رسانه و فرهنگ، پژوهشگاه علوم انسانی و مطالعات فرهنگی
سال ششم، شمارهٔ اول، بهار و تابستان ۱۳۹۵، ۱-۲۳

جرایم علیه حریم خصوصی داده‌ها در فضای سایبری ایران و آلمان

زهرا احمدی ناطور*

حسین آقابابایی**

چکیده

با ورود به عصر فنّاوری اطلاعات و ارتباطات، به‌تدریج مسائل و دشواری‌های نوینی دربارهٔ حریم خصوصی اشخاص و حقوق حمایت از داده‌ها مطرح شده است که حل و فصل آن‌ها نیازمند بازنگری در قوانین فعلی یا وضع قوانینی جدید و فراگیر است. اغلب کشورها، از جمله آلمان، قوانین حمایت از داده دارند، اما برخی کشورها، نظیر ایران، فاقد قانونی جامع و منسجم در این زمینه‌اند. هدف ما از تحقیق حاضر مقایسهٔ جرایم علیه حریم خصوصی داده‌ها در فضای سایبری ایران و آلمان است. مقایسهٔ مذکور نشان می‌دهد که حقوق ایران به‌لحاظ فقدان برخی از اصول حاکم‌بر داده‌های شخصی، کامل نبودن اصول پیش‌بینی‌شده، و ارجاع برخی اصول به آیین‌نامه‌های گوناگون نقایص جدی دارد که باید از سوی مقنن بازنگری شود. از سوی دیگر، فقدان مقررات جامع در زمینهٔ حمایت از حریم خصوصی مانع از درک و اجرای صحیح حمایت از داده‌ها در دادگاه‌ها و مراجع اداری می‌شود. «لایحهٔ حریم خصوصی»، که برای ارائه به مجلس شورای اسلامی تدوین شده، این اشکال را تا حدودی مرتفع کرده است که در صورت رفع ایرادات و تصویب آن این نقایص تا حدی رفع می‌شود.

کلیدواژه‌ها: حریم خصوصی، فضای سایبری، فنّاوری اطلاعات و ارتباطات، ایران، آلمان.

۱. مقدمه

در اواخر قرن بیستم و در عصر فراصنعتی، جهان شاهد ظهور پدیده‌های شگرف بر اثر پیش‌رفت‌های علمی و فنّاوری‌های نوین بود. پدیده‌ای که در حقیقت به‌معنای تولد جهانی

* دانشجوی دکتری حقوق جزا و جرم‌شناسی، دانشگاه تهران (نویسندهٔ مسئول)، Ahmadi.papers@gmail.com
** دانشیار گروه حقوق، دانشگاه گیلان، f.h.papers@gmail.com
تاریخ دریافت: ۱۳۹٤/۹/۵، تاریخ پذیرش: ۱۳۹۵/۱۲/۲

دیگر با اوضاع و ویژگی‌هایی متفاوت با جهان کنونی بود. این دنیای جدید فضای مجازی یا فضای سایبر (cyberspace) نام گرفت. این فضا، که شناخته‌شده‌ترین بخش آن «اینترنت» است، برای تسهیل ارتباطات طراحی شده است و امروزه نیز بر این کاربرد تکیه دارد. در این فضا هر آن‌چه رخ می‌دهد به‌وسیلهٔ داده‌ها صورت می‌گیرد و در واقع آن‌چه در این فضا مبادله می‌شود داده‌هاست (باستانی، ۱۳۸٦: ۵۵). مهم‌ترین اشکال تجاوز به حریم خصوصی در فضای سایبر با نقض قواعد پایه‌ای حمایت از داده رخ می‌دهد که متشکل از دو قسمت عمدهٔ «اصول به‌کارگیری داده‌ها» و «حقوق اطلاعاتی موضوع داده‌ها»ست. این اصول در حقیقت شکل ساختاربندی‌شدهٔ حقوق ماهوی شهروندان نسبت به داده‌های شخصی‌شان است. برای تضمین این حقوق ماهوی تعریف یک‌سری حقوق اطلاعاتی برای اشخاص و در مقابل آن یک‌سری تکالیف برای کنترل‌گران و پردازش‌گران لازم می‌نماید. رعایت نکردن این حقوق و تکالیف متناظر آن‌ها بخش عمده‌ای از جرایم علیه حریم خصوصی داده‌ها در فضای سایبر را تشکیل می‌دهد. به‌عبارت دیگر، بروز اتفاقاتی در دنیای مجازی، از جمله ارتکاب جرایم گوناگون و تبعات و آثار منفی و مخرب فرهنگی این محیط، دخالت علم حقوق را ضرورت بخشیده است. در حقیقت، اگرچه بهره‌گیری از ابزارهای فنی، نظیر فیلتر کردن و رمزنگاری، به‌منظور حمایت از حریم خصوصی داده‌های شخصی در ارتباطات الکترونیکی ضروری و مفید است، اما به‌هیچ‌وجه کافی نبوده است و برای حمایت کافی و مؤثر از این مقوله وضع قواعد و مقررات حقوقی دقیق و منسجم اجتناب‌ناپذیر است (زرکلام، ۱۳۸٦: ۱۷٤).

مباحث حقوقی راجع به تهدیدات حاصل از فنّاوری‌های پیش‌رفتهٔ کامپیوتری برای حریم خصوصی، پیش از مباحث حقوقی راجع به مسائل اقتصادی، در این بستر شکل گرفته است. در نتیجه، همکاری‌های بین‌المللی و به‌تبع آن هماهنگی بیش‌تری در قوانین داخلی کشورها در این زمینه به‌چشم می‌خورد. در حقوق ایران تاکنون مقررات خاصی برای حمایت از حریم خصوصی وضع نشده و لایحه‌ای که در سال‌های اخیر در این زمینه تدوین شده نیز هنوز به تصویب نرسیده است. با این حال، حمایت از داده‌های شخصی برای نخستین‌بار در قانون تجارت الکترونیکی مصوب سال ۱۳۸۲ و پس از آن، در قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸ در دستور کار قرار گرفته است. هر چند چنین حمایت‌هایی را باید ستود، اما این مقررات در مقایسه با مقررات سایر کشورها و مقررات سازمان‌های بین‌المللی در این زمینه نواقص و ایرادات جدی دارد. در مقالهٔ حاضر، مبحث حریم خصوصی داده‌ها در فضای سایبر، با تمرکز بر سیستم حقوقی ایران و مقایسه با قوانین برخی کشورهای اروپایی هم‌چون آلمان که دارای رویکردی جامع در زمینهٔ حمایت از حریم خصوصی است، مطالعه و بررسی می‌شود.

۲. چهارچوب مفهومی پژوهش

۱.۲ داده

مطابق مادهٔ ٦٠ قانون تجارت الکترونیکی، اسرار تجاری الکترونیکی داده پیامی است که شامل اطلاعات، فرمول‌ها، الگوها، نرم‌افزارها و برنامه‌ها، ابزارها و روش‌ها، فرایندها، تألیفات فشرده‌نشده، روش‌های انجام دادن تجارت و دادوستد، فنون، نقشه‌ها و اطلاعات مالی، فهرست مشتریان، طرح‌های تجاری، و امثال این‌هاست که به‌طور مستقل دارای ارزش اقتصادی است و در دسترس عموم قرار ندارد و تلاش‌های معقولانه برای حفظ و حراست از آن‌ها انجام شده است (نوری، ۱۳۸۳: ۳۸). هم‌چنین، طبق مادهٔ ۲ قانون تجارت الکترونیک ایران، داده پیامی از واقعه، اطلاعات، یا مفهوم است که با وسایل الکترونیکی، نوری، و یا فنّاوری‌های جدید تولید، ارسال، دریافت، ذخیره، یا پردازش می‌شود.

۲.۲ حریم خصوصی

در حال حاضر در ارائهٔ تعریفی جهانی و واحد از حریم خصوصی توافقی وجود ندارد. این اصطلاح را نخستین‌بار، در مقاله‌ای در سال ۱۸۹۰، ساموئل وارن (Samuel Warren) و لوئیس براندیس (Louis Brandeis)، حقوق‌دانان امریکایی، مطرح کردند و سپس اندیشمندان قرن نوزدهم هر چه بیش‌تر به مباحث هنجارین آن پرداختند (نوبهار، ١٣٨٦: ١٨٦). به نظر آنان، حریم خصوصی از جملهٔ ارجمندترین حقوق در دموکراسی است و حمایت از آن باید در قانون اساسی بازتاب یابد. آلن وستین (Alen Vestin) در *حریم خصوصی و آزادی* پیش‌نهاد می‌کند که حریم خصوصی کنترل شخص بر توزیع اطلاعات مربوط به خود تعریف شود. مطابق این تعریف، تجاوز به حریم خصوصی عبارت است از تلاش برای به‌دست آوردن اطلاعاتی مربوط به شخص و بعضی اوقات انتشار عمومی آن. حریم خصوصی قلمروی از زندگی شخصی است که انسان نوعی و متعارف با درک نیازهای جامعه در هیچ وضعیتی تجاوز به آن را مجاز نمی‌داند. می‌توان بین انواع حریم خصوصی از قبیل حریم خصوصی ارضی، حریم خصوصی جسمانی، حریم خصوصی ارتباطات، و حریم خصوصی اطلاعات تفکیک قائل شد؛[1] البته در پژوهش حاضر توجه بر حریم خصوصی اطلاعات معطوف است. تجاوز به حریم خصوصی اطلاعات شامل گردآوری، استفاده، و پخش اطلاعات راجع به افراد است. حق حریم خصوصی اطلاعات نیز حق نظارت بر افشا و دسترسی به اطلاعات شخصی است.

