رسانه و فرهنگ، پژوهشگاه علوم انسانی و مطالعات فرهنگی
سال ششم، شمارهٔ اول، بهار و تابستان ۱۳۹۵، ۱ – ۱۷

مطالعهٔ تطبیقی جرایم علیه حریم خصوصی در فضای سایبری ایران و آلمان

زهرا احمدی ناطور*
حسین آقابابایی**

چکیده

با ورود به عصر فناوری اطلاعات و ارتباطات، به تدریج مسایل و دشواری‌های نوینی در ارتباط با 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 می‌باشد. اغلب کشورها از جمله آلمان دارای قوانین حمایت از داده هستند اما برخی از کشورها نظیر ایران فاقد قانونی جامع و منسجم در این زمینه می‌باشند. از این رو هدف از تحقیق حاضر مقایسه جرایم علیه حریم خصوصی در فضای سایبری بین ایران و آلمان می باشد. مقایسه مذکور نشان می‌دهد که حقوق ایران به لحاظ فقدان برخی از اصول حاکم بر داده های شخصی، کامل نبودن اصول پیش بینی شده و ارجاع برخی دیگر به آیین نامه های مختلف، دارای نقایص جدی است که باید از سوی مقنن مورد بازنگری قرار گیرد. از سوی دیگر، فقدان مقررات جامع در زمینه حمایت از حریم خصوصی مانع از درک و اجرای صحیح حمایت از داده در دادگاه‌ها و مراجع اداری می‌گردد. «لایحه 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 نقائص تا حدی رفع می‌گردند.

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

---

* 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

۱- مقدمه

فضای سایبر(Cyberspace) گستره ای است که در کنار دنیـای فیزیکـی و جـدا از آن قـرار دارد. این محیط عبارتست از یک واقعیت مفهومی مشترک که با مسامحه آن را

«دنیای مجازی» نیز می‌نامند. این فضا که شناخته شده ترین بخش آن «اینترنـت» اسـت برای تسهیل ارتباطات طراحی شده و امروزه نیز در این کاربرد تکیه دارد. در این فضـا هـر آنچه که رخ می‌دهد به وسیله داده‌ها صورت می‌گیرد(دزیانی، ۱۳۸٦: ۸٦) و آنچه که در این فضا مبادله می‌شود داده‌ها هستند(باستانی، ۱۳۸٦: ۵۵). بنا به تعریفی، «فضای سـایبر» یعنـی آنچه از مجموعه ذخیره و انتقال داده های الکترونیکی به وجود می‌آید(Kabay, 2002: 53). بنابراین، «حریم خصوصی در فضای سایبر» بر مبنای داده‌ها باز تعریف شده است و مفهوم «حمایت از داده های شخصی» جایگزین عنوان «حریم خصوصی در فضـای سـایبر» شـده است(اصلانی، ۱۳۸٤(ب): ۵۱). مهم‌ترین اشکال تجاوز به حریم خصوصی در فضای سایبر با نقض قواعد پایه ای حمایت از داده که متشکل از دو قسمت عمده‌ی «اصول به‌کـارگیری داده‌ها» و «حقوق اطلاعاتی موضوع داده‌ها» سـت رخ مـی‌دهـد(حسـنی، ۱۳۸۵: ۳۵). ایـن اصول در حقیقت، شکل ساختاربندی شده‌ی حقوق ماهوی شهروندان نسبت به داده هـای شخصی‌شان می‌باشد. برای تضمین این حقوق ماهوی، تعریف یکسری حقـوق اطلاعـاتی برای اشخاص و در مقابل آن یکسـری تکـالیف بـرای کنتـرل‌گـران و پـردازش‌گـران لازم می‌نماید. عدم رعایت این حقوق و تکالیف متناظر آن‌ها، بخش عمـده ای از جـرایم علیـه حریم خصوصی در فضای سایبر را تشکیل می‌دهد(همان: ۱۳۵).

