازار نسبت به شرکت‌های دیگر، قدرت رقابتی خود را علامت‌دهی و به بازار و ذینفعان مخابره می‌کنند؛ بنابراین، علامت‌دهی به بازار نسبت به کیفیت واقعی شرکت مانند افزایش ارزش شرکت یا کاهش هزینه سرمایه و جلب رضایت سرمایه‌گذاران، دلیلی برای افشای بیشتر اطلاعات می‌باشد. بر پایه این نظریه، شرکت‌هایی که سودآوری و نقدینگی بالایی دارند، تمایل بیشتری برای افشای اطلاعات و علامت‌دهی نسبت به عملکرد خوب جهت جذب سرمایه‌گذار و جلب اعتماد سهامدار دارند؛ زیرا شرکت‌ها به‌منظور دستیابی

شده است؛ لذا بهتر است اقتصاد اطلاعات را نه به‌عنوان یک واحد، بلکه ترکیبی از چند موضوع مرتبط در نظر بگیریم. یکی از این موارد که موردتوجه روزافزون اقتصاددانان و حقوقدانان قرار گرفته است، موضوع پژوهش حاضر یعنی حریم خصوصی است.(Acquisti et al., 2016, p. 443)

مهم‌ترین دلیل اهمیت حریم خصوصی و برجسته شدن آن در شرایط فعلی، تأثیر فنّاوری بر حریم خصوصی است. پیشرفت صنعت و فنّاوری، به حریم خصوصی هجوم آورده و آن را در معرض نابودی قرار داده است.(Aghababaii, 2017, p. 61) با افزایش استفاده از فنّاوری‌های دیجیتالی، تولید و پردازش داده شخصی، به‌صرفه‌تر و سریع‌تر شده است: شرکت‌ها، جزئیات هر تراکنش مشتری و وب‌سایت‌ها، رفتارهای بازدیدکنندگان خود را ثبت می‌کنند و تجمیع کنندگان داده،[1] اطلاعات به‌دست‌آمده از منابع مختلف را برای ساخت پروفایل افراد به یکدیگر مرتبط و متصل می‌کنند. این مقیاس گسترده و بی‌سابقه از تولید داده شخصی به همراه کاهش هزینه ذخیره و تجزیه‌وتحلیل داده و همچنین استفاده‌های متنوع از آن‌ها،[2] منجر به مسائل مهم حریم خصوصی برای اشخاص و سیاست‌گذاران شده است.(Choi et al., 2018, p. 1) باوجود تمایل افراد به حفاظت از امنیت داده خود و جلوگیری از سوءاستفاده از اطلاعاتی که در اختیار شرکت‌ها قرار می‌دهند، آن‌ها همچنین از به اشتراک‌گذاری اطلاعات با همکاران و اشخاص ثالث که معاملات و تبادلات رضایت‌بخش متقابلی را میسر می‌سازد، سود می‌برند. سازمان‌ها نیز باوجود تمایل به آگاهی بیشتر از طریق ردیابی تراکنش‌های طرف‌های معامله خود، نمی‌خواهند طرف معامله خود را با سیاست‌هایی که ممکن است بیش‌ازحد تهاجمی باشد، از خود دور کنند؛ لذا افراد و

به منابع محدود سرمایه با یکدیگر در رقابت هستند. اگر شرکت ازلحاظ گزارشگری مالی خوش‌نام باشد و در مورد فعالیت‌های خود اطلاعات بیشتری اعلام و افشا نماید، توانایی بیشتری در جذب سرمایه خواهد داشت؛ چراکه اعتماد سرمایه‌گذاران را به خود جلب خواهد نمود. (Hoseyni & Safari Gerayli, 2018, p. 2)

1- data aggregators

۲- بسیاری از فعالیت‌های روزمره از طریق فنّاوری اطلاعات، قابل‌ردیابی است. ازآنجایی‌که پرداخت‌های الکترونیکی یک فرد خاص را با خرید خاص مرتبط می‌سازد، امکان ردیابی الگوهای مصرف و همچنین ردیابی اقدامات اشخاص وجود دارد. هزینه کرد افراد، اطلاعات ارزشمندی راارائه می‌دهد؛ چراکه بر اساس آن، می‌توان معاملات زیادی را در مورد فرد موردنظر پیش‌بینی کرد. (Sharman, 2009, p. 719)

سازمان‌ها، با بده بستان‌های پیچیده و غالباً مبهمی در انتخاب تعادل بین به اشتراک‌گذاری و یا پنهان کردن اطلاعات شخصی، روبرو می‌شوند.

در این پژوهش، به‌منظور تعیین حدود بهینه مداخله دولت و ارزیابی اقتصادی قطعی از اینکه آیا حمایت قانونی کمتر یا بیشتری از حریم خصوصی موردنیاز است، با روش توصیفی تحلیلی، پس از بیان مفهوم حریم خصوصی و مفهوم اقتصاد حریم خصوصی، به مقایسه ارزش کلی حفاظت از حریم خصوصی و افشای داده شخصی(عدم حفاظت از حریم خصوصی) و پیامدهای اقتصادی آن ها از طریق تجزیه‌وتحلیل جریان‌های متنوع نظری در مورد اقتصاد حریم خصوصی و همچنین تجزیه وتحلیل بده بستان های متنوعی که دارندگان داده، موضوعات داده و اشخاص ثالث با آن مواجه هستند، می پرداریم.

مبحث اول: مفهوم حریم خصوصی

در اختیار گذاردن داده‌های شخصی، پیش‌شرط انعقاد هر قرارداد است. ولی سؤال این است که افشای اطلاعات تا چه مقدار بوده و موانع حقوقی و طبیعی آن چیست؟(Nicola Jentzsch, 2006, p. 1) یکی از موانع حقوقی در افشای اطلاعات، حریم خصوصی افراد است. برای اولین بار، مفهوم حقوقی حریم خصوصی، توسط وارن و براندیس در سال ۱۸۹۰ تحت عنوان «حق تنها ماندن» ایجاد شد.(Warren & Brandeis, 1890) حریم خصوصی تعریف مشخصی ندارد و مفهومی سیال است. (Ansari, 2013, p. 1) یک ویژگی تقریباً رایج در هر تجزیه‌وتحلیلی از حریم خصوصی این است که موضوع با تذکر در خصوص مشقت اساسی و شاید غیرممکن بودن ارائه تعریف دقیق از حریم خصوصی آغاز می‌شود.(Bennett & Raab, 2006, p. 6)

حریم خصوصی به‌عنوان حفاظت از فضای خصوصی شخص و حق افراد نسبت به تنها ماندن،(Warren & Brandeis, 1890, p. 6) کنترل بر اطلاعات شخصی و حفاظت از آن، (Westin, 1968)، جنبه‌ای از کرامت، خودمختاری و درنهایت آزادی انسان،(Schoeman, 1992) توصیف شده است.

«در ایالات‌متحده، حریم خصوصی موضوعی است که سخنرانی و نظریه‌پردازی، در مورد آن زیاد هست؛ اما تجزیه‌وتحلیل حقوقی مناسب و یا قوی وجود ندارد. این ایده که حقوق حریم خصوصی وجود دارد، یک اصل سیاسی و قضایی پذیرفته‌شده است. بیشتر افراد معتقدند که

حفاظت از حریم خصوصی شخصی در عصر اطلاعات، چالشی اساسی در این دوران است؛ بااین‌حال، ایده حریم خصوصی، راهنمایی‌های محدودی در عصر اطلاعات ارائه می‌دهد». (Bergelson, 2003, p. 400, quotes Raymond T. Nimmer, The Law of Computer Technology, 16.02, at 16-4 2001) «یکی از موانع جدی برای رسیدن به رویکرد جامع در مورد حریم خصوصی در آمریکا، عدم شفافیت ماهیت علایقی است که افراد از اطلاعات مربوط به خود دارند. آیا این علاقه مربوط به کالا، حمایت از مصرف‌کننده، کرامت انسانی، حقوق مدنی و یا همه این علایق است یا هیچ علاقه‌ای وجود ندارد؟» (Samuelson, 2000, pp. 70-71) حق حریم خصوصی اطلاعات، زیرمجموعه‌ای از حریم خصوصی به‌طورکلی است و مانند مفهوم اصلی آن نشان‌دهنده همزیستی شکننده بین دو پارادایم عمده رقیب هست. پارادایم‌های رقیب عبارت از: «حریم خصوصی به‌عنوان رازداری»[1] و «حریم خصوصی به‌عنوان کنترل»[2] هستند.(Bergelson, 2003, p. 401)

مدل حریم خصوصی به‌عنوان کنترل در حقوق ایالات‌متحده آمریکا، حمایت علمی قابل‌توجهی را در سال‌های اخیر به دست آورده است. (Schwartz, 1999, p. 815,820) این مدل، حریم خصوصی اطلاعات را به‌عنوان شکلی از قدرت، «ادعای افراد، گروه‌ها و یا مؤسسات برای تعیین اینکه چگونه و تا چه حد اطلاعات در مورد آن‌ها به دیگران منتقل شود» تلقی می‌کند.(Westin, 1968, p. 7) حریم خصوصی به‌عنوان یک وسیله کنترل تلقی می‌شود که افراد نسبت به قلمرو زندگی خصوصی خویش دارند. طبق این نظر، حریم خصوصی، به افراد، حق استقلال و خودمختاری نسبت به برخی جنبه‌های زندگی خصوصی‌شان را اعطا می‌کند؛ لذا حریم خصوصی، کنترل افراد نسبت به دسترسی دیگران به اطلاعات راجع به آن‌ها و فردی که حق کنترل مذکور را به‌صورت ممنوع ساختن افشای برخی از جنبه‌های زندگی خصوصی اعمال می‌کند، درصورتی‌که دیگران به آن اطلاعات دسترسی یابند، شاهد نقض حریم خصوصی خویش

1- privacy as secrecy
2- privacy as control

است.(Ansari, 2017, p. 219)[۱]

باوجود ارائه تعاریف متفاوت از حریم خصوصی، می‌توان گفت این تعاریف باهم مرتبط هستند؛ زیرا تمامی تعاریف مربوط به مرزهای بین خود و دیگران و درواقع مرز بین خصوصی و به اشتراک گذاشته‌شده یا درواقع عمومی است.(Acquisti et al., 2016, p. 443) به‌طور مداوم این مرزها توسط اشخاص نادیده گرفته می‌شود و تصمیماتی که در مورد چنین مرزهایی گرفته می‌شود، منافع و هزینه‌هایی را برای شخص و جامعه تعیین می‌کند؛ بنابراین، اقتصاد حریم خصوصی، به بررسی بده بستان‌های مربوط به تعادل حوزه عمومی و خصوصی بین اشخاص، سازمان‌ها و دولت‌ها می‌پردازد.(Acquisti et al., 2016, p. 443)

لازم به ذکر است: اولاً، تمرکز تحقیقات اقتصادی اخیر بر حریم خصوصی اطلاعات[۲] و داده شخصی[۳] مصرف‌کننده، به معنای انکار وجود سایر ابعاد حریم خصوصی که ممکن است بررسی آن‌ها در قالب اصطلاحات اقتصادی دشوارتر باشد، نیست؛ ثانیاً، بررسی بده بستان مربوط به حفاظت و افشای داده افراد، بدان معنا نیست که تمامی بده بستان‌های حریم خصوصی، بعد مالی مشخصی دارند؛ بلکه اقتصاد حریم خصوصی، سعی در درک بده بستان‌هایی که به تعادل حوزه‌های خصوصی و عمومی فرد و تعادل منافع مختلف دو طرف معاوضه، مرتبط می‌شود، دارد (Jentzsch, 2007, p. 4)؛ ثالثاً، حریم خصوصی ابعادی معنوی و غیرقابل سنجش دارد که بر

۱- پارادایم کنترل، توسط برخی محققان(Allen, 1999, pp. 861, 865) به خاطر کم‌توجهی به ارزش اجتماعی و سیاسی حریم خصوصی و نقش دولت در شکل‌گیری و اجرای این ارزش، موردانتقاد قرارگرفته است.(Allen, 1999, p. 868) در حقیقت اعتماد کلی بر کنترل اشخاص و مقررات خودتنظیمی صنعت، بدون اقدام قانون‌گذاری و یا اجرایی، ممکن است منجر به فرسایش حریم خصوصی شود.

۲- حریم خصوصی به حریم خصوصی مکانی، حریم خصوصی جسمانی، حریم خصوصی ارتباطات و حریم خصوصی اطلاعات تقسیم‌بندی می‌شود. مرکزیت اصلی مفهوم حریم خصوصی به فضای خانه و دیگر فضاهای خصوصی بسته، مربوط می‌شود؛ ولی به علت افزایش انواع فناوری‌های ذخیره و پردازش اطلاعات در اواخر دهه ۱۹۶۰، تمرکز حریم خصوصی به اطلاعات شخصی سوق پیداکرده است.(Van Dijk, 2010, p. 63)

۳- اطلاعات شخصی، اطلاعاتی است که به یک فرد مربوط می‌شود و از طریق آن می‌توان وضعیت آن فرد نظیر اطلاعات مربوط به وضعیت خانوادگی، جسمی، روحی، اقتصادی، قومی، مذهبی و فرهنگی را شناسایی کرد. رجوع شود به ماده یک قانون انتشار و دسترسی آزاد به اطلاعات.

سلامت افراد تأثیر می‌گذارد[۱] و مستقل از ملاحظات اقتصادی است که در این قسمت در مورد آن بحث خواهیم کرد.

مبحث دوم: نظریه‌های اقتصادی حریم خصوصی

در این قسمت نظریه‌های اقتصادی حریم خصوصی، بیان می‌شود و بین نظریه‌هایی که بر کاهش رفاه در ممنوعیت جریان اطلاعات شخصی تأکید می‌کنند و مطالعاتی که به نتایج متعارضی رسیده‌اند، تمیز داده خواهد شد.

الف) حفاظت از حریم خصوصی، منشأ ناکارایی اقتصادی و کاهش رفاه

اقتصاددانان، از دهه ۱۹۷۰ در حال نگارش موضوع حریم خصوصی بوده‌اند. در محدوده تئوری اقتصادی نئوکلاسیک‌ها در خصوص بازارهای رقابتی کامل، اطلاعات کامل، یعنی قابلیت دسترسی اطلاعات مرتبط برای همه شرکت‌کنندگان در بازار، منجر به کارایی اقتصادی خواهد شد.[۲] یکی از علل شکست بازار، وجود اطلاعات نامتقارن[۳] میان مصرف‌کنندگان و تولیدکنندگان است. این نقص اطلاعاتی، باعث می‌شود که کنشگران بازار تصمیمات اشتباهی اتخاذ کنند؛ درحالی‌که اگر فعالان بازار در خصوص گزینه‌های خود و آثار انتخاب هر یک از آن‌ها، اطلاعات درستی داشته باشند، بازار می‌تواند کارآمدترین و عادلانه‌ترین تخصیص منابع را به بار آورد. (Zarei & Shokuhyan, 2016, p. 174) همچنین یکی از حقوق اولیه مصرف‌کننده، انتخاب آزاد کالاها و خدمات (Asadollahi, 2016, p. 38) و در اختیار داشتن اطلاعات کامل است.