۳.۲ فضای سایبر

منظور از فضای سایبر یا فضای مجازی ترکیبی از ده‌ها هزار رایانهٔ به‌هم‌پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سویچ‌ها، و کابل‌های فیبر نوری است که امکان برقراری ارتباطات را در سامانه‌ای جامع فراهم می‌آورد (حسینی و ظریف‌منش، ۱۳۹۲: ٤٣). اصطلاح فضای سایبر یا دنیای مجازیِ آنلاین اصطلاحی است که نخستین‌بار ویلیام گیبسون (William Gibson) در رمانی با عنوان *نیورومانسر* (*Newromanser*) در سال ۱۹۸٤ به‌کار برد (پاکزاد، ۱۳۸۸: ۲۱). بنابراین، می‌توان فضای سایبر را محیطی مجازی و غیرملموس و موجود در شبکه‌های بین‌المللی تعریف کرد که همهٔ اطلاعات راجع به روابطِ افراد، فرهنگ‌ها، ملت‌ها، کشورها، و به‌طور کلی هر آن‌چه به‌صورت فیزیکی و ملموس در کرهٔ خاکی در این فضا به‌شکل دیجیتالی وجود دارد و قابل استفاده و در دسترسِ کاربران است که از طریق رایانه، اجزای آن، و شبکه‌های بین‌المللی به هم مرتبط است. از جمله ویژگی‌های فضای سایبر می‌توان به ارتباطات سریع، قابلیت ارسال پیام، ارائهٔ سرویس‌های ارتباطی، و تبادل اطلاعات با فرمت‌های گوناگون اشاره کرد (Mutula, 2007: 15).

۳. جرایم سایبری و انواع آن

ارائهٔ تعریفی دقیق و جامع از جرایم سایبری مشکل به‌نظر می‌رسد. به همین علت، همواره تعاریف متعدد و گوناگونی در این زمینه ارائه شده است، اما با وجود این تفاوت‌ها، بایستی سه ویژگی اصلی جرایم سایبری را همواره در تعاریف ارائه‌شده مدنظر قرار داد. این ویژگی‌ها شامل پیچیدگی فنّاوری، تنوع و گوناگونی، و توان مرموزسازی جرایم سایبری است (Zavrsink, 2008: 11). در این زمینه، مراجع قانون‌گذاری کشورهای گوناگون و اسناد بین‌المللی، اعم از ارشادی و الزام‌آور، هریک به فراخور نیازها و تهدیدات پیش رو تعاریف متفاوتی از این جرایم ارائه داده‌اند. به‌طور کلی در تعریفی جامع و مانع جرایم سایبری را می‌توان به این صورت تعریف کرد: «هر فعل یا ترک فعل مجرمانه‌ای که علیه رایانه یا موضوعات مرتبط با آن صورت گرفته یا به‌واسطهٔ رایانه محقق گردد جرم سایبری می‌باشد» (ویلیامز، ۱۳۹۱: ٤٨). بر اساس تقسیم‌بندی صورت‌گرفته در کنوانسیون جرایم سایبری، آن‌ها را می‌توان به چهار دسته تقسیم کرد:

دستهٔ نخست، جرایم علیه محرمانگی، تمامیت، و دسترس‌پذیری سیستم‌ها و داده‌های رایانه‌ای: این جرایم در مواد ۲ تا ٦ کنوانسیون مذکور ذکر شده است که به‌ترتیب، دسترسی غیرمجاز، شنود غیرمجاز، مختل کردن داده‌ها، و سوءاستفاده از دستگاه‌ها را شامل می‌شود؛

در پژوهش حاضر وضعیت حقوقی این دسته از جرایم سایبری را (با عنوان جرایم علیه حریم خصوصی داده‌ها) در ایران و آلمان تجزیه و تحلیل و با هم مقایسه می‌کنیم. دستهٔ دوم، جرایم مرتبط با رایانه: در مواد ۷ و ۸ کنوانسیون جرایم سایبر به‌ترتیب به دو جرم جعل و کلاه‌برداری مرتبط با رایانه اشاره شده است. دستهٔ سوم، جرایم مرتبط با محتوا: مادهٔ ۹ کنوانسیون به جرایم مرتبط با هرزه‌نگاری کودکان اشاره کرده است که این جرایم جزو جرایم مرتبط با محتوای داده‌های رایانه‌ای محسوب می‌شود. دستهٔ چهارم، جرایم مرتبط با نقض حق نشر و حقوق مرتبط: در مادهٔ ۱۰ کنوانسیون به جرایم مربوط به نقض حقوق مالکیت فکری از جمله حق نشر اشاره شده است (جلالی فراهانی، ۱۳۸۹: ۱۵۲).

در قانون جرایم رایانه‌ای ایران در قالب مواد ۱ تا ۲۵، جرایم سایبری با عنوان جرایم رایانه‌ای در هفت فصل احصا شده که عبارت است از: جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی از قبیل دسترسی غیرمجاز، شنود غیرمجاز، و جاسوسی رایانه‌ای؛ جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی از قبیل جعل رایانه‌ای و تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی؛ سرقت و کلاه‌برداری مرتبط با رایانه؛ جرایم علیه عفت و اخلاق عمومی مانند انتشار، توزیع، یا معاملهٔ محتویات مستهجن با استفاده از سامانه‌های رایانه‌ای یا حامل‌های داده، هتک حیثیت، و نشر اکاذیب؛ مسئولیت کیفری اشخاص حقوقی؛ جرایمی از قبیل تولید، انتشار، یا توزیع داده‌هایی که صرفاً به‌منظور ارتکاب جرایم رایانه‌ای به‌کار می‌روند؛ و سایر جرایم مصرح در مواد گوناگون.

۴. جرایم علیه حریم خصوصی داده‌ها در فضای سایبر در قانون آلمان

قانون مرتبط با حمایت از داده در آلمان قانون فدرال حمایت از داده (Bundes daten schutz gesetz/ BDSG) است که هدف اصلی آن حمایت از حق حریم خصوصی افراد در هنگام تبادل اطلاعات و داده های شخصی، از طریق اعمال یک سری اصول و قواعد در پردازش و استفاده از داده‌های شخصی، است. این قانون هم در بخش عمومی و هم در بخش خصوصی، که داده‌ها را برای پردازش سیستم‌ها جمع‌آوری می‌کند، لازم‌الاجراست؛ به‌جز مواردی که داده‌های جمع آوری‌شده منحصراً برای فعالیت های شخصی یا خانوادگی استفاده شود (Clavijo, 2013: 9).

به‌علت طبیعت فرامرزی و فراملی پردازش داده‌های شخصی در فضای سایبر، از دو دههٔ پیش جنبشی هماهنگ به‌منظور تدوین اصول کلی آن، شامل شورای اروپا، پارلمان اروپایی،

OECD، و سازمان ملل شکل گرفته است. نتایج این اقدامات بین‌المللی هم‌اکنون در ساختار قانونی بسیاری از کشورهای پیش‌رفته منعکس شده است. اکثر قوانین حمایت از داده در کشورهای گوناگون، از جمله آلمان، مبتنی‌بر هشت اصل زیر است:

۱. داده‌های شخصی باید به‌طور قانونی و منصفانه پردازش شود؛

۲. داده‌ها باید صرفاً برای اهدافی که جمع‌آوری می‌شود پردازش شود؛

۳. داده‌ها باید متناسب و مرتبط با اهداف باشد؛

٤. داده‌ها باید صریح و روزآمد باشد؛

۵. داده‌ها نباید بیش از زمان لازم نگه‌داری شود؛

٦. داده‌ها باید مطابق حقوق شخصی موضوعِ داده باشد؛

۷. ضمانت اجرایی مناسب علیه پردازش غیرمجاز و غیرقانونی داده‌ها معمول شود؛

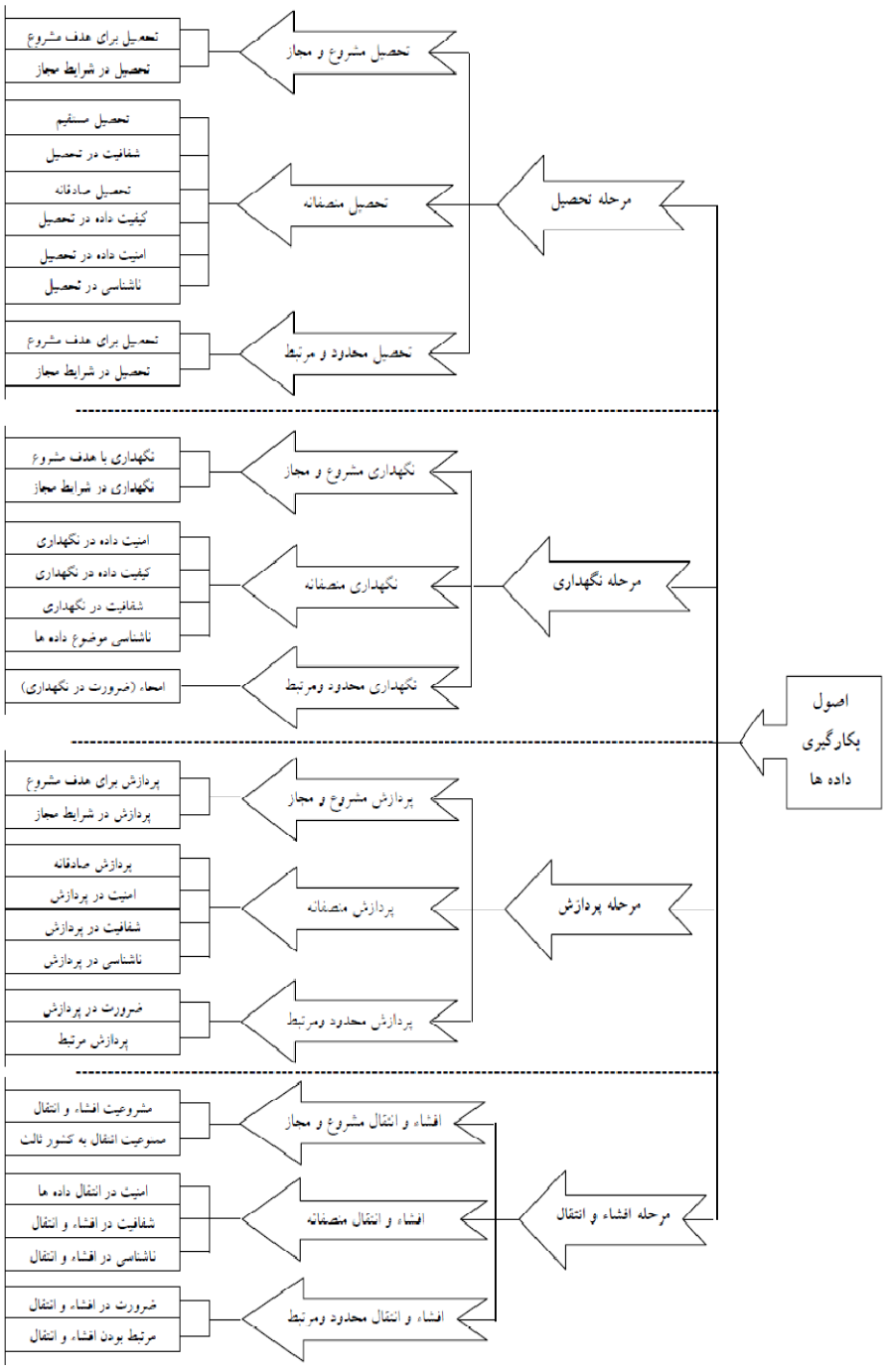
۸. انتقال داده‌ها به خارج از کشور یا قلمرو باید سطح مقتضی حمایت از حقوق و آزادی‌های اشخاص موضوع داده را از حیث پردازش داده‌های شخصی تأمین کند (نیسی و مدحج، ۱۳۹۰: ۳).

در حقوق کشورهای پیش‌رفته، از جمله آلمان، نقض اصول فوق‌الذکر منجر به نقض حریم خصوصی افراد می‌شود و با واکنش قانونی مواجه خواهد شد. در ادامه اصولی که نقض آن‌ها منجر به نقض حریم خصوصی داده‌ها در فضای سایبر می‌شود، طی دو مبحث «نقض اصول اولیهٔ به‌کارگیری داده‌ها» و «نقض حقوق اطلاعاتی موضوع داده‌ها»، بررسی می‌شود.

۱.٤ نقض اصول اولیهٔ به‌کارگیری داده‌ها

برای درک صحیح از جرم‌انگاری‌های صورت‌گرفته در قوانین و نیز پایه‌ریزی ارزش‌گذاری کیفری منطقی در حمایت از حریم خصوصی داده‌ها در فضای سایبر، می‌بایست نخست الزامات اساسی در حمایت از داده‌ها و اصول و مبانی حاکم بر جمع‌آوری، نگه‌داری، پردازش، انتقال، و افشای اطلاعات شخصی تبیین شود.

اصول اولیهٔ به‌کارگیری داده‌ها بخش اول از الزامات اساسی در حمایت از داده‌های شخصی است که نقض آن‌ها در حقوق کیفری کشورهای اروپایی می‌تواند تخلفی اداری یا جرمی کیفری در نظر گرفته شود. مطالعهٔ تطبیقی قوانین این کشورها نشان می‌دهد که نقض اصول مذکور بخش عمده‌ای از جرایم علیه حریم خصوصی داده‌ها در فضای سایبر را تشکیل می‌دهد. این اصول به‌تفصیل در نمودار ۱ نشان داده شده است.



نمودار ۱. اصول اولیهٔ به‌کارگیری داده‌ها (حسنی، ۱۳۸۵: ۱۴۰)

۱.۱.۴ گردآوری و تحصیل غیرمجاز داده‌ها

روش‌های متفاوتی برای جمع‌آوری داده‌ها وجود دارد که بعضاً تجاوزاتی آشکار و زیان‌بار نسبت به حریم خصوصی محسوب می‌شود؛ مانند استراق سمع، پایش تماس‌های تلفنی، یا تحصیل غیرمجاز فایل‌های حاوی داده‌های شخصی از طریق نقض تدابیر امنیتی. نقض هریک از اصول مربوط به تحصیل و گردآوری داده‌های شخصی می‌تواند به تجاوز علیه حریم خصوصی شهروندان منجر شود و به ایجاد مسئولیت بینجامد.

بر اساس مادهٔ ۲ بخش ٤ قانون فدرال حمایت از دادهٔ آلمان، داده‌ها تا حد امکان بایستی از شخص موضوع داده‌ها جمع‌آوری شود و در صورتی که این داده‌ها از اشخاص ثالث جمع‌آوری می‌شود، بایستی اجازهٔ قانونی در این خصوص وجود داشته باشد و هم‌چنین باید امکان دسترسی به اطلاعات لازم برای موضوع داده‌ها در صورت درخواست آنان فراهم باشد. این قانون هم‌چنین در بخش (a)۱۹ تکلیفی را برای کنترل‌گر، مبنی‌بر اطلاع‌رسانی به موضوع داده‌ها در صورتی که این داده‌ها از شخص ثالث جمع‌آوری شده باشد، مقرر کرده است. هم‌چنین مطابق مادهٔ ۱ بخش ۱۳ این قانون جمع‌آوری داده‌ها بایستی فقط در حد ضرورت باشد.

بر اساس بندهای ۱ و ۳ مادهٔ ۲ بخش ٤۳ این قانون، تخلف اداری زمانی ارتکاب می‌یابد که شخص عمداً یا به‌واسطهٔ بی‌مبالاتی داده‌های شخصی را، که عموماً قابل دسترسی بدون مجوز نیست، جمع‌آوری، پردازش، یا نگه‌داری کند، یا با استفاده از چنین داده‌هایی از طریق اقدامات غیرمجاز برای خود یا دیگری منفعت مالی کسب کند، یا داده‌های شخصی را که عموماً قابل دسترسی نیست انتقال دهد، یا از طریق بازیابی این داده‌ها برای خود یا دیگری کسب منفعت کند. هم‌چنین بر اساس مادهٔ ۱ بخش ٤٤ این قانون، هر کس در زمینهٔ ارتکاب عامدانهٔ جرم موضوع مادهٔ ٤۳ با قصد کسب منفعت برای خود یا دیگری ضرر یا صدمه‌ای به دیگران برساند، به زندان تا دو سال و جزای نقدی محکوم می‌شود و چنین جرایمی، در صورت اقامهٔ شکایت از سوی شخص زیان‌دیده، از سوی کمیسیونر فدرال حمایت از داده و مقام نظارتی تعقیب می‌شود.

در این ماده، در خصوص کسب منفعت مالی از طریق نقض حریم خصوصی، فقط به مجازات زندان تا دو سال و جزای نقدی اشاره شده و در خصوص بازگرداندن اموال بحثی به‌میان نیامده است. در حالی که در قوانین ایران قانون‌گذار در مادهٔ ۱۳ قانون جرایم رایانه‌ای مرتکب را، علاوه‌بر بازگرداندن اموال به صاحب آن، به حبس از یک تا پنج سال و جزای نقدی محکوم کرده است. هم‌چنین، نکتهٔ جالبی که در قسمت اخیر این ماده بیان شده این

است که تعقیب این نوع جرایم را منوط به شکایت شاکی کرده و حال آن‌که در قانون ایران به این موضوع اشاره نشده است. حال این سؤال مطرح می‌شود که جرایم موضوع این قانون جنبهٔ عمومی دارد یا خصوصی؟ و آیا در صورت وقوع جرم نیاز به شکایت شاکی برای امر تعقیب وجود دارد یا این‌که بدون نیاز به شکایت مراجع ذی‌صلاح موظف به تعقیب‌اند؟

۲.۱.۴ ذخیره و نگه‌داری غیرمجاز داده‌ها

دربارهٔ رعایت اصل شفافیت در نگه‌داری داده‌ها و حق دسترسی به داده‌ها برای سوژه، مادهٔ ۲ بخش ٦ قانون فدرال حمایت از دادهٔ آلمان مقرر می‌دارد که نگه‌داری‌کنندهٔ داده‌ها بایستی همواره اطلاعاتی مبنی‌بر هویت خود یا نمایندهٔ خود که اقدام به ذخیرهٔ داده‌ها کرده است، نشانی محل اقامت، منابع جمع‌آوری داده‌ها، اشخاصی که داده‌ها برای آن‌ها افشا خواهد شد، و حقوق موضوعِ داده‌ها در زمان نگه‌داری فراهم کند تا طبق مقررات، در صورت درخواست موضوعِ داده‌ها، این اطلاعات به وی ارائه شود. در جایی که به‌لحاظ عملی یا قانونی ارائهٔ اطلاعات به موضوع داده‌ها امکان‌پذیر نباشد، این اطلاعات به مقام ناظر ارائه می‌شود.