در دهه های اخیر، امکانات توسعه یافته‌ی جمع آوری، ذخیره سازی، دستیابی، تطبیـق، انتخاب، اتصال و انتقال داده‌ها که به وسیله‌ی فناوری‌های نوین به وجود آمده است، موجب خطرناک‌تر شدن تهدیدها نسبت به حقوق فردی شده اسـت(Kelleher & Murray, 1999: 223). بهره گیری از ابزار های فنی موجود به منظور حمایـت از داده‌هـا نظیـر فیلتـر کـردن و رمزنگاری ضروری و مفید هستند ولی به هیچ وجه کافی نیستند. برای حمایت کافی و مـؤثر از حریم خصوصی داده های شخصی در ارتباطات الکترونیکی از جمله اینترنت وجود قواعد حقوقی متناسب با چنین حمایتی اجتنـاب ناپـذیر هسـتند(زر کـلام، ۱۳۸٦: ۱۷٤). مباحـث حقوقی راجع به تهدیدهای حاصل از فناوری‌های پیشـرفته کـامپیوتری نسـبت بـه حـریم خصوصی پیش از مباحث حقوقی راجع به مسایل اقتصـادی در ایـن بسـتر، شـکل گرفتـه است؛ در نتیجه همکاری‌های بین‌المللی و به تبع آن هماهنگی بیشـتری در قـوانین داخلـی

کشورها به چشم می‌خورد(دزیانی، ۱۳۷٦: ۲۵ و ۲٦ و زیبر، ۱۳۸۳: ۱٦۸). علیرغم این مشابهت‌ها، تفاوت‌های زیادی هم در این قوانین دیده می‌شود. این تفاوت‌ها مربوط به پوشش یا عدم پوشش داده های اشخاص حقوقی، تفاوت در روش داده پردازی(خودکار یا ثبت دستی)، تفاوت در شرایط مشروعیت پردازش یا شروع پردازش به صورت شکلی یا ماهوی می باشد. با این حال تفاوت عمده‌ی بین قوانین، به منطق تقنینی و اعمال غیر قانونی جرم انگاری شده توسط آن‌ها بر می‌گردد. این تفاوت‌ها ناشی از اختلاف رویکرد نسبت به حریم خصوصی نیست؛ بلکه ناشی از تفاوت ارزیابی‌ها از خصیصه‌ی کیفری نقض حریم خصوصی و نقشی است که حقوق کیفری باید در این زمینه به عهده گیرد. در حالی که در برخی کشورها مانند آمریکای شمالی و نیز هلند در اروپا و ژاپن در آسیا، استفاده از مقررات کیفری در حمایت از داده‌ها بسیار کم است در مقابل، قوانین مربوط به حریم خصوصی در بسیاری از کشورهای اروپایی، فهرست‌های جامعی از تخلفات کیفری را در بر دارند. در حقوق ایران، تاکنون مقررات خاصی برای حمایت از حریم خصوصی وجود نداشته و لایحه ای که در سال‌های اخیر در این زمینه تدوین شده نیز هنوز به تصویب نرسیده است. با این حال، حمایت از داده های شخصی برای نخستین بار در قانون تجارت الکترونیکی مصوب سال ۱۳۸۲ و پس از آن در قانون جرایم رایانه ای مصوب سال ۱۳۸۸مورد توجه قرار گرفته است. هر چند چنین حمایت‌هایی را باید به فال نیک گرفت، لیکن این مقررات در مقایسه با مقررات سایر کشورها و مقررات سازمان‌های بین‌المللی در این خصوص، دارای نواقص و ایرادات جدی است. در مقاله حاضر، با توجه به سیستم حقوقی ایران و با تاکید بر قوانین برخی کشورهای اروپایی مانند آلمان که دارای رویکرد حمایت جامع از حریم خصوصی هستند، به مطالعه تطبیقی جرایم علیه حریم خصوصی در فضای سایبری ایران و آلمان خواهیم پرداخت.