۱- برای مثال، برخلاف قانون‌گذار ایالات‌متحده که رویکردی فایده گرایانه به حفاظت داده داشته است، قانون‌گذار اروپایی حریم خصوصی را یک حق بشری اساسی تعریف می‌کند. (Jentzsch, 2007, p. 4)

۲- هنگامی‌که تمامی مصرف‌کنندگان قیمت‌هایی را که هر مؤسسه کالایش را می‌فروشد بدانند، رقابت منجر به کم کردن قیمت‌ها تا پایین‌ترین حد ممکن که با فناوری تولید، میسر است خواهد شد که این امر رفاه مصرف‌کننده را افزایش خواهد داد.

۳- یکی از منابع نارسایی یا شکست بازار، عدم توازن (تقارن) اطلاعات بین طرف‌های مبادله است. این عدم توازن آن‌قدر زیاد است که مانع انجام مبادله می‌شود. عدم تقارن اطلاعاتی، به موقعیتی اطلاق می‌شود که در آن دو عامل اقتصادی در تقابل با یکدیگر، اطلاعات یکسانی را در اختیار نداشته باشند. در این شرایط ممکن است یک‌طرف به‌اندازه طرف مقابل اطلاعات لازم را نداشته باشد و یا یکی از آن‌ها به‌طورکلی فاقد اطلاعات لازم باشد؛ درواقع در این حالت، عدم تقارن اطلاعاتی به وجود آمده ناشی از پنهان کردن اطلاعات لازم است.(Cooter & Ulen, 2010, pp. 65-66)

مصرف‌کننده باید در شرایطی قرار گیرد که کالاها و خدمات با قیمت‌های رقابتی به وی عرضه شود تا او بتواند با مقایسه محصولات موجود در بازار، از حیث کیفیت و قیمت، دست به انتخاب بزند.(Ghasemi Hamed, 2012, p. 99)

با توجه به نظریه پوزنر از اندیشمندان مکتب شیکاگو،[۱] حفاظت از حریم خصوصی، موجب ناکارایی در بازار می‌شود؛ چراکه به‌طور بالقوه اطلاعات مربوطه را از سایر عاملان اقتصادی پنهان می‌کند؛(Posner, 1981) برای مثال، حفاظت از اطلاعات شخصی یک متقاضی کار که اطلاعات اشتباهی در مورد سوابق خود برای مؤسسه کاریابی ارائه می‌کند، بر تصمیم مؤسسه در خصوص استخدام فرد تأثیر منفی خواهد گذاشت؛ بنابراین، حفاظت از حریم خصوصی یک شخص، به هزینه سودبخشی[۲] برای شخص دیگر، منجر خواهد شد؛ ازاین‌جهت، حذف اطلاعات شخصی افراد به‌وسیله مقررات حریم خصوصی از بازار، موجب انتقال هزینه ویژگی‌های منفی محتمل آن فرد بر سایر بازیگران بازار[۳] خواهد شد.

همچنین وی در تصمیم‌گیری در مورد اینکه آیا قوانین باید به یک مجله اجازه دهد تا فهرست مشتریان خود را به مجله دیگر بدون اخذ رضایت مشترکین بفروشد،(Posner, 1977, p. 393,398) تنها به هزینه مبادله توجه می‌کند. پوزنر نتیجه می‌گیرد نسبت به فروشنده هزینه تحصیل تائید و رضایت مشترک در مقایسه با ارزش فهرست، بالا خواهد بود. (Ibid) از سوی دیگر به خاطر کم‌ارزش بودن اطلاعات افشاشده، هزینه برای مشترک پایین است و خریدار فهرست قادر

۱- مهم‌ترین دغدغه پژوهشگران رویکرد شیکاگو که می‌توان آن را جریان غالب در حقوق و اقتصاد به شمار آورد، به‌کارگیری روش‌های قیاسی مرسوم در دانش اقتصاد برای تحلیل موضوعات محوری حقوق همچون قراردادها، مالکیت، شبه جرم و قوانین کیفری است. پژوهشگران این رویکرد، روش «انتخاب عقلایی» را به‌عنوان ابزاری شناخته‌شده در تحلیل مسائل حقوقی به کار می‌گیرند. حقوقدانان و اقتصاددانان منتسب به رویکرد مذکور، روش‌شناسی علم اقتصاد نئوکلاسیک و سایر مبانی معرفتی آن را پذیرفته و به همین دلیل نیز مهم‌ترین مفروضات معرفتی مکتب اقتصاد نئوکلاسیک که شامل مواردی مانند رفتار بهینه‌سازی افراد، تعادل (تسویه بازارها)، ثبات ترجیحات و فردگرایی روش‌شناختی است همچنان در این رویکرد تداوم دارد. (Sharifzadeh, 2012, pp. 49-50)

2- cost of profitability

۳- در علم اقتصاد، به کسانی که رفتارشان مورد مشاهده قرار می‌گیرد، کنشگر actor گفته می‌شود. همچنین در ادبیات اقتصادی به‌جای کنشگران از اصطلاحاتی مانند بازیگران players، کارگزاران brokers یا عاملان agents استفاده می‌شود. (Naeemi & Rasekh, 2012, p. 138)

نخواهد بود از آن برای تحمیل هزینه‌های قابل‌توجهی بر مشترکین استفاده نماید.(Posner, 1977, pp. 398-399)

استیگلر، معتقد است که دخالت دولتی در بازار اطلاعات شخصی، در بهترین حالت، باعث ناکارایی است. ازآنجایی‌که افراد در افشای عمومی اطلاعات شخصی مطلوب و پنهان نمودن ویژگی‌های منفی، نفع دارند، تصمیم به محافظت از اطلاعات شخصی خود می‌گیرند؛ به‌مانند بدهکاری که نمی‌خواهد سوابق اعتباری خود را افشا نماید.(Stigler, 1980) درواقع وی معتقد است وقتی اطلاعات بیشتر در مورد یک فرد در دسترس است، مشکل‌تر است مردم در مورد خودشان دروغ بگویند و برای معامله‌کنندگان با آن‌ها ارزان‌تر است تا خطرات مربوط به معامله با ایشان را ارزیابی نمایند.(Stigler, 1980, pp. 628-33)

برخی نیز استدلال می‌کنند که به‌طورکلی، محدودیت در جریان آزاد اطلاعات به نام حریم خصوصی حداکثر ثروت اجتماعی نیستند؛ چراکه آن‌ها مانع تصمیم‌گیری شده، هزینه‌های معامله را افزایش داده و کلاه‌برداری را تشویق می‌نمایند.(Murphy, 1995, p. 2382)

همچنین بیان شده است که به اشتراک‌گذاری بدون محدودیت داده شخصی مصرف‌کننده میان دو شرکت، ممکن است نواقص بازار[1] را کاهش دهد و رفاه اجتماعی ازجمله برای مصرف‌کنندگان را افزایش دهد.(Calzolari & Pavan, 2006) اگر اطلاعات شخصی کمی راجع به مصرف‌کنندگان با افراد ثالث به اشتراک گذاشته شود، مصرف‌کنندگان ممکن است متحمل هزینه‌های حفاظت از حریم خصوصی[2] شوند. مصرف‌کننده ممکن است به‌طور معقولانه‌ای بخواهد که بعضی از اطلاعات شخصی وی، برای اشخاص دیگر شناخته شود.(Varian, 2009)[3]

محفوظ ماندن داده مصرف‌کننده، بستگی به حفاظت قانونی و تخصیص حقوق در مورد حفاظت اطلاعات شخصی ندارد؛ بلکه بستگی زیادی به ارزش‌گذاری طرفین ذینفع در داده دارد.(See Noam, 1997a) اگر مصرف‌کننده، حریم خصوصی خود را بیشتر از ارزش‌گذاری‌های

1- market distortions
2- privacy costs
۳- برای مثال، مصرف‌کننده ممکن است بخواهد که ترجیحات مسافرتی وی برای بازاریابان تلفنی، به جهت دریافت پیشنهادها از جانب آن‌ها و انعقاد معامله با موارد دلخواه خود، شناخته شود.

شرکت بازاریابی داده که داده مصرف‌کننده را تحصیل کرده است، ارزش‌گذاری کند، داده حفاظت‌شده باقی خواهد ماند؛ چراکه حتی در فرض فقدان قانونی برای نظام‌مند کردن محافظت، مصرف‌کننده داوطلبانه حاضر به پرداخت جهت حفاظت از داده خود خواهد بود.

ب) حفاظت از حریم خصوصی، منشأ کارایی اقتصادی و افزایش رفاه

در نقد موضع پوزنر و استیگلر در خصوص حریم خصوصی، عنوان شده است که فرضیات رفتار عقلایی[1] که مدل‌های حریم خصوصی مکتب شیکاگو مبتنی بر آن است، نتوانسته پیچیدگی تصمیم‌گیری مصرف‌کننده در مورد حریم خصوصی را مورد لحاظ قرار دهد.(See Hirshleifer, 1980; Murphy, 1995) درواقع، مطالعات مکتب شیکاگو در خصوص حریم خصوصی، به‌پیش از فنّاوری‌های نوین اطلاعات و ارتباطات، برمی‌گردد. توسعه و پیشرفت فنّاوری‌های اطلاعاتی جدید، محققین را به سمت توسعه دیدگاه‌های متنوع‌تر و عمیق‌تری در خصوص بده بستان‌های مرتبط با حفاظت از حریم خصوصی و به اشتراک‌گذاری داده سوق داده است؛ برای مثال، استفاده دست‌دوم از داده شخصی، منجر به بروز مسائل اقتصادی خاصی می‌شود: مصرف‌کننده ممکن است آگاهانه، تصمیم به اشتراک اطلاعات شخصی با یک شرکت بگیرد؛ چراکه انتظار دارد منفعتی خاص از تراکنش به دست آورد؛ باوجوداین، او آگاهی و یا کنترل اندکی بر نحوه استفاده از داده توسط شرکت در آینده دارد.(Varian, 2009) شرکت ممکن است داده مصرف‌کننده را درازای سودی، به اشخاص ثالث بفروشد؛ اما مصرف‌کننده ممکن است در آن سود شریک نشود یا حتی ممکن است زمانی که شخص ثالث از داده سوءاستفاده کند، متحمل هزینه گردد.[2] چنین پیامدهای جانبی منفی بر مصرف‌کننده، به‌وسیله شرکت درونی نشده است.(See Swire & Litan, 1998) همچنین هزینه‌های تراکنش، فقر و سایر موانع ممکن است مانع این شود که مصرف‌کنندگان تحت شرایط متعارف بازار، حفاظت حریم خصوصی به دست بیاورند.(See Noam, 1997b)

بعضی در نقد بحث مکتب شیکاگو بیان می‌دارند که حفاظت داده ممکن است اثرات مثبتی بر

1- assumptions of rational behavior

۲- برای مثال، نامه‌های الکترونیکی ناخواسته، تبعیض قیمتی و غیره(See Odlyzko, 2003)

رفاه اقتصادی داشته باشد؛ برای مثال، حفاظت از حریم خصوصی، می‌تواند حمایت از طرح‌های بیمه‌ای[1] را که در غیر از صورت حفاظت از حریم خصوصی، وجود نخواهد داشت را میسر نماید.(Hermalin & Katz, 2006)

همچنین در رد نظریه کارایی در جریان آزاد اطلاعات استدلال شده است که کارایی چنین نظامی خیلی روشن نیست؛ چراکه اولاً، در جهان واقعی، هرگز اطلاعات در مورد یک فرد، قطعاً، کامل یا دقیق نیست. اگر یک فرد هیچ کنترلی بر انتشار اطلاعات شخصی خود نداشته است، نمی‌داند چه حقایقی ممکن است تصمیم طرف قرارداد را تعیین کند و قادر نیست اشتباهات در سوابق خود را که به‌خودی‌خود ممکن است به رفتار اقتصادی ناکارآمد توسط تمام طرفین معامله منجر شود، تصحیح نماید؛ ثانیاً، بسیاری از شرکت‌کنندگان بالقوه ممکن است از ورود به چنین بازاری منصرف شوند، به همان طریقی که بسیاری از نامزدهای توانا، تاکنون به خاطر ترس از در معرض قرار گرفتن نامحدود و تبلیغات ناخواسته[2] یا افشای وقایع خصوصی، از ورود به زندگی سیاسی امتناع کرده‌اند. درنتیجه، نظام قانونی که به نام کارایی بار حمایت از حریم خصوصی را بر افراد تحمیل می‌کند، به‌احتمال‌زیاد در درازمدت ناکارآمد است.(Bergelson, 2003, pp. 424-425)

علاوه بر این، بازارها ممکن است نتوانند به‌طور کارآمد خود را با اطلاعات اضافی، تنظیم نمایند.(Ibid) در این مدل، دو عامل معقول[3] درگیر تراکنشی هستند که هر دو طرف متمایل به جمع‌آوری اطلاعات راجع به دیگری است؛ لذا حفاظت از حریم خصوصی ممکن است منجر به

۱- اگر تمامی بیمه‌گذاران برای داشتن یا نداشتن بیماری مهلک قرار بود آزمایش شوند، شرکت‌های بیمه عمر، حق بیمه را با توجه به نتایج آزمایش‌ها تعدیل می‌کردند؛ باوجوداین، اگر آزمایش دادن ممنوع شود، با ابتیاع بیمه‌نامه کامل با یک قیمت همگانی، تعادل رقابتی، قرار گرفتن تمام ریسک‌ها بر افراد خواهد بود؛ بنابراین، رفاه اجتماعی، از قرار گرفتن تحت تعادل آزمایش دادن بیشتر خواهد بود به دو دلیل؛ چراکه از هدر رفت اجتماعی هزینه‌های آزمایش جلوگیری خواهد شد و همچنین به این دلیل که افراد ریسک گریز، متحمل ریسک کمتری می‌شوند.

2- unwanted publicity
3- rational agents

تعادل[۱] کارآمد در تخصیص منابع گردد و ممکن است ممنوعیت صریح انتقال اطلاعات، برای کارایی اقتصادی لازم باشد.