۳.۱.۴ پردازش غیرمجاز داده‌ها

پردازش بایستی به اطلاع موضوع داده‌ها برسد. بر اساس قانون فدرال حمایت از دادهٔ آلمان، اطلاعاتی مانند هدف پردازش، هویت و محل اقامت کنترل‌گر یا نمایندهٔ وی، روش پردازش، انواع داده‌های تحت پردازش، و مشخصات اشخاصی که داده‌ها برای آن‌ها افشا می‌شود بایستی طبق شرایط قانونی به اطلاع موضوع داده‌ها برسد. در مواردی که اطلاع‌رسانی مغایر با اهداف قانونی پردازش است یا طبق قانون نباید به موضوع داده‌ها اطلاع داده شود، مثلاً در پردازش برای اهداف امنیت ملی، چنین اطلاعاتی بایستی به یک مقام صالح قانونی یا مقام ناظر ارائه شود یا قابل دسترسی برای آنان باشد. این اصل هم در پردازش داده‌ها از سوی بخش خصوصی و هم از سوی بخش عمومی بایستی رعایت شود (Geiger, 2003: 750). در مادهٔ ۱ بخش ٤d قانون فدرال حمایت از دادهٔ آلمان، ثبت اطلاعات لازم، به‌منظور رعایت اصل شفافیت در تحصیل داده‌ها، شرط آغاز پردازش قرار داده شده است و مطابق مادهٔ ۵ همین بخش در برخی موارد که پردازش می‌تواند متضمن خطری برای حریم خصوصی و آزادی شخصی افراد باشد، مقنن می‌تواند شرایطی برای نظارت بر پردازش از سوی مقام ناظر مقرر کند.

مطابق مادهٔ ۳۹ این قانون، داده‌های شخصی که به مناسبت مشاغل خاص، مانند پزشکی یا وکالت، در اختیار صاحبان این حرفه‌ها قرار می‌گیرد صرفاً بایستی در جهت اهداف حرفه‌ای استفاده شود و رازداری حرفه‌ای در آن‌ها مراعات شود. هم‌چنین هیچ هدف ثانویه‌ای بدون اطلاع و رضایت موضوع داده‌ها نمی‌توان برای پردازش تعیین کرد، مگر با اجازهٔ قانون؛ البته اگر این اهداف ثانویه از لوازم و فروع منطقی و اجتناب‌ناپذیر هدف اولیه باشد، این هدف ثانویه مرتبط با هدف اولیه محسوب خواهد شد. هم‌چنین مطابق مواد ۱، ۲، و ۳ بخش ٤b این قانون، اگر داده‌ها به شخص ثالثی منتقل شود، بایستی اهداف اولیهٔ جمع‌آوری به وی اطلاع داده شود و او نیز مکلف به استفادهٔ محدود و مرتبط از داده‌های شخصی است. مطابق بندهای ۵ و ٦ مادهٔ ۲ بخش ٤۳ این قانون، در صورتی که از داده‌های شخصی برای اهدافی غیرمرتبط با انتقال این داده‌ها به شخص ثالث استفاده شود و یا نتیجهٔ پردازش داده‌ها به‌صورت ناشناس با نتیجهٔ تحقیقات علمی یا داده‌های شخصی افراد با هویت معلوم یا قابل شناسایی ترکیب شود، تخلفی اداری رخ داده است که براساس مادهٔ ۱ بخش ٤٤ این قانون هر گاه این جرایم عمداً در جهت تغییر میزان پرداخت یا با قصد کسب منفعت مالی برای خود یا دیگری یا با هدف آسیب زدن به شخص دیگر انجام شود، جرمی کیفری با مجازات حبس حداکثر تا دو سال یا جزای نقدی محسوب می‌شود.

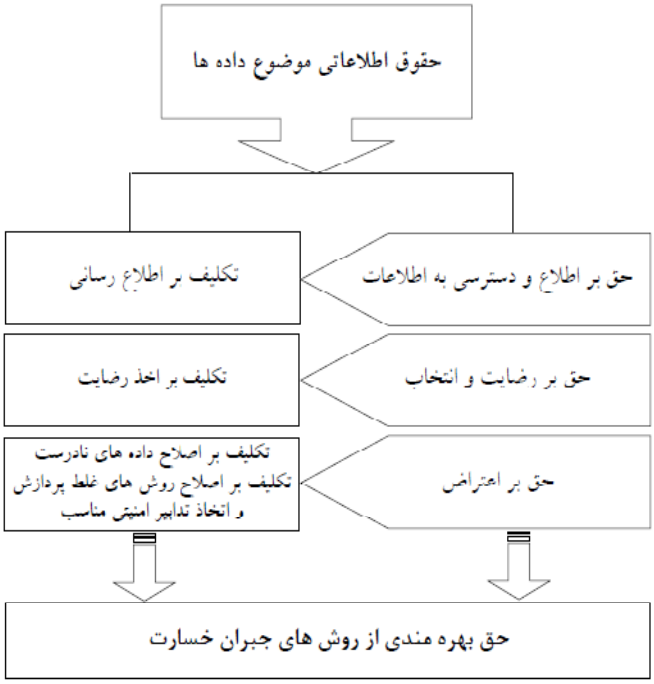
۴.۱.۴ افشا و انتقال غیرمجاز داده‌ها

مرحله‌ای که نقض آشکار حریم خصوصی اغلب در آن واقع می‌شود مرحلهٔ افشا و انتقال و به‌عبارت عام‌تر دردسترس‌سازی داده‌های شخصی است. نقض حق حریم خصوصی، به‌ویژه با افشای غیرمجاز، تجاوزی بی‌بازگشت است. شاید بتوان گفت همهٔ اصول مذکور در مراحل قبلی به‌کارگیری داده‌ها برای حفظ تمامیت معنوی و حیثیت اشخاص و حفظ محرمانگی اسرار ایشان در این مرحله است؛ ضمن این‌که نظام‌مند نبودن این مرحله از به‌کارگیری داده‌های شخصی می‌تواند موجب بی‌اثر شدن همهٔ تلاش‌ها در دیگر مراحل شود. مطابق مادهٔ ۱ بخش ۱۵ و مادهٔ ۱ بخش ١٦ قانون فدرال حمایت از دادهٔ آلمان، در دسترس قرار دادن داده‌های شخصی بایستی به‌منظور انجام دادن وظیفه و تکلیف در بخش عمومی یا اجرای قرارداد در بخش خصوصی ضرورت داشته باشد و فقط به اندازهٔ ضرورت صورت گیرد. استثنائاتی مانند دفاع از امنیت ملی یا عمومی و یا پیش‌گیری از تجاوزی مهم به حقوق دیگران می‌تواند توجیه‌کنندهٔ این ضرورت باشد. هم‌چنین براساس بند ٤ مادهٔ ۲ بخش ٤۳ و مادهٔ ۱ بخش ٤٤ این قانون، انتقال غیرمجاز داده‌های شخصی

تخلفی اداری محسوب می‌شود که اگر کسی آن را عمداً به‌منظور تغییر میزان پرداخت یا با قصد کسب منفعت مالی برای خود یا دیگری یا با هدف آسیب زدن به شخص دیگر انجام دهد، جرمی کیفری با مجازات حبس حداکثر تا دو سال یا جزای نقدی مرتکب شده است. هم‌چنین بر اساس مادهٔ ٤ بخش ۲۸ این قانون، انتقال و افشا مغایر با اهداف جمع‌آوری و پردازش ممنوع است. بنابراین، بازاریابی و نیز تبلیغات تجاری با استفاده از داده‌های شخصی و بدون رضایت موضوع داده‌ها ممنوع است و اگر قصد شود که داده‌های شخصی برای اهداف بازاریابی استفاده شود یا به شخص ثالث منتقل شود، این امر بایستی به اطلاع موضوع داده‌ها برسد و رضایت مجدد از وی اخذ شود.

۲.٤ نقض حقوق اطلاعاتی موضوع داده‌ها

حقوق اطلاعاتی موضوع داده‌ها، به‌منزلهٔ قسمت دوم از الزامات اساسی حمایت از داده‌ها، به‌حدی حائز اهمیت است که نقض آن‌ها دستهٔ مهمی از جرائم علیه حریم خصوصی در فضای سایبر را به‌وجود می‌آورد. این حقوق در نمودار ۲ نشان داده شده است.



نمودار ۲. حقوق اطلاعاتی موضوع داده‌ها (حسنی، ۱۳۸۵: ۱٤۰)

مهم‌ترین موارد نقض حقوق اطلاعاتی اشخاص عبارت است از: ۱. پاسخ‌های کذب یا پاسخ ندادن به تقاضای به‌عمل‌آمده برای حق دست‌یابی فرد، ۲. اخذ نکردن رضایت در موارد لزوم و بی‌توجهی به رد پردازش یا شرایط مقرر از جانب موضوع داده‌ها، ۳. بی‌اعتنایی به اعتراض موضوع داده‌ها و تصحیح نکردن داده‌های نادرست یا اصلاح نکردن روش پردازش (حسنی، ۱۳۸۵: ۱٤۸). با توجه به طبقه‌بندی سه‌گانهٔ حقوق اطلاعاتی موضوع داده‌ها، جرایم این طبقه را در سه دسته بررسی خواهیم کرد.