۲- جرایم علیه حریم خصوصی در فضای سایبری در قانون فدرال آلمان

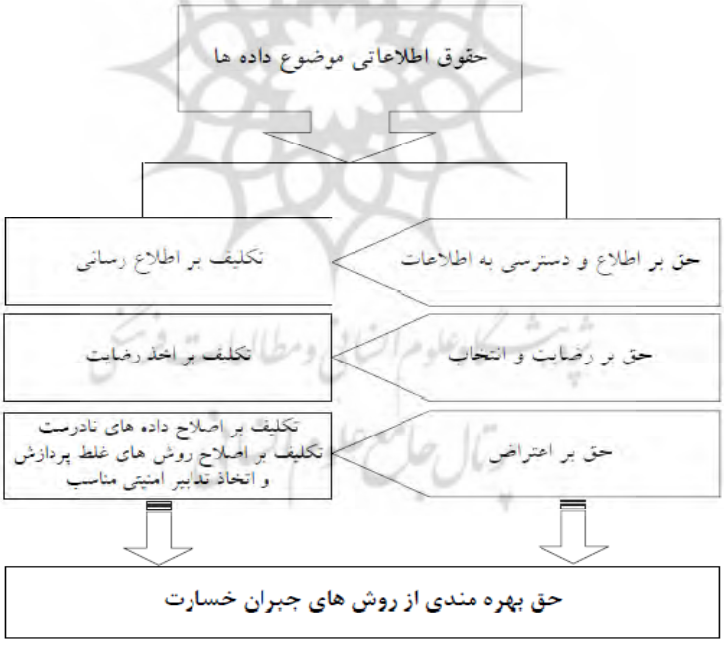
۲-۱- نقض اصول اولیه به‌کارگیری داده‌ها

اصول اولیه به‌کارگیری داده‌ها، بخش اول الزامات اساسی در حمایت از داده های شخصی است. مطالعه‌ی تطبیقی قوانین کشورهای مختلف اروپایی نشان می‌دهد که نقض این اصول، بخش عمده ای از جرایم کیفری در نقض حریم خصوصی در فضای سایبر را تشکیل می‌دهد. رئوس این جرایم را می‌توان بدین شرح بر شمرد: ۱) افشاء، انتشار، تهیه‌ی

غیر قانونی یا دستیابی غیر قانونی به داده‌ها، ۲) استفاده‌ی غیر قانونی از داده‌ها، ورود، تغییر یا کذب سازی غیر قانونی داده‌ها با قصد ایراد خسارت، ۳) جمع آوری یا ذخیره سازی داده‌ها که به دلایل ماهوی غیر قانونی است، ٤) ذخیره سازی داده های غیر صحیح که در بیشتر کشورها به وسیله‌ی قوانین اضافی در خلال قوانین مربوط به حقوق فردی تحت پوشش قرار گرفته است. حدود و وسعت و شرایط این جرایم از کشوری به کشور دیگر متفاوت است و در همه‌ی کشورها، همه‌ی این عناوین جرم انگاری نشده است.

۲-۲- نقض حقوق اطلاعاتی موضوع داده‌ها

حقوق اطلاعاتی موضوع داده‌ها، به عنوان قسمت دوم الزامات اساسی حمایت از داده‌ها برای تضمین حق حریم خصوصی شهروندان، به حدی حائز اهمیت است که نقض آن‌ها دسته‌ی مهمی از جرائم علیه حریم خصوصی در فضای سایبر را به وجود می‌آورند. این حقوق ذیلاً به صورت نمودار ۱ نشان داده شده است.



نمودار ۱- حقوق اطلاعاتی موضوع داده‌ها

مهم‌ترین موارد نقض حقوق اطلاعاتی اشخاص عبارتند از: ۱) اطلاعات کذب یا عدم اطلاع در همه‌ی موارد ثبت شده، ۲) پاسخ‌های کذب یا عدم جواب به تقاضای به عمل آمده برای حق دستیابی فرد، ۳) عدم اخذ رضایت در موارد لزوم و بی توجهی نسبت به رد پردازش یا شرایط مقرر از جانب موضوع داده‌ها، ٤) بی اعتنایی به اعتراض موضوع داده‌ها و عدم تصحیح داده های نادرست یا عدم اصلاح روش پردازش.

با توجه به نمودار ۱، جرایم این طبقه را در ۳ دسته بررسی خواهیم کرد.