همچنین باوجود فنّاوری‌های ردیابی که به کمک آن می‌توان به تمایلات مصرف‌کننده پی برد و سپس تبعیض قیمتی[۲] اعمال کرد،[۳] این‌که آیا حمایت قانونی از حریم خصوصی، رفاه مصرف‌کننده و رفاه کل را افزایش می‌دهد یا خیر، به مهارت مصرف‌کننده بستگی دارد.(Taylor, 2004) مصرف‌کنندگان ساده باور، توانایی فروشنده را برای استفاده از سوابق مصرف‌کننده جهت تبعیض قیمتی پیش‌بینی نمی‌کنند؛ لذا، در تعادل، تمام اضافه رفاه (مازاد) آن‌ها توسط شرکت‌ها گرفته می‌شود؛ مگر این‌که حفاظت از حریم خصوصی از طریق قانون به اجرا درآید؛ باوجوداین، اگر مصرف‌کنندگان از نحوه استفاده از داده توسط تجار آگاه بوده و برای اتخاذ رفتار مطابق با آن، به‌قدر کافی استراتژیک[۴] باشند، نیاز به حمایت قانونی نیست. درواقع مصرف‌کنندگان، به

۱- تعادل equilibrium وضعیتی است که نیروهای اقتصادی مانند عرضه و تقاضا، متعادل هستند و در غیاب نفوذ تأثیرات خارجی، ارزش متغیرهای اقتصادی تغییر نخواهد کرد. (See chapter 2 Dixon, 2001)

۲- یکی از اشکال تبعیض قیمتی، تبعیض قیمتی درجه اول است که به آن «تبعیض قیمتی کامل» نیز گفته می‌شود. فروشنده با قیمت‌گذاری هر واحد فروش با قیمت موردنظر و دلخواه خریدار، به‌طور کامل از مازاد رفاه مصرف‌کننده بهره‌مند می‌شود. این نوع تبعیض قیمت مستلزم آن است که فروشنده اطلاعات کاملی درباره هر یک از مشتریان خود داشته باشد.(Safaei & Hasani Sangani, 2016, pp. 173-174)

۳- برخی نویسندگان معتقدند پاسخ این معما که چرا حریم خصوصی روبه‌زوال است، اهمیت روزافزون تبعیض قیمتی است: حریم خصوصی از بین می‌رود تا تبعیض قیمتی را تسهیل نماید. غالباً محرک تبعیض قیمتی در سازمان‌های تجاری، انگیزه افزایش قیمت است که به توانایی افزایش قیمت، متصل است. همان انگیزه‌ای که بسیاری از سیستم‌های حمل‌ونقل را به ابداع انواع مختلفی از تبعیض قیمت و کیفیت سوق داده است. نفوذ به حریم خصوصی برای تأمین اطلاعاتی به کار می‌رود که به فروشندگان اجازه می‌دهد تمایلات پرداختی خریداران را تعیین نمایند. از یک‌سو، ازلحاظ اقتصادی، تبعیض قیمتی مطلوب است؛ چراکه غالباً سبب افزایش کارایی اقتصادی می‌شود. از سوی دیگر، عموم مردم با تبعیض قیمتی مخالفت شدیدی دارند. هیچ راه‌حلی جهت رفع چنین تعارضی وجود ندارد.(Odlyzko, 2003, p. 1)

۴- رفتار یک شخص بر اهداف شخص دیگر و بالعکس چه به‌صورت مثبت و چه منفی تأثیرگذار بوده و اصطلاحاً نوعی وابستگی متقابل وجود دارد. موقعیت‌های وابستگی متقابل، «شرایط استراتژیک» خوانده می‌شوند؛ زیرا هر بازیگر برای آنکه تصمیم بگیرد چه انتخابی را انجام دهد تا به بهترین وجه به هدفش برسد، باید به‌دقت به رفتار دیگران توجه نماید. نظریه بازی به‌عنوان شاخه‌ای از علم ریاضی، در بررسی موقعیت‌های تعامل‌های اجتماعی، به علوم اجتماعی وارد شده است. این نظریه پیشنهادهایی برای چگونگی رفتار در چنین موقعیت‌های استراتژیک ارائه می‌دهد.(Taherkhani, 2011, p. 220)به

هنگام انتخاب فواید کوتاه‌مدت و هزینه‌های بلندمدت افشای اطلاعات و تعدیات حریم خصوصی، به‌درستی عمل نمی‌کنند.

نتایج مشابهی با مدل دیگری از برخی نویسندگان به‌دست‌آمده است. در این مدل، تجار به فنّاوری‌های ردیابی و مصرف‌کنندگان به فنّاوری‌های مخفی کردن دسترسی دارند.[1] در این صورت، سود تاجر صرفاً زمانی افزایش می‌یابد که ردیابی برای تمهید خدمات فزاینده و شخصی شده برای مصرف‌کننده نیز استفاده شود.(Acquisti & Varian, 2005)

علاوه بر هزینه‌های حریم خصوصی مربوط به تبعیض قیمتی و پیامدهای رفاه اجتماعی از به اشتراک‌گذاری داده مصرف‌کننده با اشخاص ثالث، سوءاستفاده از اطلاعات شخصی برای بازاریابی ناخواسته[2] نیز می‌تواند موجب ایجاد اثر جانبی منفی برای مصرف‌کننده می‌گردد.(Hann et al., 2003)

مبحث سوم: منافع و هزینه‌های داده افشاشده و داده حفاظت‌شده

بخشی از مباحث تحلیل اقتصادی حقوق، با بهره‌گیری از ابزارهای اقتصادی به تحلیل مباحث حقوقی می‌پردازد و از این حیث که سعی می‌کند از هرگونه پیش‌داوری ارزشی در مورد قواعد حقوقی به دور باشد، می‌تواند پیامدهای مثبت و منفی به‌کارگیری یک قاعده را نمایان سازد.(Shokuhyan & Edrisian, 2017, p. 7)

در این قسمت، به بررسی ارزش اقتصادی داده شخصی و حفاظت از حریم خصوصی با تجزیه‌وتحلیل منافع و هزینه‌های فردی و اجتماعی مربوط به افشا و حفاظت می‌پردازیم. در این بحث، موضوعات داده، مصرف‌کنندگان و دارندگان داده، شرکت‌ها هستند. تجزیه‌وتحلیل با

عبارتی نظریه بازی‌ها، یک تحلیل ریاضی از هر موقعیت اجتماعی است که در آن یک بازیکن سعی می‌کند تا آنچه را که دیگر بازیکنان انجام می‌دهند، درک کرده و با استفاده از این حدس‌ها، بهترین استراتژی را انتخاب کند.(Jalali & Nasrollahi, 2019, p. 135)

۱- در تجارت اینترنتی، تجار می‌توانند از کوکی‌ها برای ردیابی رفتار مصرف‌کننده به‌خصوص خریدهای گذشته، استفاده کنند و مصرف‌کنندگان به فناوری‌های گمنام کردن (حذف کوکی‌ها، استفاده از جستجوگرهای ناشناس و یا ابزارهای پرداخت) برای پنهان کردن رفتار دسترسی دارند.

2- unsolicited marketing

معرفی بازار برای داده شخصی و بازار برای حریم خصوصی به‌عنوان دوروی یک سکه بیان می‌شود که در آن داده افشاشده[۱] ممکن است منافع و هزینه‌هایی را در برداشته باشد که نسبت به هزینه‌ها و منافع مرتبط با داده حفاظت‌شده[۲] برای هم موضوعات داده و هم دارندگان داده، متفاوت و یا یکسان باشند؛ باوجوداین، ارائه فهرست و طبقه‌بندی کاملی از تمام هزینه‌ها و منافع مرتبط با داده افشاشده و حفاظت‌شده در این پژوهش امکان‌پذیر نیست.

الف) منافع و هزینه‌های داده افشاشده

منافع و هزینه‌های داده افشاشده برای دارندگان داده، موضوعات داده و همچنین اشخاص ثالث به شرح ذیل است.

منافع داده افشاشده

منافع داده افشاشده به شرح ذیل قابل‌بررسی است.

منافع داده افشاشده برای دارندگان داده

«توانایی ایجاد روابط جذاب با مشتریان فردی، رؤیای بازرگانان است. فنّاوری در شکل پایگاه داده، در حال تبدیل این رؤیا به واقعیت است. اکنون شرکت‌ها می‌توانند ترجیحات مشتری را دنبال کنند و تبلیغات و پیشرفت‌های خود را با آن نیازها متناسب کنند».(Deighton & Blattberg, 1991, pp. 5-14) امروزه این پیش‌بینی به واقعیت مبدل گشته است. به لحاظ آنلاین، ترکیب

۱- مراد از داده افشاشده، وضعیتی است که موضوع داده ممکن است عالماً، عامداً و یا غیر عامدانه، داده را با دارندگان داده به اشتراک گذاشته و یا حالاتی که در آن سایر اشخاص، ممکن است تصرف داده را بدون آگاهی و یا حتی رضایت موضوع داده به دست آوردند.

۲- مراد از داده حفاظت‌شده، اشاره به وضعیتی است که چنین افشاهایی صورت نگرفته است؛ صرف‌نظر از اینکه به جهت حفاظت عمدی موضوع داده از اطلاعات شخصی بوده و یا این‌که نگه‌دارنده بالقوه داده در دسترسی بعدی به داده ناتوان و یا بی‌علاقه بوده است.

مواردی چون آدرس آی پی، کوکی‌ها، داده کلیک استریم،[1] ایجاد تصاویری دقیق از رفتار مصرف‌کننده را میسر ساخته است. به لحاظ آفلاین، آژانس‌های گزارش اعتبار و تجمیع کنندگان داده، داده مصرف‌کننده را از سازمان‌های عمومی و خصوصی خریداری و تصفیه کرده و آن را برای گردآوری سوابق غنی از اطلاعات مصرف‌کننده مانند سوابق اعتباری و سلامت، ترجیحات فردی، الگوهای خرید، طبقه‌بندی می‌کنند و دوباره به بخش‌های عمومی و خصوصی می‌فروشند. ادغام داده‌های فردی آنلاین و آفلاین و همچنین پیگیری رفتار آنلاین از طریق سایت‌ها و شبکه‌های تبلیغاتی و ادغام اطلاعات رفتاری و وب‌گردی آنلاین با اطلاعات شخصی که خود مصرف‌کننده از طریق رسانه‌های اجتماعی افشا می‌سازد، نیز میسر شده است.

شرکت‌ها می‌توانند به‌طور گسترده‌ای از توانایی آگاهی یافتن بسیار زیاد در مورد مشتریان کنونی و یا محتملشان منتفع شوند. مجموعه‌های داده غنی مصرف‌کنندگان می‌تواند توانایی‌های بازاریابی شرکت‌ها را با ارتقای توانایی آن‌ها در بررسی بازارهای هدف یا مشتریان خاص و با کاهش هزینه‌های تبلیغاتی خود بهبود بخشد.(Acquisti, 2010, pp. 12-13)

با تجزیه‌وتحلیل حجم زیادی از داده مصرف‌کننده، شرکت‌ها قادر به پیش‌بینی گرایش‌های تجمیع شده نظیر تغییرات تقاضای مصرف‌کننده و همچنین ترجیحات افراد خواهند بود؛ بنابراین خطرات مالی کاهش می‌یابد و بازده‌های سرمایه‌گذاری بازاریابی به حداکثر می‌رسد. آن‌ها می‌توانند توانایی خویش را در ارائه پیشنهادهای سودمند به مصرف‌کنندگان و همچنین در اجرای تبعیض‌های قیمتی سودافزا بهبود بخشند. علاوه بر این، از طریق مشاهده رفتار فرد، شرکت‌ها می‌توانند به چگونگی بهبود خدمات و یا طراحی دوباره آن پی ببرند. مثالی از این‌که چطور اطلاعات مصرف‌کننده می‌تواند برای کسب سود بیشتر مورداستفاده قرار گیرد، تبلیغات آنلاین است که می‌تواند بر هر فرد و بر اساس رفتار آنلاین وی نظیر جستجوهای وی، سایت‌های بازدید شده، داده کلیک‌ها بر روی یک سایت و استنتاج‌هایی که از طریق آن داده صورت پذیرفته است،

۱- داده‌های مسیر کلیک یا کلیک استریم click path or clickstream توالی هایپر لینک‌های یک شخص یا بازدیدکنندگان یک وب‌سایت یا چندین وب‌سایت که یک سایت خاص را دنبال می‌کنند است که در یک نظمی ارائه می‌شود. (Click path," 2019")

هدف‌گذاری شود.(Ibid, p. 13)

چنین قابلیت هدف‌گذاری دلالت بر این دارد که شرکت‌ها هزینه تبلیغات هدررفته بر مصرف‌کنندگانی را که تمایلی به پذیرفتن آن‌ها را ندارند کاهش می‌دهند. علاوه بر این، ازآنجایی‌که عرضه تبلیغات آنلاین، رفتار از طریق کلیک[1] و گاهی اوقات حتی رفتار آنلاین پس از عرضه قابل‌اندازه‌گیری هستند، تبلیغ‌کنندگان می‌توانند نظارت کنند و میزان تأثیر تبلیغات آنلاین را بیشتر از سایر کانال‌های بازاریابی بهبود ببخشند. اولاً، این امر دربردارنده منافع بیشتری برای بازاریابان و بازرگانان است؛ چراکه ارزش تبلیغات رفتاری هدفمند بیشتر از ارزش تبلیغات غیر هدفمند است؛ ثانیاً، این امر می‌تواند برای مصرف‌کننده نیز سودآور باشد: تبلیغات هدفمند ممکن است اطلاعات مفیدی در اختیار مصرف‌کننده قرار دهد؛ چراکه تبلیغات، متناسب با علایق مصرف‌کننده هستند؛ ازاین‌جهت، این‌گونه هدف‌گذاری ممکن است هزینه برقراری ارتباط تولیدکننده با مصرف‌کننده و هزینه کسب اطلاعات سودمند از جانب مصرف‌کننده را کاهش دهد.(Ibid, p. 14)

مثالی دیگر از این‌که چطور جمع‌آوری و تجزیه‌وتحلیل جریانات داده مصرف‌کننده می‌تواند منجر به افزایش رفاه گردد، صنعت گزارش اعتبار است. اطلاعات جمع‌آوری‌شده، تجزیه‌وتحلیل شده و سپس دوباره فروخته‌شده به‌وسیله آژانس‌های گزارش اعتبار برای تخصیص اعتبار، به‌طور کارآمد در میان وام‌گیرندگان احتمالی استفاده می‌شود؛ لذا موجب افزودن ارزش به بازار خواهد بود.(Rubin & Lenard, 2002)

سازمان‌ها همچنین به‌طور غیرمستقیم از داده مصرف‌کننده با فروش آن به سایر شرکت‌ها منتفع می‌شوند. انتفاع مذکور برای شرکت‌هایی که محصول اولیه آن‌ها داده مصرف‌کننده نیست، نیز میسور است.[2]

حتی زمانی که داده فردی مصرف‌کننده به‌صورت شخصی شناسایی‌شده نیست، تجمیع ممکن

1- click-through behavior

۲- دارایی اولیه شرکت‌های وب ۲ نظیر شبکه‌های اجتماعی آنلاین، داده مصرف‌کننده، است. درواقع مصرف‌کنندگان آن‌ها، محصول هستند. مشتریان واقعی متشکل‌اند از بازاریابان، تبلیغ‌کنندگان و تجمیع کنندگان داده که ذینفع در داده رفتاری و افشاشده کاربر که بر روی پلت فرم تولید می‌شوند، هستند.