۱.۲.۴ نقض حق اطلاع یا دسترسی به اطلاعات

موضوع داده‌ها حق دارد قبل از جمع‌آوری هر گونه اطلاعات شخصی دربارهٔ وی از این امر مطلع شود. در این زمینه، هویت کنترل‌گر یا نمایندهٔ وی، اهداف پردازش، نوع داده‌هایی که جمع‌آوری خواهد شد، افرادی که داده‌های شخصی برای آنان افشا خواهد شد، و نیز حقوق موضوع داده‌ها در مراحل گوناگون به‌کارگیری داده‌ها بایستی به اشخاص اطلاع داده شود. هر گونه اطلاعات دیگر که برای تضمین منافع موضوع داده‌ها لازم است و به‌موجب قانون مقرر می‌شود بایستی به اطلاع وی برسد. در صورتی که داده‌ها از شخص ثالث تحصیل شود یا گردآورنده امکان عملی اطلاع‌رسانی را نداشته باشد، بایستی امکان دسترسی شخص به اطلاعات فوق را با روشی آسان و ارزان فراهم آورد. این حق در همهٔ مراحل به‌کارگیری داده برقرار است. تکلیف متناظر این حق مبنی‌بر اطلاع‌رسانی بر عهدهٔ کنترل‌گر و هر شخص دیگری است که داده‌های شخصی را پردازش می‌کند. نقض این حق در قوانین حمایت از داده‌ها جرم‌انگاری شده است (اصلانی، ۱۳۸٤: ۱۱). براساس مفاد بخش ۱۹ قانون فدرال حمایت از دادهٔ آلمان، در صورت درخواست شخص سوژه، داده‌های ذخیره‌شده در خصوص او از جمله منبع و مقصد احتمالی آن‌ها و هم‌چنین هدف از ذخیره‌سازی داده‌ها باید در اختیار او قرار گیرد. هم‌چنین به‌موجب مفاد بخش ۲۰ این قانون، لزوم تصحیح، امحا، و توقیف داده‌های شخصی ناصحیح مقرر شده است. به‌علاوه به‌موجب بند ۳ مادهٔ ۱ بخش ٤۳ این قانون، در صورت نقض حق اطلاع و دسترسی به اطلاعات دربارهٔ استفاده از داده‌های شخصی در زمینهٔ بازاریابی و تبلیغات تجاری، خواه عامداً خواه با بی‌احتیاطی، و براساس بند ۸ این ماده، در صورت نقض حق اطلاع شخص یا انجام ندادن صحیح و کامل آن، خواه عامداً خواه با بی‌احتیاطی، تخلفی اداری ارتکاب می‌یابد.

البته اجرای مطلق این حق، ضمن این‌که می‌تواند مانع جریان آزاد اطلاعات باشد، در موارد عدیده‌ای نیز به‌لحاظ عقلانی امکان‌پذیر نیست و یا لازم به‌نظر نمی‌رسد؛ بنابراین،

همواره استثنائاتی در قوانین بر آن وارد شده است. برای مثال، مطابق مادهٔ ٤ بخش ۱۹ قانون حمایت از دادهٔ آلمان، قانون‌گذار در مواردی مانند پردازش برای منافع عمومی مهم مثل امنیت و دفاع ملی، سلامت عمومی، اهداف تحقیقاتی علمی، آماری، و تاریخی و نیز اهداف هنری، ادبی، یا روزنامه‌نگاری، در زمینهٔ آزادی بیان و یا ذخیره و پردازش برای اهداف صرفاً شخصی، می‌تواند این استثنائات را توسعه دهد. این استثنائات به‌منظور برقراری توازن میان منافع عمومی و حقوق فردی است و بایستی به میزان ضرورت و به‌صورت صریح پیش‌بینی شود و تا حدی گسترده نشود که از اصل چیزی باقی نگذارد.

۲.۲.۴ نقض حق رضایت و انتخاب

گردآورندهٔ داده‌ها باید این امکان را برای موضوع داده‌ها فراهم آورد که وی صریحاً نظر خود را مبنی‌بر این‌که با گردآوری داده‌های شخصی خود موافق است یا خیر اعلام کند و هم‌چنین پس از اطلاع شخص از تصمیم کنترل‌گر، مبنی‌بر جمع‌آوری اطلاعات شخصی مربوط به وی، بتواند نارضایتی خود را اعلام و از جمع‌آوری ممانعت کند. در صورت رضایت، شخص می‌تواند حدود جمع‌آوری اطلاعات، نحوهٔ پردازش، و حدود افشا و انتقال را تعیین و رضایت خود را به حوزهٔ مشخص‌شده محدود کند. این حق نیز در همهٔ مراحل به‌کارگیری داده برقرار است و نقض آن باعث وضع جرایمی در قوانین حمایت از داده شده است (عامل نجف‌آبادی، ۱۳۸۷: ۸۲).

در قانون فدرال حمایت از دادهٔ آلمان، تخلف اداری مبنی‌بر نقض حق رضایت دربارهٔ استفاده از داده‌های شخصی در زمینهٔ بازاریابی و تبلیغات تجاری پیش‌بینی شده است. این قانون هم‌چنین در مادهٔ ۱ بخش ٤a مقرر کرده است که رضایت سوژه بایستی به‌صورت کتبی اعلام شود، مگر این‌که قانون طور دیگری مقرر کرده باشد.

۳.۲.۴ نقض حق اعتراض

اگر در نتیجهٔ اطلاعاتی که کنترل‌گر در اختیار موضوع داده‌ها قرار می‌دهد یا به هر روش دیگر شخص مطلع شود که داده‌های جمع‌آوری‌شده از وی یا داده‌های در حال پردازش یا انتقال از او نادرست یا ناقص یا قدیمی است، حق اعتراض به دارندهٔ داده‌ها را دارد. حق اعتراض برای موضوع داده‌ها در همهٔ مواردی که کنترل‌گر از اصول پردازش داده تخطی می‌کند برقرار است. اگر این اعتراض موجه و منطقی باشد، به تکلیفی بر عهدهٔ کنترل‌گر مبنی بر اصلاح، پاک کردن، یا متوقف‌سازی داده‌های نادرست یا اصلاح روش پردازش یا

توقف پردازش غیرمجاز می انجامد. نقض این حق یا بی‌توجهی به آن و رعایت نکردن تکلیف برای اصلاح موجب پیش‌بینی جرایمی در قوانین حمایت از داده شده است.

براساس مفاد بخش‌های ۲۰ و ۳۵ قانون حمایت از دادهٔ آلمان، داده‌های نادرست بایستی تصحیح شود و اگر کار ذخیرهٔ داده‌ها ناموجه باشد یا دانستن آن‌ها برای اجرای وظایف کنترل‌گر لازم نباشد، بایستی پاک شود و اگر پاک کردن داده در آن زمان طبق قانون مجاز نباشد یا مضر به منافع مهم دیگران باشد یا پاک کردن عملاً غیرممکن یا مستلزم تلاش بیش از حد معقولی باشد، بایستی بلوکه شود. در این قانون هم‌چنین، براساس بند ۳ مادهٔ ۱ بخش ٤۳، تخلفی اداری در خصوص نقض حق اعتراض در صورت استفاده از داده‌های شخصی در زمینهٔ بازاریابی و تبلیغات تجاری پیش‌بینی شده است.

۴.۲.۴ حق بهره‌مندی از جبران خسارت

هر جا که حقی مشروع برای شخصی مقرر شود، این وظیفهٔ قانون است که با ضمانت اجراهای متناسب از آن حمایت کند. این حق در موارد تجاوز از اصول پردازش داده نیز جریان دارد و شخص می‌تواند به‌علت نقض حقوق خود تقاضای جبران خسارت داشته باشد. در کشورهای گوناگون بهره‌مندی از جبران خسارت در موارد تجاوز به حقوق شخصی امری پذیرفته‌شده است. این مسئولیت در قبال اعمال توجیه‌ناپذیر و نادرست ایجاد می‌شود. مطابق مفاد بخش ۷ قانون حمایت از دادهٔ آلمان، اگر شخصی که خسارت به‌بار آورده است ثابت کند که مراقبت‌های لازم را چه به‌لحاظ فنی و چه به‌لحاظ حقوقی اعمال کرده است، مسئول نخواهد بود. هم‌چنین بخش ۸ این قانون حق بهره‌مندی از جبران خسارت برای موضوع داده‌ها را، در صورتی که خسارت در پردازش از سوی بخش‌های عمومی صورت گرفته باشد، پیش‌بینی می‌کند.

در حقوق داخلی ایران مادهٔ ۷۸ قانون تجارت الکترونیکی[۲] در همین باره مقرر شده است، اما حکم مادهٔ مذکور فقط ناظر بر مسئولیت مدنی قهری و منصرف از مسئولیت مدنی قراردادی است؛ بنابراین در مواردی که ایراد خسارت ناشی از نقض مفاد تعهد قراردادی باشد، مبنای مسئولیت متعهد متخلف رابطهٔ قراردادی فی‌مابین است که بر طبق قواعد حقوق قراردادها اعمال می‌شود. هم‌چنین، متن این ماده به‌گونه‌ای تنظیم شده است که فقط موارد خاصی از علل ورود خسارت را شامل می‌شود و شمول و گسترهٔ کافی ندارد. در واقع، حکم مقرر این ماده موهِم این معناست که در حوزهٔ مسئولیت مدنی قهری ناشی از تخلف از مقررات مربوط به حمایت از داده نمی‌توان به قواعد عام مسئولیت مدنی استناد کرد و فقط در حدود مقرر در این ماده می‌توان به جبران خسارت حکم داد.