۲-۲-۱- نقض اطلاع یا دسترسی به اطلاعات

موضوع داده‌ها حق دارد که قبل از جمع آوری هر گونه اطلاعات شخص درباره‌ی وی، از این امر مطلع شود. در این راستا هویت کنترل گر یا نماینده‌ی وی، اهداف پردازش و نوع داده‌هایی که جمع آوری خواهند شد، افرادی که داده های شخصی برای ایشان افشاء خواهد شد و نیز حقوق موضوع داده‌ها در مراحل مختلف به‌کارگیری داده‌ها بایستی به اشخاص اطلاع داده شود. هر گونه اطلاعات دیگر که برای تضمین منافع موضوع داده‌ها لازم است و به موجب قانون مقرر می‌شود بایستی به اطلاع وی برسد. در صورتی که داده‌ها از شخص ثالث تحصیل شود یا گردآورنده امکان عملی اطلاع رسانی را نداشته باشد، بایستی امکان دسترسی شخص به اطلاعات فوق را با یک روش آسان و ارزان فراهم آورد. این حق در تمام مراحل به‌کارگیری داده برقرار است. تکلیف متناظر این حق مبنی بر اطلاع رسانی بر عهده‌ی کنترل گر و هر شخص دیگری که داده های شخصی را پردازش می‌کند می‌باشد. نقض این حق در قوانین حمایت از داده‌ها، جرم انگاری شده است(اصلانی، (الف)١٣٨٤: ١١). ماده ۱۹ قانون فدرال حمایت از داده آلمان مقرر می‌دارد: در صورت درخواست شخص سوژه، اطلاعات زیر باید در اختیار او قرار گیرد:

الف- داده های ذخیره شده در خصوص او از جمله منبع و مقصد احتمال آن‌ها

ب- هدف از ذخیره سازی داده‌ها

این ماده لزوم رایگان بودن ایفای تعهد را نیز مقرر می‌دارد. همچنین به موجب ماده ۲۰ این قانون، لزوم تصحیح، امحاء و توقیف داده های شخصی ناصحیح مقرر گردیده است. به علاوه این قانون، یک جرم اداری را خواه عامداً خواه با بی احتیاطی ارتکاب یافته باشد در موارد زیر وضع می‌کند:

ـ نقض حق اطلاع و دسترسی به اطلاعات در مورد استفاده از داده های شخصی در زمینه‌ی بازاریابی و تبلیغات تجاری(بند ۳ ماده (۱)٤٣ قانون فدرال حمایت از داده آلمان)

ـ نقض حق اطلاع شخص یا عدم انجام صحیح و کامل آن(بند ۸ ماده (۱)۴۳ قانون فدرال حمایت از داده آلمان)

البته اجرای مطلق این حق، ضمن اینکه می‌تواند مانع جریان آزاد اطلاعات باشد در موارد عدیده‌ای نیز به لحاظ عقلی، امکان پذیر نیست و یا لازم به نظر نمی‌رسد. بنابراین همواره استثنائاتی در قوانین بر آن وارد شده است مثلاً مطابق ماده (٤)۱۹ قانون حمایت از داده آلمان، قانونگذار در مواردی مانند پردازش برای منافع عمومی مهم مثل امنیت ملی، دفاع، سلامت عمومی، اهداف تحقیقاتی علمی، آماری و تاریخی و نیز اهداف هنری، ادبی یا روزنامه نگاری در راستای آزادی بیان و یا ذخیره و پردازش برای اهداف صرفاً شخصی می‌تواند این استثنائات را توسعه دهد. این استثنائات در راستای ایجاد توازن میان منافع عمومی و حقوق فردی است و بایستی به میزان ضرورت و به صورت صریح پیش بینی شوند و تا حدی گسترده نشوند که از اصل، چیزی باقی نگذارند. تکلیف متناظر این حق، تکلیف اطلاع رسانی از سوی کنترل گر یا اشخاص مرتبط دیگر است(ماده (۳)٤ قانون حمایت از داده آلمان).