است موجب سوددهی به شرکت‌ها شود. شرکت‌ها ممکن است از پی بردن به تمایلات مصرف‌کننده بر اساس تجزیه‌وتحلیل‌های مرکب از رفتار عاملان شخصی زیاد سود ببرند.

منافع داده افشاشده برای موضوعات داده

موضوعات داده می‌توانند به‌طور مستقیم از به اشتراک‌گذاری اطلاعات شخصی با شرکت‌ها منتفع شوند. یک مشتری ممکن است برای افشای داده شخصی، خسارت پولی مستقیم[1] نظیر تخفیف‌ها و یا منافع غیر عینی و غیر محسوسی[2] چون شخصی و سفارشی شدن محتوای اطلاعاتش را دریافت نماید. در برخی موارد، فرد همچنین ممکن است در قبال ارائه داده به اشخاص ثالث، در قالب خدمات بهبودیافته شده، از پیشنهادهای هدفمند و یا نامه‌های کمتر مزاحم[3] سود ببرد.[4] متعاقباً، برخی اقتصاددانان نیز «مال‌انگاری»[5] حریم خصوصی را پیشنهاد کرده‌اند که در آن فرد اطلاعات شخصی خودش را در بازار می‌فروشد.

اطلاعات بازاریابی بهتر در دسترس شرکت‌ها، ممکن است به‌طور غیرمستقیم موجب سودرسانی به مشتریان و جامعه از طریق پیامدهای جانبی مثبت نیز گردد؛ برای مثال، داده بهتر مصرف‌کننده ممکن است به شرکت‌ها این توانایی را بدهد که محصولات خاص به بازار بیاورند که بدون داده متمرکز در خصوص مصرف‌کنندگان علاقه‌مند بالقوه، توسعه و گسترش آن ممکن است بسیار پرخطر باشد. گاهی اوقات، قیمت‌ها ممکن است درنتیجه تبلیغات و بازاریابی هدفمند کاهش یابد. اتلاف اجتماعی نیروی کار صرف شده در ساخت داده مشتری بر اساس اطلاعات غلط و جزئی، ممکن است با یک بازار داده شخصی سازمان‌یافته، کاهش یابد. ترکیب مناسب به اشتراک‌گذاری و مخفی نمودن اجزای متفاوت اطلاعات، می‌تواند توأمان به شرکت‌ها و مصرف‌کنندگان از یک‌سو برای کاهش مزاحمت‌های بازاریابی‌های تلفنی و همچنین از سوی

1- immediate monetary compensation
2- intangible benefits
3- less junk mail
۴- موضوع فوق تحت این فرض است که اطلاعات، درواقع مشروط بر استفاده شدن به‌وسیله بازاریابان جهت غربال پیشنهادها برای ارسال به مصرف‌کنندگان خواهد بود. (See Varian, 2009)
5- propertization

دیگر افزایش اعتبار داده جمع‌آوری‌شده کمک کند. علاوه بر این، مصرف‌کنندگانی که به دنبال خرید ارزان هستند ممکن است از تبعیض قیمتی بر پایه اطلاعات سود ببرند؛ به این معنا که ممکن است بتوانند کالاها را با قیمتی پایین‌تر به دست آورند.

تبلیغات آنلاین، خصوصاً تبلیغات هدفمند، ممکن است هم مصرف‌کنندگان را مطلع و برای آن‌ها اطلاعات بهتر با هزینه جست‌وجوی کمتر فراهم کند و هم به سایر خدمات اجازه دهد که به‌صورت رایگان به مصرف‌کنندگان ارائه شوند و در ظاهر نیز از تبلیغات غیر هدفمند، کمتر مداخله‌گر، ناخوانده و مزاحم است.(Goldfarb & Tucker, 2011) وجود بازار ثانویه، ممکن است منجر به اثرات مثبت خارجی برای مصرف‌کننده گردد.[۱]علاوه بر این، در سطح اقتصاد کلان نیز افشای داده شخصی منافعی در بردارد: تجزیه‌وتحلیل و تجمیع رفتار آنلاین، داده حس‌گر،[۲] تصمیمات افراد از یک انبوه عوامل اقتصادی جداگانه ممکن است موجب شناسایی زودهنگام گرایش‌ها و الگوهایی شود که در غیر این صورت شناختن آن‌ها دشوار و یا غیرممکن است و یا حداقل در یک مدت‌زمان محدود میسر نیست که این موضوع می‌تواند به جامعه به‌عنوان یک کل سود برساند.[۳]

باوجوداین، ممکن است عنوان شود که مصرف‌کنندگان ممکن است ازاین‌گونه منافع، بدون الزام به افشای داده شخصی شناسایی‌شده برخوردار گردند: فنّاوری‌های افزایش حریم خصوصی می‌توانند هم ضرورت حفظ حریم خصوصی و هم نیاز به انتشار داده را از طریق حفاظت و افشای

۱- برای مثال، داده‌ای که در اختیار یک وب‌سایت قرار گرفته است، آن خدمت را مناسب‌تر و یا کارآمدتر بر روی سایت دیگری، به دلیل به اشتراک‌گذاری داده در میان خدمات متفاوت ایجاد می‌کند؛ به‌مانند ارتباط فیس‌بوک که تصدیق یکپارچه‌ای را بر وب‌سایت‌های شخص ثالث فراهم می‌کند و موجب کاهش هزینه عضویت کاربر در میان سایت‌های متفاوت می‌شود.

۲- داده‌های حس‌گر sensor data خروجی و تولید یک دستگاه است که برخی انواع ورودی از محیط فیزیکی را تشخیص و پاسخ می‌دهد. این خروجی ممکن است برای ارائه اطلاعات، ورودی به سیستم دیگر یا برای هدایت روند استفاده شود. https://internetofthingsagenda.techtarget.com/definition/sensor-data

۳- برای مثال، نظارت و تجمیع جست‌وجوهای وب، می‌تواند موجب شناسایی سریع شیوع یک بیماری عفونی گردد؛ ترکیب ورودی‌هایی از دستگاه‌های قابل‌حمل ممکن است برای کنترل ترافیک و ازدحام، به کار گرفته شود؛ داده به‌دست‌آمده از حس‌گرهای از راه دور و توزیع‌شده بر دستگاه‌های مصرف‌کننده ممکن است برای نظارت محیطی مورداستفاده قرار گیرد.

گزینشی اجزای اطلاعات شخصی برطرف نمایند.(Acquisti, 2010, p. 18)

منافع داده افشاشده برای اشخاص ثالث

تصمیم افراد جهت به اشتراک‌گذاری اطلاعات شخصی خویش، سبب می‌شود اشخاصی که به اطلاعات آن‌ها دسترسی دارند، در مورد حتی کسانی که تصمیم به اشتراک‌گذاری اطلاعات شخصی خود نمی‌گیرند، اطلاعات بیشتر یا بهتری[۱] کسب نمایند.[۲] هر مصرف‌کننده ممکن است از ضرر احتمالی افشای داده شخصی به خودش آگاه باشد؛ ولی ممکن است پیامدهای خارجی مثبت یا منفی آن را بر اشخاص ثالث و سایر کاربران در نظر نگیرد.(Choi et al., 2018, p. 2) یکی از پیامدهای مثبت اطلاعات، در فرآیندهای استنتاج داده است. مطابق یکی از قواعد علم اقتصاد به نام «صرفه‌جویی به مقیاس»،[۳] هر چه داده، بیشتر باشد، امکان استنتاج بیشتری از داده وجود خواهد داشت. اشخاصی که به داده دسترسی دارند، می‌توانند تجربه کاربران دیگر را اصلاح کنند؛ چراکه داده بیشتر می‌تواند منجر به مطابقت دادن عوامل مؤثر بیشتر یا نتایج بهتر جستجوی آنلاین شود. (Ibid, pp. 7-8)

هزینه‌های داده افشاشده

هزینه‌های داده افشاشده برای دارندگان داده ناشی از داده افشاشده و فعل جمع‌آوری داده است و برای موضوعات داده، هزینه‌ها به دو دسته ذهنی و عینی و همچنین هزینه‌های بی‌واسطه، باواسطه

۱- در تحقیقی در آمریکا توسط دانشجویان دانشگاه ام آی تی، نشان داده شده است که تمایلات جنسی مردان با تجزیه‌وتحلیل سایت‌های شبکه‌های اجتماعی چون فیس‌بوک قابل پیش‌بینی است؛ بر این اساس که مردان هم‌جنس‌گرا به نسبت مردان سالم دوستان پسر بیشتری دارند. ازاین‌رو، گرایش جنسی مردان صرفاً بر اساس جنسیت دوستان آن‌ها قابل پیش‌بینی است. (Choi et al., 2018, p. 7)

۲- چنین پدیده‌ای، پیامد جانبی اطلاعات نامیده شده که می‌تواند مثبت یا منفی باشد. پیامد جانبی اطلاعات به علت پیشرفت عمده در تجزیه‌وتحلیل‌های کلان داده، بسیار مهم و قدرتمند است.(Choi et al., 2018, p. 2)

۳- مفهوم صرفه‌جویی به مقیاس Economies of scale به کسب مزیت کاهش هزینه در اثر افزایش حجم ستاده اشاره دارد؛ یعنی با افزایش حجم ستاده، هزینه متوسط هر واحد ستاده کاهش می‌یابد. (Salehi & Khanmohammadi, 2018, p. 70)

و احتمالی تقسیم می‌شود.

هزینه‌های داده افشاشده و فعل جمع‌آوری داده برای دارندگان داده

هزینه‌های داده افشاشده و فعل جمع‌آوری داده در دو قسمت مجزا بررسی شده است.

هزینه‌های داده افشاشده

دارندگان داده ممکن است از داده افشاشده متحمل هزینه‌های مادی و معنوی شوند. برخی از این هزینه‌ها، ممکن است مربوط به‌صرف جمع‌آوری داده باشند؛ مثل زمانی که مصرف‌کنندگان یک شیوه خاص جمع‌آوری داده را بیش‌ازحد مداخله‌گر می‌پندارند. سایر هزینه‌ها مربوط به استفاده و سوءاستفاده واقعی از داده جمع‌آوری‌شده است. شرکت‌های آنلاین و آفلاین بسیاری از طریق بازار برای رفتارهای جمع‌آوری داده‌ای که لزوماً غیرقانونی نبوده‌اند و به‌عنوان تعدی بر حریم خصوصی مصرف‌کننده در نظر گرفته‌شده است، مجازات گردیده‌اند.[1] نقض‌های داده، دربردارنده علل متفاوتی از صرف تلف لپ تاب‌های دربردارنده داده مصرف‌کننده که شاید درواقع به‌وسیله اشخاص با سوءنیت درخطر افتاده است تا افشای داده مصرف‌کننده در پی حمله هکرها است.

شرکت‌های نقض‌کننده ممکن است متحمل هزینه‌های زیادی برای جبران خسارت مصرف‌کننده شوند؛ اگرچه اکثر دعاوی حقوقی مصرف‌کنندگان در مقابل شرکت‌های نقض‌کننده داده به‌وسیله دادگاه‌های ایالات‌متحده رد می‌شود، (Romanosky & Acquisti, 2009) غالباً مصرف‌کنندگان به‌وسیله شرکت‌های نقض‌کننده مورد پیشنهاد و یا بازپرداخت هزینه‌های هشدارهای اعتباری[2] و خدمات بیمه‌ای سرقت هویت قرار می‌گیرند. علاوه بر این،

۱- در سپتامبر ۲۰۰۰، شرکت آمازون آزمایش‌های قیمت‌گذاری پویا را انجام داد که در آن فیلم‌های دی‌وی‌دی به مشتریان مختلف باقیمت‌های مختلف (تا ۴۰ درصد متفاوت) بر اساس تاریخ خرید آن‌ها فروخته می‌شدند. زمانی که خبر این آزمایش قیمت‌گذاری پویا منتشر گردید، شرکت آمازون توسط گروه‌های حفظ حریم خصوصی مصرف‌کننده مورد انتقاد شدید قرار گرفت. این شرکت به‌طور عمومی عذرخواهی و مبالغ اضافی را به مشتریان مسترد نمود. (Taylor, 2004, pp. 631-632)

2- credit alerts

صرف فعل مطلع نمودن مصرف‌کنندگان از نقض، می‌تواند هزینه‌بردار باشد. مصرف‌کنندگان همچنین ممکن است شرکت‌هایی را که به‌اندازه کافی محافظت‌کننده داده خویش نمی‌پندارند، به‌طور غیرمستقیم برای مثال از طریق فسخ رابطه خود با شرکت، مجازات کنند. نگرانی‌های حریم خصوصی ممکن است تمایل مصرف‌کننده را به انجام برخی معاملات فقط به جهت ترس از خسارات حریم خصوصی آینده، کاهش دهند.

باوجوداین، تخمین دقیق اثرات کار دشواری است: اولاً، رفتارهایی نظیر فسخ رابطه ممکن است دقیقاً عکس‌العمل واقعی مصرف‌کننده را پیش‌بینی نکند؛ چراکه نقض‌های داده ممکن است به تصویر شرکت بدون حذف مصرف‌کنندگان صدمه بزند؛[1] ثانیاً، تعرض‌های متعدد حریم خصوصی و تعداد فزاینده نقض‌های داده، ممکن است درنهایت از طریق فرایند روانی عادت، منجر به عدم واکنش مصرف‌کنندگان گردد. به‌طور مشابه، فعالیت‌های تبعیض قیمتی، با دادن این توانایی به بازرگانان که بتوانند به‌طور کارآمدی قیمت‌ها را در معاملات آنلاین پنهان نمایند و احتمال پیوند داده[2] در میان وب‌سایت‌ها به طرقی که برای عموم مصرف‌کنندگان غیرقابل‌تصور باشد، ممکن است مورد بی‌توجهی قرار گیرد و درنتیجه مجازات نشود.