۵. بررسی جرایم علیه حریم خصوصی داده‌ها در فضای سایبر در قانون ایران

۱.۵ قانون تجارت الکترونیک مصوب ۱۳۸۲

یکی از مباحث عمده در تجارت الکترونیک بحث حمایت از داده‌های شخصی است. اطلاعات همواره نقش بسیار مهمی در تجارت دارد. بازاریابی، تعیین زمان و مکان خرید و فروش اجناس، و همهٔ فعالیت‌های مرتبط با تجارت رابطهٔ نزدیکی با اطلاعات دارد. از این رو، مقنن در چند ماده از قانون تجارت الکترونیکی به بحث «حمایت از داده‌ها» توجه نشان داده است. براساس مادهٔ ۵۸ این قانون، ذخیره، پردازش، و یا توزیع دادهٔ پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی ـ مذهبی، خصوصیات اخلاقی، و دادهٔ پیام‌های راجع به وضعیت جسمانی، روانی، و یا جنسیتی اشخاص، بدون رضایت صریح آن‌ها، جرم‌انگاری شده است. این ماده به‌ظاهر بر رعایت «اصل تحصیل قانونی و مبتنی‌بر رضایت سوژه یا شخص موضوع گردآوری و پردازش» تأکید کرده است، اما باید توجه داشت که واژهٔ «ذخیره» را، که در این ماده از مصادیق اعمال ممنوع تلقی شده است، نمی‌توان مرادف با اصطلاح «گردآوری» تلقی کرد، زیرا گردآوری ناظر بر مرحلهٔ تحصیل داده‌ها و ذخیره ناظر بر مرحلهٔ نگه‌داری داده‌هاست. با این وصف، نمی‌توان به ممنوعیت گردآوری غیرمجاز داده‌ها براساس این ماده قائل بود. در ادامه و در زمینهٔ موضوع مادهٔ مذکور، مادهٔ ۵۹ مقرر می‌دارد که در صورت رضایت شخص موضوع داده نیز ذخیره، پردازش، و توزیع دادهٔ پیام‌های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایطی صورت پذیرد؛ از جمله: ۱. اهداف این قبیل اقدامات مشخص باشد و به‌طور واضح شرح داده شده باشد (اصول تحصیل، نگه‌داری، و پردازش محدود و مرتبط)، ۲. دادهٔ پیام باید به اندازهٔ ضرورت و متناسب با اهداف شرح‌داده‌شده برای شخص موضوع دادهٔ پیام جمع‌آوری شود و فقط برای اهداف تعیین‌شده استفاده شود (اصول تحصیل و پردازش محدود و مرتبط)، ۳. دادهٔ پیام باید صحیح و روزآمد باشد (اصل درستی یا صحت داده‌های گردآوری‌شده)، ٤. شخص موضوع دادهٔ پیام باید به پرونده‌های رایانه‌ای حاوی دادهٔ پیام‌های شخصی مربوط به خود دسترسی داشته باشد و بتواند دادهٔ پیام‌های ناقص و یا نادرست را محو یا اصلاح کند (اصل حق اطلاع و دسترسی به اطلاعات برای سوژه)، و ۵. شخص موضوع دادهٔ پیام باید بتواند در هر زمان، با رعایت ضوابط مربوط، محو کامل پروندهٔ رایانه‌ای دادهٔ پیام شخصی مربوط به خود را درخواست کند (اصل حق امحا برای سوژه). در مادهٔ ٦٤ این قانون، به‌منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبادلات

الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسسات برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم‌انگاری شده است (اصول تحصیل مشروع و مجاز داده‌ها و افشا و انتقال مشروع و مجاز داده‌ها). براساس مادهٔ ۷۵، متخلفان از این ماده و هر کس که در بستر مبادلات الکترونیکی به‌منظور رقابت، منفعت، و یا ورود خسارت به بنگاه‌های تجاری، صنعتی، اقتصادی، و خدماتی، با نقض حقوق قراردادهای استخدام مبنی‌بر افشا نکردن اسرار شغلی و یا دست‌یابی غیرمجاز، اسرار تجاری آنان را برای خود تحصیل و یا برای اشخاص ثالث افشا کند، به حبس از شش ماه تا دو و نیم سال و جزای نقدی معادل ۵۰ میلیون ریال محکوم خواهد شد (اصول تحصیل مشروع و مجاز داده‌ها و افشا و انتقال مشروع و مجاز داده‌ها). هم‌چنین در مادهٔ ۷۸ قانون مذکور، قانون‌گذار به اصل حق بهره‌مندی از جبران خسارت توجه نشان داده است. بدین‌صورت که هر گاه در بستر مبادلات الکترونیک، بر اثر نقص یا ضعف سیستم مؤسسات خصوصی و دولتی، به‌جز در نتیجهٔ قطع فیزیکی ارتباط الکترونیکی، خسارتی به اشخاص وارد شود، مؤسسات مزبور مسئول جبران خسارت‌اند، مگر این‌که خسارات واردشده ناشی از فعل شخصی افراد باشد، که در این صورت جبران خسارات بر عهدهٔ این اشخاص خواهد بود (اصل حق بهره‌مندی از جبران خسارت).

همان‌گونه که ملاحظه می‌شود، مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی در زمینهٔ حمایت از داده‌های شخصی به برخی از اصول ناظر بر حمایت از حریم خصوصی داده‌ها و اطلاعات شخصی در محیط الکترونیکی توجه کرده است. از آن جمله می‌توان به اصل تحصیل قانونی و مبتنی‌بر رضایت سوژه یا شخص موضوع گردآوری و پردازش (مادهٔ ۵۸)، اصل تحصیل مضیق و مرتبط (بندهای الف و ب مادهٔ ۵۹)، اصل درستی یا صحت داده‌های گردآوری‌شده (بند ج مادهٔ ۵۹)، اصل دسترسی (بند د مادهٔ ۵۹)، و اصل امحا (بند هـ مادهٔ ۵۹) اشاره کرد. با این حال، برخی از اصول دیگر که در حقوق اروپایی و مقررات برخی کشورها به آن‌ها تصریح شده در حقوق ایران قانون‌گذار به آن‌ها توجهی نکرده است؛ از آن جمله می‌توان به اصل انتخاب، اصل امنیت، اصل شفاف‌سازی، اصل ممنوعیت افشا، اصل پردازش مرتبط، و اصل ممنوعیت انتقال اشاره کرد. به‌علاوه، هر چند قانون‌گذار ایران برخی از اصول حاکم‌بر حمایت از داده‌های شخصی را تصریح کرده، با این حال، گاه همهٔ مقتضیات آن را پیش‌بینی نکرده است. برای مثال، در خصوص اصل قانونی بودن و لزوم تحصیل رضایت سوژه، هر چند ضرورت آن در مادهٔ ۵۸ به‌صراحت ذکر شده است، اما مستثنیات آن پیش‌بینی نشده و با توجه به مادهٔ ٦١ آن قانون به آیین‌نامه واگذار شده است

که این مسئله جای تأسف دارد، زیرا مستثنیات نیز به اندازهٔ خود اصل حائز اهمیت است و بایستی در قالب قانون پیش‌بینی شود تا از هر گونه سوءاستفادهٔ احتمالی جلوگیری به عمل آید. از سوی دیگر، بدیهی است که مقررات آمره و ضمانت اجراها، اعم از حقوقی و کیفری، در چهارچوب آیین‌نامه امکان پیش‌بینی ندارد. هم‌چنین توجه به مفاد بند اخیر مادهٔ ۵۹ مبین آن است که صرف‌نظر از انشای ناصواب و غیرحقوقی ماده، با توجه به اطلاق و عموم عبارات به‌کاررفته در قانون که مشمول همهٔ مؤسسات و نهادها (حتی دولتی و عمومی) می‌شود، این حکم به‌هیچ‌وجه توجیه و حتی امکان اجرا ندارد و از مصادیق افراط و تفریط قانون‌گذار در امر حمایت از داده است. در خصوص مادهٔ ۷۳ این قانون[۳] نیز نکاتی قابل ذکر است: ۱. مجازات مقرر در این ماده فقط اختصاص به فرضی دارد که جرم ارتکابی ناشی از بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی باشد، نه مطلق اشخاصی که داده‌های شخصی افراد را در اختیار دارند، ۲. مجازات مقرر در این ماده فقط ناظر بر فرضی است که به‌واسطهٔ بی‌مبالاتی و بی‌احتیاطی مؤسسات مورد بحث جرمی راجع به داده‌های شخصی روی دهد و در هر مورد که نقض حقوق سوژه یا اصول حاکم‌بر قانون صورت پذیرد کارایی ندارد.

در مقابل، قانون فدرال حمایت از دادهٔ آلمان مقررات صریح و روشنی را در خصوص وظایف و اختیارات و نیز مسئولیت‌های اشخاصی که داده‌های شخصی را گردآوری و پردازش می‌کنند وضع کرده و وضعیت حقوقی تمامی اشخاص دست‌اندرکار و ذی‌نفع در بحث داده‌های شخصی را مشخص کرده است.