۲-۲-۲- نقض حق رضایت و انتخاب

گردآورنده‌ی داده‌ها باید این امکان را برای موضوع داده‌ها فراهم آورد که وی صریحاً نظر خود را مبنی بر اینکه با گردآوری داده های شخصی خود موافق است یا خیر اعلام کند و همچنین پس از اطلاع شخص از تصمیم کنترل گر مبنی بر جمع آوری اطلاعات شخصی مربوط به وی، بتواند عدم رضایت خود را اعلام کند و از جمع آوری ممانعت نماید. در صورت رضایت، شخص می‌تواند حدود جمع آوری اطلاعات، نحوه‌ی پردازش و حدود افشا و انتقال را تعیین کرده و رضایت خود را محدود به حوزه‌ی مشخص شده نماید. این حق نیز در تمام مراحل به‌کارگیری داده برقرار است و نقض آن باعث ایجاد جرایمی در قانون حمایت از داده شده است(عامل نجف آبادی، همان: ۸۲). در قانون فدرال حمایت از داده آلمان یک جرم اداری مبنی بر نقض حق رضایت در مورد استفاده از داده های شخصی در زمینه‌ی بازاریابی و تبلیغات تجاری پیش بینی شده است. این قانون همچنین در ماده (۱)٤a مقرر کرده است که رضایت سوژه بایستی به صورت کتبی اعلام شود مگر اینکه قانون طور دیگری مقرر کرده باشد.

۲-۲-۳- نقض حق اعتراض

اگر در نتیجه‌ی اطلاعاتی که کنترل گر در اختیار موضوع داده‌ها قرار می‌دهد یا به هر روش دیگر شخص مطلع شود که داده های جمع آوری شده، از وی یا داده های در حال پردازش یا انتقال او، نادرست یا ناقص یا قدیمی هستند، حق اعتراض بـه دارنـده‌ی داده‌هـا را دارد. حق اعتراض برای موضوع داده‌ها در تمام مواردی که کنتـرل گـر از اصـول پـردازش داده تخطی می‌کند نیز برقرار است. اگر این اعتراض موجه و منطقی باشد، باعث ایجاد تکلیفـی بر عهده‌ی کنترل گر مبنی بر اصلاح، پاک کردن یا متوقـف سـازی داده هـای نادرسـت یـا اصلاح روش پردازش یا توقف پردازش غیر مجاز می‌شود. نقض این حق با عدم توجه بـه آن و عدم رعایت تکلیف بر اصلاح، موجب پیش بینی جرایمی در قـوانین حمایـت از داده شده است. بر اساس مواد ۲۰ و ۳۵ قانون حمایت از داده آلمان، داده های نادرست بایسـتی تصحیح شود و اگر کار ذخیره داده‌ها ناموجه باشد یا دانستن آن‌هـا بـرای اجـرای وظـایف کنترل گر لازم نباشد، بایستی پاک شود و اگر پاک کردن داده در آن زمان طبق قانون مجـاز نباشد یا مضر به منافع مهم دیگران باشد یا پاک کردن عملاً غیـر ممکـن باشـد یـا مسـتلزم تلاش بیش از حد معقولی باشد، بایستی بلوکه شود. در این قانون همچنین یک جرم اداری مبنی بر نقض حق اعتراض در مورد استفاده از داده های شخصـی در زمینـه‌ی بازاریـابی و تبلیغات تجاری پیش بینی شده است(بند ۳ ماده (۱)۴۳ قانون فدرال حمایت از داده آلمان). همچنین انتقال دادن داده‌ها به شخص ثالث بدون صادر کـردن اعلامیـه‌ی متقابـل در برابـر اعتراض موضوع داده‌ها (نقض حق اعتراض موضوع داده‌ها با عدم توجه به آن) بـه عنـوان یک جرم اداری در نظر گرفته شده است(بند ۹ مـاده (۱)۴۳ قـانون فـدرال حمایـت از داده آلمان).

۲-۳- حق بهره‌مندی از جبران خسارت

هر جا که حقی مشروع برای شخصی مقرر شود این وظیفه قـانون اسـت کـه بـا ضـمانت اجراهای متناسب از آن حمایت کند. این حق در موارد تجاوز از اصـول پـردازش داده نیـز جریان دارد و شخص می‌تواند به دلیل نقض حقوق ماهوی خود تقاضای جبران خسـارت داشته باشد. در کشورهای مختلف، بهره‌مندی از جبران خسارت در موارد تجاوز به حقـوق شخصیت امری پذیرفته شده است. این مسئولیت در قبال اعمال غیر قابل توجیه و نادرست ایجاد می‌شود. مطابق ماده ۷ قانون حمایت از داده آلمان، اگر شخصی که خسـارت بـه بـار

آورده است ثابت کند مراقبت‌های لازم را چه به لحاظ فنی و چه به لحاظ حقوقی صورت داده است مسئول نخواهد بود. همچنین ماده 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 پیش بینی می‌کند.