به‌طور مشابه، در این پرونده‌ها وضع سطح مناسبی از مجازات و مسئولیت برای سوءاستفاده‌های از داده مصرف‌کننده[3] دشوار است: آیا مجازات می‌بایست متناسب با خسارت مصرف‌کننده باشد که خود این ارزیابی ممکن است دشوار باشد و یا این‌که برای ایجاد عامل بازدارنده، تحت قاعده و اصول معینی درآید؟ وضع کیفر بسیار شدید ممکن است مانع رشد و خلاقیت شود و وضع آن

1- Ellen Messmer, Data Breaches Hurt Corporate Image but Don't Necessarily Drive Customers way, Networked World, Aug. 29, 2007.

۲- داده‌های پیوندی، داده‌های منتشرشده در وب و صورت ماشین خوان است که معنای آن داده‌ها به‌صورت دقیق تعریف‌شده و درعین‌حال به سایر مجموعه داده‌های موجود در وب، پیوند برقرار کرده است و می‌تواند به‌وسیله سایر مجموعه‌های داده نیز مورد پیوند قرار گیرد.(Niknia, 2016, p. 182)

۳- تعدادی از نهادهای نظارتی حریم خصوصی در سرتاسر دنیا دعاوی جمعی در برابر شرکت‌های درگیر در خطاهای حریم خصوصی، مطرح کرده‌اند. برای مثال، در پی ناتوانی در مسدود کردن یک ویدئو بر روی سایت یوتیوب که پسری توهمی را نشان می‌دهد که توسط سایر دانش آموزان مورد آزار و اذیت قرار می‌گیرد، سه مسئول اجرائی گوگل توسط یک دادگاه ایتالیایی به شش ماه زندان محکوم شدند. رجوع شود به (Liptak, 2010)

به‌صورت خفیف نیز ممکن است منجر به اثر معکوس مشروع سازی رفتار تعدی‌گرایانه گردد و آن را تنها مبدل به یک هزینه انجام تجارت گرداند.(Acquisti, 2010, pp. 22-23)

هزینه‌های فعل جمع‌آوری داده

منافع ناشی از داده افشاشده، در تقابل با هزینه‌های لازم برای جمع‌آوری و پردازش داده قرار می‌گیرد. این هزینه‌ها زمانی قابل توجیه هستند که شرکت‌ها انتظار کسب منافع بیشتری از تجزیه‌وتحلیل داده مصرف‌کننده دارند، درحالی‌که جلوی هزینه‌هایی را که ممکن است از سوءاستفاده‌های آن ناشی شود را می‌گیرند. هزینه‌های جمع‌آوری و نگهداری داده به‌طور پیوسته با سیر تکاملی فنّاوری اطلاعات رو به کاهش است.(Krasnikov et al., 2009)

هزینه‌های داده افشاشده برای موضوعات داده

نظرسنجی‌های بازار در طول سال‌ها به‌طور پیوسته نشان داده است که مصرف‌کنندگان در رابطه با شیوه جمع‌آوری داده توسط شرکت‌ها نگران هستند. طبقه‌بندی هزینه‌هایی که مصرف‌کنندگان به دلیل افشا و یا سوءاستفاده از داده متحمل می‌شوند، مشکل و پیچیده است؛ چراکه هزینه‌ها دربردارنده خساراتی است که ممکن است مدت مدیدی پس از افشای داده اتفاق بیفتند.(Acquisti, 2010, p. 25). چند نوع طبقه‌بندی از هزینه‌های حریم خصوصی به شرح ذیل است:

هزینه‌های ذهنی و عینی[1]

برخی نویسندگان معتقدند که ضررهای حریم خصوصی؛ مثل سوختگی که ضرر ناشی از حرارت است، منحصربه‌فرد با ویژگی‌ها و مرزهای خاص خود است و این ضررها را به دو دسته ذهنی و عینی تقسیم می‌کنند. ضررهای ذهنی حریم خصوصی، اطلاع از مشاهده ناخواسته و تصور تحت نظارت بودن و دربردارنده حالات روانی ناخوشایندی چون اضطراب، خجالت و ترس است؛

1- subjective and objective harms

مثال‌های آن از استراق سمع توسط یک صاحب‌خانه تا نظارت عمومی دولت می‌تواند باشد. ضررهای عینی حریم خصوصی، استفاده غیرمنتظره و اجباری از اطلاعات فرد علیه وی است؛ مثال‌های آن شامل نتایج متنوعی چون سرقت هویت، انتشار اطلاعات طبقه‌بندی‌شده‌ای که یک عامل سری را آشکار سازد و استفاده از خون شخص مظنون به رانندگی در حال مستی به‌عنوان مدرکی علیه وی است.(Calo, 2011, p. 1131) ضررهای ذهنی و عینی از هم متمایز ولی به هم مرتبط است. ادراک مشاهده ناخواسته، مثل تهدید به ایراد ضرب[1] که خوف از ایراد ضرب[2] است، به‌طور گسترده‌ای یک خوف از زیان ناشی از اطلاعات است.(Calo, 2011, p. 1131) طبقه‌بندی‌ها به ترتیب، پیش‌بینی و نتیجه از دست دادن کنترل بر اطلاعات شخصی را نشان می‌دهد.[3]

در اصطلاح اقتصادی، خسارت ذهنی کم‌اهمیت‌تر از خسارات عینی نیست؛ باوجوداین، خسارت عینی غالباً می‌تواند در قالب مسئولیت مدنی توصیف گردد؛ درحالی‌که خسارات ذهنی عموماً توسط دادگاه‌های ایالات‌متحده به‌عنوان خسارت واقعی[4] شناخته نمی‌شوند. علاوه بر این، خسارات ذهنی، غالباً منجر به هزینه‌های مورد انتظار[5] می‌شوند؛[1] لذا می‌توان گفت اطلاعات

۱- «حالت تهدید و تهاجم» (assault) یکی از انواع شبه جرم‌های علیه اشخاص و از مصادیق تعدی به شخص و هم یکی از جرائم علیه اشخاص محسوب می‌گردد. هنگامی‌که عمل ترس آفرین به‌قصد ترساندن باشد و فرد هم بترسد، به‌عنوان «حالت تهدید و تهاجم مجرمانه» شناخته می‌شود؛ ولی چنانچه فقط قصد فعل وجود داشته باشد (نه قصد ترساندن) و منجر به ورود زیان گردد، آنگاه در شمار خطاهای مدنی است و از آن به‌عنوان «حالت تهدید و تهاجم خطایی» یاد می‌شود. از منظر حقوق جزا، بروز ترس ناگهانی برای تحقق جرم «حالت تهدید و تهاجم» کافی دانسته شده؛ لکن از منظر حقوق شبه جرم‌ها، مطالبه جبران خسارت ناشی از «حالت تهدید و تهاجم»، مستلزم ورود زیان است؛ بنابراین، ترس صرفی که زیانی را به بار نیاورد، قابلیت طرح دعوا نیز ندارد. (Vesali Naseh & Parsapour, 2016, p. 158)

2- battery

۳- یکی از مزیت‌های رویکرد مذکور این است که در این دسته‌بندی ضرر حریم خصوصی از نقض حریم خصوصی جدا می‌شود با نشان دادن اینکه هیچ شخصی برای اینکه ضرر حریم خصوصی محقق شود، نیاز به اثبات نقض حریم خصوصی ندارد و برعکس. برای دیدن سایر مزیت‌های این رویکرد رجوع شود به (Calo, 2011, pp. 1131-1132)

4- actual damage

۵- هزینه‌های مورد انتظار expected costs به معنای هزینه‌های آتی و احتمالی که در مقابل خساراتی است که به وقوع پیوسته‌اند.

آشکارشده در طول یک تراکنش، ممکن است در آینده درزمانی غیرمنتظره و یا به اشکال جدیدی و یا با محتوای متفاوتی دوباره ظاهر شود. طیفی از خسارات از آزار و اذیت‌های کوچک گرفته تا خسارات شدید، ممکن است اتفاق بیفتد.(Acquisti, 2010, p. 26)

هزینه‌های بی‌واسطه (مستقیم)، باواسطه (غیرمستقیم) و احتمالی

یک تقسیم دیگر از هزینه‌های داده افشاشده برای موضوعات داده، تقسیم هزینه‌ها به هزینه‌های بی‌واسطه(مستقیم)، باواسطه (غیرمستقیم) و احتمالی است که مثال‌های آن به شرح ذیل است:

هزینه‌های بی‌واسطه (مستقیم)

هزینه‌های بی‌واسطه به دو نوع غیر مشهود و مشهود قابل‌تقسیم است: برخی از هزینه‌های بی‌واسطه، غیر مشهود[۲] هستند؛ برای مثال، ناخوشنودی روانی همراه با احساس تحت نظر بودن و یا مورد تجاوز قرار گرفتن؛ خجالت و یا رسوایی اجتماعی به سبب افشای داده؛ ترس از تعرض به حیطه شخصی. برخی دیگر از هزینه‌های بی‌واسطه، مشهود[۳] هستند؛ برای مثال، زمان و انرژی صرف شده برای حذف ایمیل‌های ناشناس؛ آزار و اذیت‌های ناشی از بازاریابی تلفنی؛ پرداخت قیمت‌های بالاتر به سبب تبعیض قیمتی.(Ibid, 2010, p. 26)

هزینه‌های باواسطه (غیرمستقیم)

برخی هزینه‌ها بیشتر جنبه غیرمستقیم دارند؛ برای مثال، خوشه‌بندی[۴] و پروفایل بندی[۵] به‌ویژه به

۱- یک روش قابل‌فهم برای توصیف مشخص نبودن هزینه‌های حریم خصوصی، تشبیه به چک سفید امضا است. یک فرد با افشای اطلاعات شخصی خود، به‌نوعی در حال امضای یک چک سفید امضا است که ممکن است هیچ‌گاه به وی برنگردد و یا با مبلغی بسیار ناچیز و یا بسیار زیاد برای پرداخت به وی برگردد. در اینجا آن قیمت می‌تواند یک بین رفتن خفیف آبرو، یک نامه الکترونیکی ناخواسته و یا یک سرقت هویت ویران‌کننده باشد. به‌اختصار، احتمال، شکل و خسارت واقعی ناشی از داده افشاشده، مبهم است.(See Knight, 1921)

2- intangible
3- tangible
4- segmentation
5- profiling

شکل هدف‌گذاری رفتاری و تبلیغاتی، ممکن است منجر به هدایت مصرف‌کننده به‌سوی خدماتی شود که متمایل به آن‌ها نیست و یا استطاعت مالی آن را ندارد. همچنین وجود بازار ثانویه برای داده مشتری می‌تواند مبدل به منبع اثرات منفی برای مصرف‌کنندگان شود. این پیامدها ممکن است زمانی به وجود آید که شرکت نگه‌دارنده داده حداکثر سود را با استفاده از اطلاعات در تلاش‌های بازاریابی خودش کسب کند یا حداکثر قیمت را درازای فروش به اشخاص ثالث تحصیل کند، لکن خساراتی را که ممکن است برای مصرف‌کننده به سبب افشای اطلاعات خصوصی ایجاد شود را درونی نسازد. ازآنجایی‌که مشتریان غالباً به منابع افشای داده و یا طرقی که داده‌شان تجمیع یا استفاده می‌شود آگاهی ندارند، ممکن است نتوانند به‌طور کارآمد شرکت‌هایی را که از داده سوءاستفاده می‌کنند را مجازات نمایند.(Acquisti, 2010, p. 29)

درنهایت، یک شکل غیر مشهودتر از خسارات غیرمستقیم، از این امر نشأت می‌گیرد که هر چه بیشتر داده فردی با سایر اشخاص به اشتراک گذاشته شود، اشخاص مذکور، مزیت چانه‌زنی بیشتری در معاملات آتی با آن فرد به دست خواهند آورد؛ برای مثال، درحالی‌که مصرف‌کننده برای محصولاتی که علاقه‌مند است، پیشنهاد دریافت می‌کند، دارندگان داده در طول زمان و در تمامی تراکنش‌ها، اطلاعات وی را جمع‌آوری کرده و گزارش مفصلی از تمایلات و علایق مصرف‌کننده و پیش‌بینی رفتار آتی وی فراهم می‌کنند. باوجود مشتریان ساده باور، اطلاعات مذکور (افشای داده شخصی) بر تخصیص مازاد از تراکنش‌های آتی، یعنی بر تعادل قدرت بین موضوع داده و نگه‌دارنده داده، تأثیر خواهد گذاشت.(Acquisti, 2010, p. 29)

هزینه‌های احتمالی

سایر هزینه‌ها صرفاً احتمالی هستند؛ برای مثال، خطاهای در پایگاه‌های داده مصرف‌کننده به سبب رویه نامطلوب مدیریت داده توسط شرکت‌ها ممکن است در آینده موجب شود درخواست مصرف‌کننده به‌اشتباه رد شود و یا پایگاه‌های داده نقض شده[1] ممکن است در آینده منجر به

۱- نقض پایگاه داده، درواقع تهاجم‌هایی است که به پایگاه داده صورت می‌گیرد. ازجمله دلایل این تهاجمات، افزودن دسترسی به داده‌های ذخیره‌شده در پایگاه داده و درنتیجه افزایش فرصت سرقت داده، انگیزه تحصیل پول با فروش داده‌های

سرقت هویت شود.(Camp, 2007)

به جهت ماهیت نامشخص هزینه‌های حریم خصوصی، ارزیابی آن‌ها دشوار هست؛ اما به‌هیچ‌وجه غیرواقعی نیستند. چنین هزینه‌هایی عموماً به شکل رویدادهای بسیار محتمل با تأثیر فردی قابل‌اغماض و جزئی (برای مثال، نامه‌های الکترونیکی ناخواسته) و یا به‌عنوان رویدادهای بسیار مهم با احتمال وقوع بسیار کم (برای مثال، انکار یک وام رهنی پس از سرقت هویت) هستند. در هر دو مورد، به جهت احتمال پایین وقوع و یا تأثیر محدود آن‌ها، ممکن است در سطح فردی بی‌اهمیت تلقی شوند؛ حتی اگر در تجمیع، به خسارت اجتماعی قابل‌توجهی برسند.(Acquisti, 2010, p. 27)

سرقت هویت به سبب نقض‌های داده، نشانگر مسئله پیچیدگی ارزیابی و جبران خسارت هزینه‌های حریم خصوصی است؛ بااین‌حال، نقض‌های داده،[1] می‌تواند نتایج بسیار متنوعی برای موضوعات داده داشته باشد. هنگامی‌که نقض حقیقتاً دربردارنده تلف داده است (برای مثال، یک لپ تاب جابه‌جاشده)، موضوع داده ممکن است متحمل هیچ خسارتی نشود. هنگامی‌که نقض ناشی از حمله عمدی به‌وسیله یک شخص ثالث همراه با سوءنیت است، احتمال بیشتری وجود دارد که داده شخصی در راه‌هایی استفاده شود که مستقیماً بر موضوع تأثیر می‌گذارد؛ دعاوی برای مثال، دعاوی فریبکارانه بیکار بودن؛[2] وام‌ها، هزینه‌های کارت اعتباری؛[3] هزینه‌های بیمه سلامت.