۲.۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸

در بخش یکم قانون جرایم رایانه‌ای ایران مصوب ۱۳۸۸، در قالب فصول اول و دوم به‌ترتیب «جرایم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی» و «جرایم علیه صحت و تمامیت داده و سیستم‌های رایانه‌ای و مخابراتی» بیان شده است.

در مادهٔ ۱ این قانون، که نقض «اصل تحصیل مشروع و مجاز» را جرم‌انگاری کرده است، قانون‌گذار برای دسترسی غیرمجاز به داده‌ها حبس از ۹۱ روز تا یک سال یا جزای نقدی از ۵ تا ۲۰ میلیون ریال و یا هر دو مجازات را مقرر کرده است.

مادهٔ ۲ این قانون نیز نقض «اصل تحصیل منصفانهٔ داده‌ها» را جرم‌انگاری کرده و در خصوص شنود[۴] غیرمجاز مجازات حبس از شش ماه تا دو سال یا جزای نقدی از ۱۰ تا ۴۰

میلیون ریال یا هر دو را مقرر کرده است. هم‌چنین بـا دقـت در مفـاد مـواد ۳، ٤، و ۵ ایـن قانون، نسبت به داده‌های سری یا ارتکاب جرم از سوی مأموران دولتی کـه مسـئول حفـظ داده‌های سری باشند، مجازات سنگین‌تری در نظر گرفته است.

در مواد ٦ و ۷ این قانون در خصوص جعل یارانه‌ای صحبت شده است. جعل در لغت به معنی ساختن، کردن، آفریدن، قرار دادن، وضع کردن، و تقلب کردن است و در اصطلاح عبارت است از قلب متقلبانهٔ حقیقت در سند یا نوشته یا چیز دیگری به قصد اضرار به غیر و به طریق پیش‌بینی‌شده در قانون (شاملو احمدی، ۱۳۸۰: ۱۸٦). مصادیقی که در مادهٔ ٦ قانون جرایم رایانه‌ای ذکر شده است به‌مراتب خیلی کم‌تر از مصادیق مذکور در مادهٔ ۵۳۲ قانون مجازات اسلامی در خصوص جعل و تزویر است. در بندهای الف و ب قانون جرایم رایانه‌ای، مصادیق جعل با عناوین تغییر داده‌ها، ایجاد یا وارد کردن متقلبانهٔ داده‌ها، یا تغییر داده‌ها یا علائم در انواع وسایل ذخیره‌سازی از قبیل کارت‌های حافظه و تراشه‌ها بیان شده است. به‌نظر می‌رسد که مصادیق مذکور در بندهای این ماده برخلاف مادهٔ ۵۲۳ قانون مجازات اسلامی حصری‌اند. هم‌چنین استفاده از داده‌ها با علم به مجعول بودن آن‌ها در مادهٔ ۷ بیان شده است. سؤالی که مطرح می‌شود این است که، در صورت یکی بودن جاعل و استفاده‌کننده، فرد مشمول دو مجازات جداگانهٔ مذکور در مواد ٦ و ۷ قرار می‌گیرد یا یک مجازات نسبت به وی اعمال می‌شود؟ به‌نظر می‌رسد، همان‌گونه که در رأی وحدت رویهٔ شمارهٔ ۱۱۸۸–۱۳۳٦/۳/۳۰ هیئت عمومی دیوان عالی کشور بیان شده است، در اعمال تعدد مجازات تفاوتی ندارد که استفاده‌کننده از سند مجعول همان جاعل باشد یا شخص دیگر، بنابراین تعدد مجازات اعمال می‌شود (زراعت، ۱۳۸٦: ۳۹۳). از طرف دیگر، می‌توان استدلال کرد که جعل مذکور در جرایم رایانه‌ای با جعل در قانون مجازات اسلامی متفاوت است و نمی‌توان رأی وحدت رویه را به جعل جرایم رایانه‌ای تعمیم داد. اصل تفسیر به نفع متهم نیز اقتضا می‌کند که رأی وحدت رویه را منصرف از این موضوع بدانیم. بنابراین بهتر بود که قانون‌گذار دربارهٔ این موضوع تعیین تکلیف می‌کرد.

فصل سوم این قانون در خصوص سرقت و کلاه‌برداری رایانه‌ای بحث کرده است. در مادهٔ ۱۲ قانون‌گذار بیان کرده است که هر کس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنان‌چه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی تا ۲۰ میلیون ریال و در غیر این صورت، یعنی در صورتی که این داده‌ها در اختیار صاحب آن نباشد، به حبس از ۹۱ روز تا یک سال و جزای نقدی از ۵ تا ۲۰ میلیون ریال یا هر دو مجازات محکوم می‌شود.

قانون‌گذار در مواد ۱۶ و ۱۷ این قانون مقرر کرده است که هر کس از طریق سیستم‌های رایانه‌ای فیلم، صوت، یا تصویر افراد را تغییر دهد یا تحریف کند، یا فیلم خانوادگی یا اسرار دیگران را بدون رضایت آن‌ها منتشر کند یا در دسترس دیگران قرار دهد و یا با ایجاد تغییر یا تحریف به انتشار آن‌ها اقدام کند، به حبس از ۹۱ روز تا یک سال یا جزای نقدی از ۵ تا ۴۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد. مادهٔ مذکور به‌عبارتی، نقض عامدانهٔ «اصل کیفیت داده‌های شخصی در مرحلهٔ پردازش» و «اصل پردازش صادقانه با تغییر داده‌های درست یا تولید داده‌های نادرست» و مادهٔ ۱۷ نیز نقض «اصول راجع به افشا و انتقال داده‌ها» را جرم‌انگاری کرده است.

هم چنین طبق بندهای الف و ب مادهٔ ۲۵، هر کس از طریق تولید، انتشار، یا معامل، داده‌ها یا فروش یا در دسترس قرار دادن داده‌ها و گذرواژه‌ها، که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم آورد، متجاوز به حریم خصوصی دیگران شود، به حبس از ۹۱ روز تا یک سال یا جزای نقدی از ۵ تا ۲۰ میلیون ریال یا هر دو مجازات محکوم می‌شود.

قانون گذار در مواد ۲۸ تا ۳۱ صلاحیت محاکم ایران رسیدگی به این جرایم را پیش‌بینی کرده است و در صورتی که جرم علیه اشخاص ایرانی یا علیه جمهوری اسلامی ایران باشد، صرف‌نظر از این‌که مرتکب آن ایرانی باشد یا غیرایرانی و این‌که این جرایم در داخل یا خارج از کشور واقع شوند، محاکم ایران صالح به رسیدگی‌اند.

۳.۵ آیین‌نامهٔ دفاتر خدمات حضوری اینترنت (coffee net)

این دفاتر محلی برای ارائهٔ خدمات دسترسی حضوری به شبکه‌های اطلاع‌رسانی (اینترنت و اینترانت) است و مطابق بند ۷ آیین‌نامهٔ این مراکز، افشای روابط خصوصی افراد و تجاوز به حریم اطلاعات شخصی آنان، انتشار اطلاعات حاوی کلیدهای رمز بانک‌های اطلاعاتی، نرم‌افزارهای خاص، صندوق‌های پست الکترونیکی و یا روش شکستن آن‌ها، هر گونه نفوذ غیرمجاز به مراکز دارندهٔ اطلاعات خصوصی و محرمانه و تلاش برای شکستن قفل رمز سیستم‌ها، و هر گونه تلاش برای شنود و بررسی بسته‌های اطلاعاتی در حال گذر در شبکه که به دیگران تعلق دارد ممنوع اعلام شده است؛ به‌عبارتی، نقض اصولی از قبیل تحصیل مشروع و مجاز، تحصیل منصفانه، و اصول راجع به در دسترس قرار دادن داده‌ها ممنوع شده است.

٤.٥ آیین‌نامهٔ واحدهای ارائه‌کنندهٔ خدمات اطلاع‌رسانی و اینترنت (ISP)[٥]

یک رسا (ISP) اتصال به شبکهٔ اطلاع‌رسانی و اینترنت را فراهم می‌آورد و جزء ضروری دسترسی و اتصال افراد به شبکهٔ اینترنت است. رساها با داشتن امکانات ویژه راحت‌تر از دیگران می‌توانند حریم خصوصی شهروندان را نقض کنند. از طرف دیگر، فعالیت نظام‌مند آن‌ها مبتنی‌بر تدابیر امنیتی می‌تواند از ارتکاب بسیاری از جرایم علیه داده‌های شخصی پیش‌گیری کند.

آیین‌نامهٔ واحدهای ارائه‌کنندهٔ خدمات اطلاع‌رسانی و اینترنت نیز همانند آیین‌نامهٔ دفاتر خدمات حضوری اینترنت، ضمن تأکید بر مصونیت حریم خصوصی کاربران در بندهای ٥-٣-١٥ و ٦، در بند ٩ تجاوز به حریم خصوصی کاربران را به یک‌سری ضمانت اجراهای اداری از قبیل تذکر، قطع موقت مجوز، لغو پروانه، و طرح در دادگاه‌ها و محاکم قانونی بسته به نوع تخلف مقید کرده است؛ ضمن این‌که این ضمانت اجراها مانع از طرح مورد در دادگاه‌ها و اعمال حقوق کیفری نخواهد بود. در بند ٦ مصادیق مهمی از تجاوز به حریم خصوصی مانند شنود یا دسترسی غیرمجاز تخلف شمرده شده است، از جمله افشای روابط خصوصی افراد و تجاوز به حریم اطلاعات شخصی آنان، انتشار اطلاعات حاوی کلیدهای رمز بانک‌های اطلاعاتی، نرم‌افزارهای خاص، صندوق‌های پست الکترونیکی و یا روش شکستن آن‌ها، هر گونه نفوذ غیرمجاز به مراکز دارندهٔ اطلاعات خصوصی و محرمانه و تلاش برای شکستن قفل رمز سیستم‌ها، و هر گونه تلاش برای شنود و بررسی بسته‌های اطلاعاتی در حال گذر در شبکه که به دیگران تعلق دارد. به‌عبارتی، در آیین‌نامهٔ مذکور نقض اصولی از قبیل تحصیل مشروع و مجاز، تحصیل منصفانه، و اصول راجع به در دسترس قرار دادن داده‌ها ممنوع شده است.