حساس (شماره کارت‌های اعتباری، شماره امنیت اجتماعی و غیره) است. تهدید نسبت به پایگاه داده از منابع خارج از سازمان، (مثل هکرها، گروه‌های کیفری سازمان‌یافته و نهادهای دولتی به همان اندازه رویدادهای محیطی) منابع داخل سازمان، (مثل نیروهای انسانی، مدیران شرکت، کارمندان و کارآموزان) و اشخاص ثالثی که با سازمان رابطه تجاری دارند (فروشندگان، تأمین‌کنندگان، پیمانکاران و مشتریان)، ناشی می‌شود. تهدید امنیت پایگاه داده، می‌تواند باعث از دست دادن یا تنزل یکپارچگی، قابلیت دسترسی و اعتماد گردد. (N. A. Al-Sayid & D. Aldlaeen, 2013, p. 60)

۱- اصطلاح نقض حریم داده یا data breach دربرگیرنده حالت‌های مختلفی است که یا عمدی (مثل‌اینکه شخصی به‌قصد دسترسی به این داده‌ها، هدف حمله قرار گیرد) یا غیرعمدی (مثل ارسال اشتباه ایمیلی حاوی این داده‌ها، به شخصی که نباید گیرنده آن می‌بود) است. (Price, 2017, p. 94)

2- fraudulent unemployment claims
3- credit card charges

همچنین نمره اعتباری بزه دیدگان ممکن است خراب شود[۱] یا ممکن است آنها در دسترسی یا استفاده از کارت اعتباری ناتوان شده و یا حتی ممکن است علاوه بر خسارت مالی، هزینه های روانی و خسارات زمانی، متحمل هزینه‌های کیفری نیز شوند؛ باوجوداین، هم‌اکنون، صرفاً کسری از آن خسارات به‌وسیله مصرف کنندگان قابل دریافت و جبران هستند؛ برای مثال، هزینه‌های کلاهبردارانه بر روی کارت اعتباری فرد جبران خواهند شد؛ لکن به‌طورکلی، دادگاه ایالات‌متحده، به خسارات ناشی از نقض‌های اطلاعات شخصی، به سبب عجز خواهان در اثبات خسارات واقعی[۲] (آن‌گونه که توسط دعاوی مربوط به خطای تقصیر[۳] لازم است)(Romanosky & Acquisti, 2009) و همچنین عجز از اثبات یک رابطه سببیت بین نقض و خسارت وارده، حکم نداده است.

در نبود مسئولیت‌های حقوقی، التزامات قراردادی یا خطر واکنش‌های نامطلوب بازار،[۴] طرف‌هایی که عهده‌دار کنترل اطلاعات فرد می‌شوند ممکن است این قبیل خسارات وارد بر حریم خصوصی را درونی نکنند؛(Swire et al., 1998) ازاین‌رو با انگیزه‌های کمتری نسبت به حفاظت داده مصرف‌کننده روبرو شوند. این امر احتمال کژمنشی[۵] نگه‌دارنده داده را افزایش می‌دهد.

هزینه‌های داده افشاشده برای اشخاص ثالث

پیامدهای جانبی اطلاعات بر اشخاص ثالث، می‌تواند به‌صورت پیامدهای منفی نیز بروز نماید. شخصی که توجه کافی به حریم خصوصی ندارد، نه‌تنها اطلاعات زیادی در مورد خودش را افشا می‌سازد؛ بلکه اطلاعات دیگران را نیز در معرض افشا قرار می‌دهد.(Fairfield & Engel, 2015, p. 385) حتی تصمیمات بهینه شخصی توسط عاملان اقتصادی کاملاً آگاه، ممکن است نتایج

۱- اشتباهات زیادی ازجمله پرداخت با تأخیر وام یا اعتبار، پرداخت با تأخیر اجاره، تحصیل کارت اعتباری در اوایل زندگی، بستن حساب کارت اعتباری، درخواست کارت اعتباری جدید، قرض پول صرفاً برای بالا بردن نمره اعتباری و سایر موارد ممکن است سبب خراب شدن نمره اعتباری اشخاص شود. رجوع شود به (" 10 Mistakes That Will Ruin Your Credit Score," 2018)

2- actual damages
3- negligence tort claims
4- adverse market reactions
5- moral hazard

مطلوبی ازلحاظ اجتماعی و برای سایر افراد جامعه در برنداشته باشد.(Choi et al., 2018, p. 2) درواقع یکی از پیامدهای منفی و مهم اطلاعات، نقض حریم خصوصی اشخاص ثالث است. همان‌طور که بیان شد، حتی اگر افراد به افشای اطلاعات شخصی خود اقدام نکنند، ممکن است با اقدام و افشای دیگران، کنترل بر اطلاعات شخصی خود، را از دست بدهند و درنتیجه حریم خصوصی آن‌ها مورد تجاوز قرار گیرد؛ (Choi et al., 2018, p. 8) ازاین‌رو، رویکرد کنونی حمایت از حریم خصوصی در ایالات‌متحده آمریکا که مبتنی بر اطلاع و رضایت است، پاسخگوی مسئله تعدی به حریم خصوصی نیست؛ چراکه رویکرد مذکور بر اساس این فرض است که هر شخص باید بر افشا و انتشار اطلاعات شخصی خویش کنترل داشته باشد؛ (Choi et al., 2018, p. 4) ولی با توجه به پیامدهای جانبی اطلاعات می‌توان گفت حریم خصوصی کالایی عمومی[۱] است(Fairfield & Engel, 2015, p. 1) و انتخاب جمعی برای به اشتراک‌گذاری موردنیاز است. (Choi et al., 2018, p. 4)

ب) منافع و هزینه‌های داده حفاظت‌شده

در این قسمت به بررسی منافع و هزینه‌های داده حفاظت‌شده برای دارندگان داده و موضوعات داده می‌پردازیم.

منافع داده حفاظت‌شده

منافع داده حفاظت‌شده برای دارندگان داده به شرح ذیل است:

منافع داده حفاظت‌شده برای دارندگان داده

این مسئله که آیا شرکت‌ها می‌توانند از حریم خصوصی به نفع مصرف‌کننده، سود رقابتی به

۱- یکی از دلایل مخالفان مال‌انگاری داده شخصی این است که مال‌انگاری اطلاعات، اهمیت ارزش‌های اجتماعی مهمی را که حریم خصوصی اطلاعات باید آن‌ها را ارتقا دهد، نادیده می‌گیرد. از این منظر، حریم خصوصی اطلاعات، همانند نوعی کالای عمومی مشابه هوای تازه یا پدافند ملی، عمل می‌کند.(Schwartz, 2004, p. 2084)

دست بیاورند، کماکان جای بحث دارد. اگرچه شرکتی که خود، جمع‌آوری و استعمال داده مصرف‌کننده را محدود می‌کند، ممکن است منافعی را از دست بدهد، اما ممکن است از محدود کردن مسئولیت‌ها و هزینه‌های داده سوءاستفاده شده و همین‌طور از جذب مصرف‌کنندگانی که به حریم خصوصی بها می‌دهند، سود ببرد. تحت شرایط خاصی، مصرف‌کنندگان سعی در خرید از بازرگانان با حفاظت حریم خصوصی بیشتر دارند؛ حتی اگر این امر مستلزم پرداخت مبلغی اضافه باشد.(Tsai et al., 2011)

همچنین ارائه خدماتی به مصرف‌کنندگان در جهت حفاظت از حریم خصوصی بیشتر، ممکن است موجب صرفه‌جویی در هزینه‌های بازرگانان شود. این صرفه‌جویی‌ها به‌گونه‌ای است که مستقیماً مربوط به حفاظت از حریم خصوصی که آن‌ها فراهم می‌کنند و یا بواسطه برخی از انواع صرفه اقتصادی ناشی از وسعت یا محدوده،[1] نیست.[2]

منافع داده حفاظت‌شده برای موضوعات داده

در مقابل، هنگامی‌که داده مصرف‌کننده حفاظت شود، برخی هزینه‌های داده افشاشده، تبدیل به منافع خواهد شد؛ برای مثال، زمانی که شرکت‌ها داده مصرف‌کننده را به‌صورت رمزگذاری نگه‌داری می‌کنند، آن‌ها این احتمال را کاهش می‌دهند که حتی اگر داده نقض شود، مصرف‌کننده از سرقت هویت صدمه ببیند. همچنین، مصرف‌کنندگان می‌توانند از عدم آگاهی بازرگان نسبت به برخی اطلاعات شخصی منتفع شوند.

بسیاری از منافع افشای داده، زمانی که داده حفاظت شود، نیز به دست می‌آید. محدودیت‌های

۱- صرفه اقتصادی ناشی از وسعت یا محدوده economies of scope که گاهی economies of vertica نامیده می‌شود، به این معناست که اگر به‌جای اینکه یک شرکت دو محصول تولید کند، دو شرکت هریک یک محصول تولید کنند، هزینه تولید کمتر می‌شود. (Mydland, 2019, p. 3)

۲- برای مثال، برخی سیستم‌های پرداخت ناشناس ممکن است ابزارهای تصدیق داشته باشد که ریسک کلاه‌برداری و یا عودت وجه را در مقایسه با پرداخت‌های کارت اعتباری آنلاین کاهش دهد و یا سرمایه‌گذاری‌های صورت گرفته برای حفاظت داده مصرف‌کننده نظیر دیوارهای ایمنی و یا رمزگذاری سرور داده، ممکن است از اسرار تجاری و سیستم‌های اطلاعات یک شرکت نیز حفاظت نماید. (Acquisti, 2010, pp. 24-25)

مربوط به افزایش حریم خصوصی در گزارش اعتباری[1] که با قانون گزارش دهی اعتباری منصفانه[2] ایجاد شده است، مانع غیرقابل رسوخی در برابر استفاده‌های پرمنفعت از داده مصرف‌کننده که منتقدان قانون قبل از وضع آن ازاین‌جهت ابراز نگرانی داشتند، نیست. اثرات کاهش رفاه مقرره حریم خصوصی ممکن است به‌طور مشابهی در سایر بخش‌ها مورد مبالغه قرار گرفته باشد؛ چراکه بازارها طرق وفق پیدا کردن با محدودیت‌های جدید را خواهند یافت.(Gellman, 2002)

به‌طور مشابه، اگرچه وضع مقررات حریم خصوصی که هدف‌گذاری رفتاری را محدود می‌نماید، اثر تبلیغات بر روی سایت‌های با محتوای عمومی را کاهش داده است؛ اما اثری بر تبلیغات بر روی سایت‌هایی با محتوای خاص، تبلیغات گسترده‌تر و یا با خصیصه تعاملی، ویدئو و یا صوتی نداشته است.

علاوه بر این، درصورتی‌که هدف‌گذاری رفتاری، هزینه‌های یافتن محصولات توسط مصرف‌کننده را کاهش می‌دهد و مصرف‌کنندگان می‌توانند تمایلات خود را تطبیق دهند، فنّاوری‌های کمتر مداخله‌گر نیز می‌توانند این کار را انجام دهند. فنّاوری‌های افزایش حریم خصوصی ممکن است برای حفاظت داده حساس مورداستفاده قرار گیرند؛ باوجوداین، فنّاوری‌های مذکور، با لحاظ منافع هم موضوعات داده و هم نگه‌دارندگان داده، جمع‌آوری، تجزیه‌وتحلیل و بهره‌برداری سودمند از داده غیر حساس، غیرقابل‌شناسایی و یا داده تجمیع شده را ممکن و مجاز می‌نماید.(Acquisti, 2008)

هزینه‌های داده حفاظت‌شده

هزینه‌های داده حفاظت‌شده برای دارندگان داده و موضوعات داده به شرح ذیل است:

هزینه‌های داده حفاظت‌شده و فعل حفاظت داده برای دارندگان داده

1- credit reporting

۲- قانون گزارش دهی اعتباری منصفانه Fair Credit Reporting Act مصوب ۱۹۷۰، اولین قانون فدرال در ایالات‌متحده آمریکا، مربوط به حریم خصوصی مالی در بخش خصوصی است و دربردارنده قواعدی در خصوص نحوه افشای اطلاعات شخصی افراد در قالب گزارش‌های اعتباری این مؤسسات است.(Solove & Schwartz, 2015, pp. 242-244)

هزینه‌های داده حفاظت‌شده برای دارندگان داده یا ناشی از خود داده حفاظت‌شده و یا صرف فعل حفاظت است.

هزینه‌های داده حفاظت‌شده

در صورت فقدان افشا، در مقابل منافع، هزینه‌های فرصت و ناکارایی ممکن است به وجود آیند؛ برای مثال، شرکت‌هایی که به داده مصرف‌کننده دسترسی ندارند، ممکن است با موانع شدیدی برای ورود و شرایط نامساعد رقابتی در برابر شرکت‌هایی با پایگاه‌های مشتری بزرگ‌تر مواجه شوند که درنتیجه این امر، رقابت محدود می‌شود. همچنین هنگامی‌که شرکت‌ها داده ارزشمند را تلف کنند، سیاست‌های رضایت صریح[1] اجباری حریم خصوصی برای برخی انواع داده ممکن است برای شرکت‌ها پرهزینه باشد.(Staten & Cate, 2002) علاوه بر این، فقدان داده مصرف‌کننده ممکن است خلاقیت و خدمات جدید برای شرکت‌ها را دشوار کند. بنا به همان دلیل، ترس از جبران خسارت‌های حقوقی محتمل در پی جمع‌آوری و یا پردازش داده، ممکن است منجر به بازداشتن نوآوری محصولات شود. به همین نحو، هزینه‌های داده افشا نشده در سطح کلان ممکن است بر جامعه نیز تحمیل شود.[2]

۱- قاعده «حق خروج» یا به تعبیری «رضایت مفروض» به این معناست که مصرف‌کنندگان گزینه خروج از به اشتراک‌گذاری اطلاعات شخصی با اشخاص ثالث دارند؛ به عبارتی اگر مصرف‌کننده اقدامی نکند، فرض بر آن است که با به اشتراک‌گذاری اطلاعات شخصی خود با طرفین ثالث، رضایت داده است. قاعده حق خروج در تضاد محرز با قاعده «رضایت صریح» است. طبق قاعده «رضایت صریح»، می‌بایست رضایت صریح مصرف‌کننده قبل از به اشتراک‌گذاری اطلاعات شخصی تحصیل گردد؛ برای مثال، طبق قاعده حق خروج مندرج در قانون گرام لیچ بلیلی (قانون نوسازی خدمات مالی ۱۹۹۹) ایالات‌متحده آمریکا، مشتریان قادر به ممانعت با به اشتراک‌گذاری داده شخصی با اشخاص ثالث غیر وابسته هستند. رجوع شود به 15 U.S.C. § 6802(b)(1) (2006)

۲- برای مثال در سال ۲۰۱۰، وزارت صنعت کانادا، اعلام نمود که پر کردن فرم پرسش‌نامه طویل سرشماری دیگر الزامی نیست. این ابتکار با موضع دولت مبنی بر این‌که کانادایی‌ها نمی‌بایست ملزم به افشای اطلاعات شخصی خود تحت تهدید جریمه، زندان و یا هر دو شوند، برانگیخته شد؛ باوجوداین، گذار از اجباری به داوطلبانه، احتمالاً می‌تواند منجر به کاهش شدید پاسخ‌دهندگان به فرم طویل پرسش‌نامه گردد. این افزایش خطر تمایل به عدم پاسخ‌گویی، می‌تواند بر کار سیاست‌گذاران، محققین و یا ارائه‌دهندگان خدمات بهداشتی اثر منفی گذارد. (See Raso, 2016)

هزینه‌های فعل حفاظت داده

حفاظت داده مصرف‌کننده می‌تواند برای شرکت‌ها از دو جهت هزینه‌بردار باشد: اولاً، ممکن است از جمع‌آوری، استخراج و پردازش داده سودمند احتمالی به‌منظور جلوگیری از هزینه‌های آتی حریم خصوصی صرف‌نظر کنند که در اصطلاح اقتصادی، موجب هزینه‌های فرصت می‌شود؛ ثانیاً، در پی تلاش برای جلوگیری از ضررهای مورد انتظار آتی[1] به علت حفاظت از حریم خصوصی، شرکت‌ها ممکن است متحمل هزینه‌های کمتر اما مطمئناً فعلی[2] شوند. شرکت‌ها ممکن است بیش‌ازحد در امنیت داده سرمایه‌گذاری کنند.[3]

هزینه‌های اضافی دیگر دربردارنده خسارات اجتماعی به علت سیاست‌های حریم خصوصی نامنسجم هست: در میان یک سری ابتکارات قانون‌گذاری و خودتنظیمی پیچیده، هم مصرف‌کنندگان و هم شرکت‌ها راجع به سطح حفاظت ایجادشده و یا لازم برای انواع متعدد داده شخصی نامطمئن هستند. این عدم اطمینان به‌نوبه خود پرهزینه است؛ چراکه موجب ملزم کردن موضوعات داده و دارندگان داده به سرمایه‌گذاری در آگاهی راجع به مقبولیت رویه داده خاصی خواهد شد. عدم اطمینان مذکور همچنین موجب ایجاد اثرات ثانوی خواهد شد؛ بدین شرح که ممکن است هم موضوعات داده و هم دارندگان داده را به سرمایه‌گذاری افراطی یا تفریطی ناکارآمد در حفاظت داده هدایت کند. (Samuelson, 2003) هزینه‌های مشابهی برای شرکت‌های اینترنتی که به‌صورت جهانی عمل می‌کنند ایجاد می‌شود که می‌بایست خدمات خویش را با استانداردهای حفاظت از حریم خصوصی متفاوت محلی منطبق نمایند.

هزینه‌های داده حفاظت‌شده و فعل حفاظت داده برای موضوعات داده

هزینه‌های داده حفاظت شده برای موضوعات داده یا ناشی از داده حفاظت شده و یا صرف فعل حفاظت است.

1- ex post expected losses
2- ex ante costs
۳- شرکت‌های ایالات‌متحده در پی وضع قوانین افشا و آشکارسازی نقض داده، در حال افزایش امنیت و سرمایه‌گذاری‌های عملیاتی بوده‌اند.(See Hoofnagle, 2007)

هزینه‌های داده حفاظت شده

به‌طور متقابل، زمانی که مصرف‌کننده تصمیم می‌گیرد که داده را افشا نکند، برخی منافع اجتماعی داده افشاشده، تبدیل به هزینه‌های فرصت می‌گردد. هزینه‌های فرصت در سطح اجتماعی، با جلوگیری داده از به‌کارگیری در اهداف مفید اجتماعی است.[۱] هزینه‌های فرصت داده افشا نشده، در سطح فردی بااهمیت‌تر است؛ چراکه محصولات و خدمات مصرف‌کننده بیشتری مشروط و یا مبتنی بر این فرض هستند که داده افشا شود؛ برای مثال، افرادی که به دلیل نگرانی‌های حریم خصوصی تصمیم به عدم عضویت در شبکه اجتماعی می‌گیرند، اطلاعاتی را که بر روی وب‌سایتی که برای مثال تنها می‌تواند از طریق یک تصدیق ارتباط فیس‌بوکی مورد جست‌وجو قرار گیرد را از دست می‌دهند. هر چه بیشتر سایر مصرف‌کنندگان با افشاهای داده کنار آیند و هر چه بیشتر شرکت‌ها برای ارائه محصولات و خدمات، داده را لازم بدانند، هزینه‌های فرصت برای مصرف‌کنندگانی که می‌خواهند از داده‌شان حفاظت کنند، بیشتر خواهد شد.[۲]

مصرف‌کنندگان برای اطلاع از مخاطرات حریم خصوصی، متحمل مخاطرات شناختی و فرصت می‌شوند. با توجه به این فرض که حفاظت از حریم خصوصی مصرف‌کنندگان بستگی به آگاهی و رضایت دارد، هزینه آگاهی یافتن مصرف‌کنندگان ممکن است نجومی باشد. به همین نحو، مصرف‌کنندگان مجبور به پردازش اطلاعات به‌منظور تصمیم‌گیری و یافتن راه‌حلی در واکنش به افشای داده می‌شوند که این امر موجب تحمیل هزینه‌های شناخت بر مصرف‌کننده می‌شود.

هزینه‌های فعل حفاظت داده

۱- برای مثال، پرونده فرم‌های طویل داوطلبانه پرسش‌نامه سرشماری کانادا را که پیش‌ازاین موردبحث قرار گرفت.

۲- برخی از نسبت «آلودگی داده» برای اشاره به پیامدهای جانبی مرتبط با افشاهای داده استفاده کرده‌اند. فشار اجتماعی مبنی بر انتشار داده در برنامه‌های وب ۲، همچنین تحلیل تدریجی انتظارات حریم خصوصی، ممکن است اثر منفی بر ایجاد راه‌حل‌های حفاظت از حریم خصوصی در خصوص محصولات و خدمات تحت شرایط کنونی بازار داشته باشد. (Camp & Wolfram, 2004)

حفاظت از اطلاعات نیز هزینه‌بردار است؛ برای مثال، هزینه صرف شده برای ناشناس کردن خدمت و فنّاوری‌های افزایش حریم خصوصی،[۱] زمان صرف شده برای یادگیری استفاده از فنّاوری یا دشواری متحمل شده به هنگام تغییر رفتار و عادات فرد.[۲]

نتیجه و پیشنهادها

مطابق تئوری اقتصادی حریم خصوصی اندیشمندان مکتب شیکاگو، حفاظت از حریم خصوصی منشأ ناکارایی اقتصادی است. علل ناکارایی نیز مواردی چون پنهان کردن اطلاعات از سایر عاملان اقتصادی، افزایش هزینه‌های مبادله، پنهان کردن ویژگی‌های منفی، دشواری ارزیابی خطرات معامله و تشویق کلاه‌برداری، بیان شده است. همچنین بیان شده است که به اشتراک‌گذاری آزاد اطلاعات، سبب کاهش نواقص بازار، افزایش رفاه و انتفاع مصرف‌کننده از اثرات مثبت بازار ثانویه می‌شود. درنهایت اینکه حفاظت از حریم خصوصی بستگی به ارزش‌گذاری طرفین ذینفع در داده و نه حفاظت قانونی از آن دارد. در نقد تئوری مذکور می‌توان گفت با توجه به فناوری‌های کنونی، فرضیات رفتار عقلایی مکتب شیکاگو، نمی‌تواند پیچیدگی تصمیم مصرف‌کننده را مورد لحاظ قرار دهد: اولاً، در بعضی موارد مصرف‌کننده نمی‌تواند آثار آتی به اشتراک‌گذاری فعلی را پیش‌بینی نماید (برای مثال، اثرات منفی بازار ثانویه، تبعیض قیمتی، سوءاستفاده از داده برای بازاریابی ناخواسته و سایر پیامدهای جانبی منفی بر مصرف‌کننده که توسط شرکت‌ها درونی نشده است)؛ ثانیاً، مصرف‌کنندگان به هنگام انتخاب فواید کوتاه‌مدت و هزینه‌های بلندمدت افشای اطلاعات به‌درستی عمل نمی‌کنند. حریم خصوصی، اثر مثبت بر رفاه و بر تعادل کارآمد در تخصیص منابع را نیز دارد. همچنین در رد نظریه کارایی در جریان آزاد اطلاعات بایستی بیان داشت که چنین نظامی در طولانی‌مدت ناکارآمد است؛ چراکه هیچ‌وقت اطلاعات در مورد یک فرد، کامل یا دقیق نیست و اگر فرد بر اطلاعات خویش کنترل نداشته

۱- فناوری‌های افزایش حریم خصوصی مثل تور (به انگلیسی Tor) رجوع شود به (" Tor (anonymity network)," (2019

۲- برای مثال، برای جلوگیری از تعقیب و یا مورد تبعیض قیمتی واقع‌شدن، مصرف‌کنندگان ممکن است متوسل به فعالیت‌های بیهوده‌ای چون سرمایه‌گذاری در نرم‌افزار حفاظتی که ایشان در غیر این صورت نیاز نمی‌داشتند یا هزینه‌های استفاده از فناوری‌های افزایش حریم خصوصی گردند.

باشد، نمی‌داند چه حقایقی ممکن است تعیین‌کننده تصمیم طرف مقابل باشد و نمی‌تواند سوابق اشتباهی که می‌تواند منجر به رفتار اقتصادی ناکارآمد توسط تمام طرفین معامله شود را تصحیح نماید. درنهایت اینکه افراد ممکن است به علت فقر، هزینه‌های تراکنش و سایر موانع نتوانند تحت شرایط متعارف بازار، حفاظت از حریم خصوصی کسب نمایند.

در بررسی و مقایسه ارزش اقتصادی حریم خصوصی و افشای اطلاعات شخصی مشخص گردید که اطلاعات شخصی افشاشده (عدم حفاظت از حریم خصوصی) دارای منافع و هزینه‌هایی برای سه دسته اشخاص یعنی دارندگان داده، موضوعات داده و اشخاص ثالث است: اطلاعات شخصی افشاشده می‌تواند منجر به منافع اقتصادی برای دارندگان داده (برای مثال، افزایش کارایی، تبعیض قیمتی، افزایش منافع از طریق ردیابی مصرف‌کننده، بهبود خدمات یا طراحی دوباره آن با توجه به رفتار مصرف‌کننده)؛ موضوعات داده (برای مثال، تخفیف‌ها، شخصی‌سازی، فروش اطلاعات شخصی با رویکرد مال‌انگاری، پیشنهادهای هدفمند، کاهش مزاحمت بازاریابی تلفنی و افزایش اعتبار داده جمع‌آوری‌شده، تبعیض قیمتی، مزایای بازار ثانویه) و همچنین اشخاص ثالث (برای مثال، اصلاح تجربه اشخاص ثالث) شود. درعین‌حال، چنین افشاهایی ممکن است دربردارنده هزینه‌هایی برای دارندگان داده (برای مثال، هزینه‌های مربوط به جمع‌آوری داده درجایی که مصرف‌کنندگان شیوه جمع‌آوری داده را مداخله گرانه محسوب نمایند و یا هزینه‌هایی که به استفاده یا سوءاستفاده از داده مربوط می‌شود؛ برای مثال، تعدی به حریم خصوصی، هزینه مطلع نمودن مصرف‌کنندگان از نقض، فسخ رابطه با شرکت و کاهش برخی معاملات به خاطر ترس از هزینه‌های آتی حریم خصوصی و همچنین هزینه‌هایی که مربوط به فعل جمع‌آوری داده است؛ برای مثال، سرمایه‌های لازم جهت ساخت سیستم‌های مدیریت ارتباط با مشتری)؛ موضوعات داده (برای مثال، هزینه‌های روانی ازجمله احساس ناخوشایند تحت نظر بودن، ترس از تعرض، خجالت به سبب افشای داده، سرقت هویت، تبعیض قیمتی، تغییر تعادل قدرت بین موضوع داده و دارنده داده؛ هزینه‌های زمانی ازجمله صرف وقت برای حذف ایمیل‌های ناخواسته و حتی هزینه‌های کیفری) و اشخاص ثالث (برای مثال، افشای اطلاعات اشخاص ثالث و نقض حریم خصوصی آن‌ها) باشد. به‌طور مشابه، اطلاعات شخصی حفاظت‌شده (حفاظت از حریم خصوصی)، دارای منافع و هزینه‌هایی برای موضوعات و دارندگان داده است که غالباً معکوس منافع و هزینه‌های داده افشاشده است: حفاظت از حریم خصوصی می‌تواند منجر به منافع اقتصادی برای

دارندگان داده (برای مثال، محدود کردن مسئولیت، مزیت رقابتی از طریق جذب مصرف‌کنندگانی که به حریم خصوصی بها می‌دهند) و موضوعات داده (برای مثال، کاهش هزینه‌های قابل پیش‌بینی سرقت هویت آینده مصرف‌کنندگان و انتفاع از عدم آگاهی فروشنده از برخی اطلاعات) شود. همچنین حفاظت از حریم خصوصی، ممکن است دربردارنده هزینه‌هایی برای دارندگان داده (برای مثال، هزینه‌های فرصت ازجمله از دست دادن فرصت‌های افزایش بهره‌وری و همچنین هزینه عمل حفاظت داده ازجمله سرمایه‌های لازم برای رمزگذاری داده) و موضوعات داده (برای مثال، هزینه‌های شناخت مربوط به مطلع شدن از نقض و پاسخ به افشای نقض، هزینه‌های فرصت به جهت عدم استفاده از داده در اهداف مفید فردی و اجتماعی و همچنین هزینه عمل حفاظت داده ازجمله هزینه‌های استفاده از فناوری‌های افزایش حریم خصوصی) باشد.