۶. نتیجه‌گیری

قوانین حمایت از داده یکی از ملزومات عصر جدید است که از اصول مهم فضای سایبر به‌شمار می‌رود و تقریباً همهٔ کشورها سطح متعارفی از اصول حمایتی را در این فضا برقرار کرده‌اند. فقدان قوانین مناسب برای حمایت از داده‌ها در زندگی امروزی حتی در ساده‌ترین استفاده‌ها از فضای مجازی اثر می‌گذارد. برای درک صحیح جرم‌انگاری‌های صورت‌گرفته و نیز پایه‌ریزی ارزش‌گذاری کیفری منطقی دربارهٔ حمایت از حریم خصوصی در برابر نقض الزامات اساسی حمایت از داده‌ها در فضای سایبر، می‌بایست نخست اصول و مبانی

حاکم‌بر جمع‌آوری، نگه‌داری، پردازش، انتقال، و افشای اطلاعات شخصی تبیین شود و سپس حقوق اشخاص موضوع داده معین شود. آن‌گاه می‌توان موارد شدید نقض و تجاوز به این اصول و حقوق را جرم‌انگاری کرد و یا در مقام تفسیر و اجرای جرم‌انگاری‌های صورت‌گرفته از چهارچوب مشخصی بهره‌مند شد. نقض این اصول و حقوق ناشی از آن‌ها طبقات عمدهٔ جرایم علیه حریم خصوصی در فضای سایبر را پدید می‌آورد؛ ضمن این‌که تبیین دقیق اصول و حقوق مبتنی‌بر واقعیت‌های اجتماعی، سیاسی، و فرهنگی موجود می‌تواند در پیش‌گیری از جرایم در این زمینه و نیز رعایت منطق و انصاف در جرم‌انگاری بسیار مهم و اثربخش باشد.

مقایسهٔ قانون فدرال حمایت از دادهٔ آلمان با قوانین ایران در زمینهٔ حمایت از داده‌های شخصی نشان می‌دهد که حقوق ایران، به‌لحاظ بی‌توجهی به برخی اصول حاکم‌بر داده‌های شخصی، کامل نبودن اصول پیش‌بینی‌شده، و ارجاع برخی دیگر به آیین‌نامه‌های گوناگون نقایص جدی دارد که باید از سوی مقنن بازنگری شود. از سوی دیگر، فقدان مقررات جامع در زمینهٔ حمایت از حریم خصوصی مانع از درک و اجرای صحیح حمایت از داده در دادگاه‌ها و مراجع اداری می‌شود. «لایحهٔ حریم خصوصی» که برای تصویب به مجلس شورای اسلامی ارائه شده این ایرادات را تا حدودی برطرف کرده است که در صورت تصویبْ خلأها و نواقص موجود تا حدودی مرتفع می‌شود. علاوه‌بر آن‌چه گفته شد، مقررات حقوق ایران ناظر بر حمایت از داده‌های شخصی، از حیث مصادیق داده‌های مورد حمایت و ضمانت اجراهای کیفری، نیز ایراداتی دارد که بحث و بررسی‌های مفصل و مستقلی را می‌طلبد.

پی‌نوشت‌ها

۱. به‌منظور آشنایی با این مفاهیم ← حسینی و ظریف‌منش، ۱۳۹۲: ٤١–٦٨.

۲. مادهٔ ۷۸: هر گاه در بستر مبادلات الکترونیکی بر اثر نقص یا ضعف سیستم مؤسسات خصوصی و دولتی، به‌جز در نتیجهٔ قطع فیزیکی ارتباط الکترونیکی، خسارتی به اشخاص وارد شود، مؤسسات مزبور مسئول جبران خسارات واردشده است مگر این‌که خسارات واردشده ناشی از فعل شخصی افراد باشد که در این صورت جبران خسارات بر عهدهٔ این اشخاص خواهد بود.

۳. مادهٔ ۷۳: اگر به‌واسطهٔ بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرایم راجع به «دادهٔ پیام»های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل ۵۰ میلیون ریال محکوم می‌شود.

٤. شنود در فضای سایبر به‌معنای دریافت داده‌های در حال انتقال یا به هر نحوی دسترسی به آن‌هاست. منظور از داده نیز در قانون فوق هر نمادی از اطلاعات یا مفاهیم قابل پردازش در سیستم رایانه‌ای یا مخابراتی است و گسترهٔ مصادیق آن بسیار وسیع است. منظور از ارتباطات غیرعمومی ارتباطاتی است که مرئی و در منظر عموم نباشد و همگان از محتوای داده‌های در حال انتقال اطلاع نیابند.

۵. اختصار ISP برگرفته از اصطلاح Internet Service Provider یعنی شرکت خدمات سرویس‌های اینترنت است. یک ISP از طریق یک خط تلفن از شرکت مخابرات و یا امکانات ماهواره‌ای می‌تواند اینترنت را به User خود سرویس دهد.

کتاب‌نامه

اصلانی، حمیدرضا (١٣٨٤). «اصول حاکم بر حمایت از داده»، *مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات*، تهران: معاونت حقوقی و توسعهٔ قضایی قوهٔ قضاییه، مرکز مطالعات توسعهٔ قضایی.

باستانی، برومند (١٣٨٦). *جرایم رایانه‌ای و اینترنتی جلوه‌ای نوین از بزهکاری*، تهران: نشر میزان.

پاکزاد، بتول (١٣٨٨). «تروریسم سایبری»، رسالهٔ دکتری حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق دانشگاه شهید بهشتی.

جلالی فراهانی، امیرحسین (١٣٨٩). *کنوانسیون جرایم سایبر و پروتکل الحاقی*، *معاونت حقوقی و توسعهٔ قضایی قوهٔ قضائیه*، تهران: خرسندی.

حسنی، جعفر (١٣٨٥). «حمایت کیفری از حریم خصوصی در فضای سایبر»، پایان‌نامهٔ کارشناسی ارشد، گرایش حقوق جزا و جرم‌شناسی، دانشگاه شهید بهشتی، دانشکدهٔ حقوق.

حسینی، پرویز و حسین ظریف‌منش (١٣٩٢). «مطالعهٔ تطبیقی ساختار دفاع سایبری کشورها»، *فصل‌نامهٔ پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین (ع)*، س ٢، ش ۵.

زراعت، عباس (١٣٨٦). *قانون مجازات اسلامی در نظم حقوقی کنونی*، تهران: ققنوس.

زرکلام، ستار (١٣٨٦). «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیهٔ اروپا)»، *مجلهٔ معارف اسلامی و حقوق*، س ٨، ش ١.

شاملو احمدی، محمدحسین (١٣٨٦). *فرهنگ اصطلاحات و عناوین جزایی*، تهران: دادیار.

عامل نجف‌آبادی، محمد (١٣٨٧). «جرم‌انگاری در فضای مجازی»، پایان‌نامهٔ کارشناسی ارشد، گرایش حقوق جزا و جرم‌شناسی، دانشگاه شهید بهشتی، دانشکدهٔ حقوق.

نوبهار، رحیم (١٣٨٧). *حمایت حقوق کیفری از حوزه‌های عمومی و خصوصی*، تهران: جنگل.

نوری، محمد و رضا نخجوانی (١٣٨٣). *حقوق حمایت داده‌ها*، تهران: کمیتهٔ مطالعات حقوق فنّاوری ریاست جمهوری.

نیسی، جمیل و نضال مدحج (۱۳۹۰). «بررسی حریم خصوصی و حمایت داده‌های محیط سایبری در مقررات کیفری ایران با نگاهی تطبیقی به مقررات کیفری کشورهای آلمان، انگلستان و ایتالیا»، *ملی‌شهر الکترونیک*، همدان: دانشگاه آزاد اسلامی.

ویلیامز، ماتیو (۱۳۹۱). *بزهکاری مجازی؛ بزه، انحراف و مقررات‌گذاری برخط*، ترجمهٔ امیرحسین جلالی فراهانی و محبوبه منفرد، تهران: بنیاد حقوقی میزان.

Clavijo, Paola (2013). *Legislation Concerningdata Protection*, Befine Solutions AG.

Federal Data Protection Act Available in: <http://www.gesetze-im-internet.de/englisch_bdsg/>.

Geiger, Jutta (2003). "The Transfer of Data Abroad by Private Sector Companies: Data Protection Under the German Federal Data Protection Act", *German Law Journal*, Vol. 4, No. 8.

Mutula, Stephen M. (2007). *Web Information Management*, UK: Cahndos Publication.

Zavrsnik, Ales (2008). "Cybercrime Definitional Challenge and Criminological Particularities", *Masaryk University Journal of Law and Technology*.