درنهایت، با توجه به فواید و هزینه‌های حفاظت از حریم خصوصی و به اشتراک‌گذاری داده شخصی که در موقعیت‌ها، شرایط و فروض مختلف متفاوت می‌شود و همچنین با توجه به این موضوع که معنا و گستره حریم خصوصی، بده بستان‌های مربوط به آن و ارزش‌گذاری‌های مصرف‌کنندگان از داده شخصی بسیار متنوع است، این نتیجه حاصل می‌شود که مقایسه ارزش کلی حفاظت از حریم خصوصی در قبال داده شخصی و برآورد اقتصادی نهایی و قطعی در مورد اینکه نیاز به حفاظت بیشتر یا کمتری از حریم خصوصی است، دشوار است. علاوه بر این بررسی نظریه‌های اقتصادی در این زمینه نیز نشان می‌دهد که حفاظت از حریم خصوصی می‌تواند رفاه کل را افزایش دهد به همان اندازه که توقف جریانات داده می‌تواند آن را کاهش دهد.

بااین‌حال، به نظر می‌رسد حل مسئله حریم خصوصی، به معنای یافتن تعادلی میان به اشتراک‌گذاری اطلاعات و مخفی کردن اطلاعات در جهت منافع موضوعات داده و همچنین جامعه به‌طور کل خواهد بود و ارزیابی حریم خصوصی از منظر اقتصادی می‌تواند در یافتن این تعادل به ما کمک کند که بررسی این مسئله خارج از موضوع تحقیق حاضر است و نیاز به تحقیق دیگری در این زمینه دارد.

References

[1] Acquisti, Alessandro. (2008). Identity Management, Privacy, and Price Discrimination. *IEEE Security & Privacy*, *6*(2).
[2] Acquisti, Alessandro. (2010). The economics of Personal Data and the

Economics of Privacy, 51.
[3] Acquisti, Alessandro; Taylor, Curtis; & Wagman, Liad. (2016). The Economics of Privacy. *Journal of Economic Literature*, *54*(2), 442-92.
[4] Acquisti, Alessandro; & Varian, Hal R. (2005). Conditioning Prices on Purchase History. *Marketing Science*, *24*(3), 367-381.
[5] Aghababaii, Hossein. (2017). *Privacy in The Islamic Criminal Law*. Tehran: Islamic Research Institute for Culture and Thought. (in Persian)
[6] Akerlof, George A. (1978). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. In *Uncertainty in Economics* (pp. 235-251). Elsevier.
[7] Allen, Anita L. (1999). Privacy-as-Data Control: Conceptual, Practical, and Moral limits of the Paradigm. *Conn. L. Rev.*, *32*, 861.
[8] Ansari, Bagher. (2013). *Privacy Law*. Tehran: The Organization for Researching and Composing University Textbooks in the Humanities (Samt). (in Persian)
[9] Ansari, Bagher. (2017). *Mass Communication Law*. Tehran: The Organization for Researching and Composing University Textbooks in the Humanities (Samt). (in Persian)
[10] Arrow, Kenneth J. (1962). The Economic Implications of Learning by Doing. *The Review of Economic Studies*, *29*(3), 155-173.
[11] Asadollahi, Simindokht. (2016). Analysis of Program Laws Legislation in Consumer Rights Protection. In *Economic Law in Public Policy-Making* (pp. 37-61). Tehran: Mizan. (in Persian)
[12] Badini, Hsan. (2004). The Philosophical Foundations of the Economic Attitude to Law. *Journal of Faculty of Law and Political Science*, *62*(0), 91-135. (in Persian)
[13] Bergelson, Vera. (2003). It's Personal but Is It Mine? Toward Property Rights in Personal Information. *UC Davis Law Review*, *37*(379).
[14] Calo, Ryan. (2011). The Boundaries of Privacy Harm. *Ind. LJ*, *86*, 1131.
[15] Calzolari, Giacomo; & Pavan, Alessandro. (2006). On the Optimality of Privacy in Sequential Contracting. *Journal of Economic Theory*, *130*(1), 168-204.
[16] Camp, L Jean. (2007). *Economics of Identity Theft: Avoidance, Causes and Possible Cures*. Springer Science & Business Media.
[17] Camp, L Jean; & Wolfram, Catherine. (2004). Pricing Security. In *Economics of Information Security* (pp. 17-34). Springer.
[18] Choi, Jay Pil; Jeon, Doh-Shin; & Kim, Byung-Cheol. (2018). Privacy and Personal Data Collection with Information Externalities.
[19] Click path. (2019, March 22). In *Wikipedia*.
[20] Cooter, Robert; & Ulen, Thomas. (2010). *Law and Economics*. (Y. Dadgar & H. Akhavan, trans.). Tehran: Tarbiat Modares University Press.
[21] Deighton, John A; & Blattberg, Robert C. (1991). Interactive Marketing: Exploiting the Age of Addressability. *Sloan Management Review*, *33*(1), 5-14.

[22] Dixon, Huw. (2001). Surfing economics.
[23] Fairfield, Joshua AT; & Engel, Christoph. (2015). Privacy as a Public Good. *Duke LJ*, *65*, 385.
[24] Gellman, Robert. (2002). Privacy, Consumers, and Costs-How the Lack of Privacy Costs Consumers and why Business Studies of Privacy Costs Are Biased and Incomplete. Presented at the Digital Media Forum, Ford Foundation.
[25] Ghasemi Hamed, Abbas. (2012). Harm the Consumer in Competitive market. *Legal Research*, *15*(148), 97-124. (in Persian)
[26] Goldfarb, Avi; & Tucker, Catherine E. (2011). Privacy Regulation and Online Advertising. *Management Science*, *57*(1), 57-71.
[27] Grossman, Sanford J. (1981). The Informational Role of Warranties and Private Disclosure about Product Quality. *The Journal of Law and Economics*, *24*(3), 461-483.
[28] Hann, Il-Horn; Hui, Kai Lung; Lee, TSY; & Png, IPL. (2003). Direct Marketing: Privacy and Competition. Presented at the Workshop on Information Systems and Economics (WISE), Seattle, Washington, USA.
[29] Hayek, F. A. (2010). The Use of Knowledge in Society. (M. Ranjbar & M. kazemi, trans.), *World Economy Newspaper*.
[30] Hermalin, Benjamin E; & Katz, Michael L. (2006). Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy. *Quantitative Marketing and Economics*, *4*(3), 209-239.
[31] Hirshleifer, Jack. (1980). Privacy: Its Origin, Function, and Future. *The Journal of Legal Studies*, *9*(4), 649-664.
[32] Hoofnagle, C. (2007). Security Breach Notification Laws: Views from Chief Security Officers.
[33] Hoseyni, Seyedeh Fatemeh; & Safari Gerayli, Mehdi. (2018). Internet Disclosure of Financial Information and Firm Value: An Empirical Test of Signaling Theory. *Journal Management System*, *7*, 1-9. (in Persian)
[34] Jalali, Omolbanin; & Nasrollahi, Zahra. (2019). Influence of Social Capital on the Incentive Reversal: Behavioral Economics Approach Based on Game Theory. *Quarterly Journal of Economic Growth and Development Research*, *9*, 131-146. (in Persian)
[35] Jentzsch, N. (2007). *Financial Privacy: An International Comparison of Credit Reporting Systems*. Springer Berlin Heidelberg.
[36] Knight, Frank H. (1921). Risk, Uncertainty and Proift. *New York: Hart, Schaffner and Marx*.
[37] Krasnikov, Alexander; Jayachandran, Satish; & Kumar, V. (2009). The Impact of Customer Relationship Management Implementation on Cost and Profit Efficiencies: Evidence from the US Commercial Banking Industry. *Journal of marketing*, *73*(6), 61-76.
[38] Liptak, Adam. (2010). When American and European Ideas of Privacy Collide. *New York Times*.
[39] Mahdavi, Ghadir; & Rajaei, Malihe. (2016). The Precautions Effect on the

Market, *31*(3), 25-44. (in Persian)
[40] Murphy, Richard S. (1995). Property rights in Personal Information: An Economic Defense of Privacy. *Geo. LJ*, *84*, 2381.
[41] Mydland, Ørjan. (2019). Lost Economies of Scope and Potential Merger Gains in the Norwegian Electricity Industry. *Empirical Economics*, 1-24.
[42] N. A. Al-Sayid; & D. Aldlaeen. (2013). Database Security Threats: A Survey Study. In *2013 5th International Conference on Computer Science and Information Technology* (pp. 60-64). https://doi.org/10.1109/CSIT.2013.6588759
[43] Naeemi, Seyyed Morteza; & Rasekh, Mohammad. (2012). Concept of "Economic Man" in Economic Approach to Law: An Explanation and a Critique. *Encyclopedia of Economic right*, *19*(2), 134-168. (in Persian)
[44] Niknia, Masoumeh. (2016). Linked Data and User Interaction: The Road Ahead. *Information & Communication Quarterly Book Review*, *3*(9), 181-192. (in Persian)
[45] Noam, Eli M. (1997a). Privacy and Self-regulation: Markets for Electronic Privacy. *Privacy and Self-Regulation in the Information Age*, 21-33.
[46] Noam, Eli M. (1997b). Privacy and Self-regulation: Markets for Electronic Privacy. *Privacy and Self-Regulation in the Information Age*, 21-33.
[47] Odlyzko, Andrew. (2003). Privacy, Economics, and Price Discrimination on the Internet (pp. 355-366). Presented at the Proceedings of the 5th international conference on Electronic commerce, ACM.
[48] Ostovar, majid. (2009). Influence of Hayek's Idea on Political Ideologies of Right and Left. *The Journal of Policy*, *38*(4), 77-97. (in Persian)
[49] Posner, Richard A. (1977). The Right of Privacy. *Ga. L. Rev.*, *12*, 393.
[50] Posner, Richard A. (1981). The Economics of Privacy. *The American Economic Review*, *71*(2), 405-409.
[51] Price, Kristen. (2017). What to Do in Data Breach; A Survey into the US Government's Recommendation to Respond to Information Flaw. (N. Moshref Javadi, tran.), *Peivast Monthly Magazine*, (48), 94-95.
[52] Raso, Jennifer. (2016). Accessible Information and Constitutional Democracy: Who Counts. *Const. F.*, *25*, 67.
[53] Reinartz, Werner. (2002). Customizing Prices in Online Markets. *Symphonya. Emerging Issues in Management*, (1), 55-65.
[54] Romanosky, Sasha; & Acquisti, Alessandro. (2009). Privacy Costs and Personal Data Protection: Economic and legal perspectives. *Berkeley Tech. LJ*, *24*, 1061.
[55] Rubin, Paul H; & Lenard, Thomas M. (2002). *Privacy and the Commercial Use of Personal Information*. Springer Science & Business Media.
[56] Safaei, Seyed Hossein; & Hasani Sangani, Vahid. (2016). Competitive Analysis of Discriminative Pricing and Intellectual Property Rights, *12*(2), 171-203. (in Persian)
[57] Safai, Sayyed Hossein. (2015). The Relationship of Law and Economics. Retrieved June 20, 2019, from http://www.ias.ac.ir/index.php/2016-04-19-10-

01-24/327-2016-04-20-08-54-23(in Persian)
[58] Salehi, mojtaba; & Khanmohammadi, Mohammad Hamed. (2018). Evaluating Economies of Scale of Country Banks With Use of Conceptual Constraints Concepts. *Financial Knowledge of Securities Analysis, 11*. (in Persian)
[59] Samuelson, Pamela. (2000). Privacy as Intellectual Property? *Stanford Law Review*, 1125-1173.
[60] Samuelson, Pamela. (2003). The Social Costs of Incoherent Privacy Policies. *Presentation at IBM Almaden Privacy Institute*.
[61] Schoeman, Ferdinand David. (1992). *Privacy and Social Freedom*. Cambridge university press.
[62] Schwartz, Paul M. (1999). Internet Privacy and the State. *Conn. L. Rev., 32*, 815.
[63] Schwartz, Paul M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review*, 2056-2128.
[64] Sharifzadeh, Mohammad Javad. (2012). *Law and Economics in Islam An Introduction to Economics Analysis of Islamic Legal Institutions(With Special Focus on the History of Early Days of Islam)*. Tehran: Imam Sadiq University Publisher. (in Persian)
[65] Sharman, Jason C. (2009). Privacy as Roguery: Personal Financial Information in an Age of Transparency. *Public Administration, 87*(4), 717-731.
[66] Shokuhyan, Seyed Alireza; & Edrisian, Mojtaba (trans.). (2017). *"Tort Law and Economics" The First Part: The Efficient Tort Rules*. Tehran: Judiciary Press and Publishing Center. (in Persian)
[67] Spence, Michael. (1978). Job Market Signaling. In *Uncertainty in Economics* (pp. 281-306). Elsevier.
[68] Staten, Michael E; & Cate, Fred H. (2002). The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Study of MBNA. *Duke LJ, 52*, 745.
[69] Stigler, George J. (1961). The Economics of Information. *Journal of Political Economy, 69*(3), 213-225.
[70] Stigler, George J. (1980). An Introduction to Privacy in Economics and Politics. *The Journal of Legal Studies, 9*(4), 623-644.
[71] Stone, Eugene F; & Stone, Dianna L. (1990). Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms. *Research in Personnel and Human Resources Management, 8*(3), 349-411.
[72] Swire, Peter P; & Litan, Robert E. (1998). *None of Your business: world data flows, electronic commerce, and the European privacy directive*. Brookings Inst Pr.
[73] Swire, Peter P; Litan, Robert E; & Litan, Robert E. (1998). *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Vol. 196). Brookings Institution Press Washington, DC.
[74] Taherkhani, Setare. (2011). An Introduction to Game Theory. *Journal of Foreign Policy, 25*(1), 219-242. (in Persian)
[75] Taylor, Curtis R. (2004). Consumer Privacy and The Market for Customer

Information. *RAND Journal of Economics*, 631-650.
[76] Tor (anonymity network). (2019, June 17). In *Wikipedia*.
[77] Tsai, Janice Y; Egelman, Serge; Cranor, Lorrie; & Acquisti, Alessandro. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254-268.
[78] Varian, Hal R. (2009). Economic Aspects of Personal Privacy. In *Internet Policy and Economics* (pp. 101-109). Springer.
[79] Vesali Naseh; & Parsapour. (2016). Liability Resulting from Fright (A Comparative Study of Imamieh Jurisprudence, Iran Law and Common Law). *Journal OF Comparative Law Research*, *20*(2), 147-169. (in Persian)
[80] Warren, Samuel D; & Brandeis, Louis D. (1890). The Right to Privacy. *Harvard Law Review*, 193-220.
[81] Westin, Alan F. (1968). Privacy and Freedom. *Washington and Lee Law Review*, *25*(1), 166.
[82] Zarei, Mohammad Hossein; & Shokuhyan, Seyed Alireza. (2016). The Role of Private Entities in Market Regulation; With a Critical Approach to the Planning Rule. In *Economic Law in Public Policy-Making*. Mizan.(in Persian)
[83] 10 Mistakes That Will Ruin Your Credit Score. (2018, June 19). Retrieved May 15, 2019, from https://smartasset.com/credit-score/10-mistakes-that-will-ruin-credit-score