در حقوق داخلی ایران مواد ۷۱ الی ۷۳ و ۷۸ قانون تجارت الکترونیکی ضمانت اجراهای کیفری خاصی را برای تضمین اجرای صحیح مقررات مربوط به حمایت از داده این قانون پیش بینی نموده است اما حکم ماده ۷۸ تنها ناظر بر مسئولیت مدنی قهری بوده و منصرف از مسئولیت مدنی قراردادی می‌باشد و لذا در مواردی که ایراد خسارت ناشی از نقض مفاد یک تعهد قراردادی باشد، مبنای مسئولیت متعهد متخلف، رابطه قراردادی فی مابین می‌باشد که بر طبق قواعد حقوق قراردادها اعمال می‌گردد. همچنین متن این ماده به گونه ای تنظیم شده است که تنها موارد خاصی از علل ورود خسارت را شامل می‌گردد و شمول و گستره کافی ندارد. فی‌الواقع حکم مقرر در ماده موهم این معناست که در حوزه مسئولیت مدنی قهری ناشی از تخلف از مقررات مربوط به حمایت از داده نمی‌توان به قواعد عام مسئولیت مدنی استناد نمود و تنها در حدود مقرر در این ماده می‌توان حکم به جبران خسارت داد.

۳- بررسی جرایم علیه حریم خصوصی در فضای سایبر در قوانین موضوعه ایران

۳-۱- قانون تجارت الکترونیک مصوب ۱۳۸۲

یکی از بحث‌های عمده در تجارت الکترونیک بحث حمایت از داده های شخصی است. اطلاعات همواره در تجارت نقش بسیار مهمی دارد. بازاریابی، تعیین زمان و مکان خرید و فروش اجناس و تمام فعالیت‌های مرتبط با تجارت رابطه نزدیکی با اطلاعات دارد. بخشی از این اطلاعات، داده های شخصی طرف‌های تجاری و نیز مصرف کنندگان می‌باشد. برای انجام مبادلات تجاری بین‌المللی، کشورهای پیشرو اقتصادی، چنین داده‌هایی را به کشورهایی که فاقد سطح حمایت کافی هستند انتقال نمی‌دهند و این امر می‌تواند باعث تحریم اطلاعاتی و کاهش توان بازیابی و ارزیابی‌های دیگر تجار در کشورهای تحت تحریم اطلاعاتی شود. حمایت از داده های شخصی حتی در تجارت‌های داخلی نیز حائز اهمیت است. از این رو مقنن در چند ماده از قانون تجارت الکترونیکی به بحث «حمایت از داده‌ها» پرداخته است که مهم‌ترین این مواد عبارتند از:

ماده ۵۸: ذخیره، پردازش و یا توزیع داده پیام شخصی مبین ریشه های قومی یا نـژادی، دیدگاه های عقیدتی مذهبی، خصوصـیات اخلاقـی و داده پیـام‌هـای راجـع بـه وضـعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیـر قـانونی است. این ماده به ظاهر، رعایت اصل تحصیل قانونی و مبتنی بر رضایت سوژه یـا شـخص موضوع گردآوری و پردازش را مورد تاکید قرار داده است لیکن باید توجه داشت کـه واژه «ذخیره» که در این ماده، از مصادیق اعمال ممنوع تلقی شده است را به هیچ وجه نمی‌تـوان مرادف با اصطلاح «گردآوری» تلقی کرد. زیرا گردآوری ناظر بر مرحله تحصـیل داده‌هـا و ذخیره ناظر بر مرحله نگهداری داده‌هاست. لذا در حقوق ایران نمی‌توان قائل به ممنوعیـت گردآوری غیرمجاز داده‌ها بود.

ماده ۵۹: در صورت رضایت شخص موضوع داده پیام نیز به شرط آن که محتـوای داده پیام بر وفق قوانین مصوب مجلس شورای اسلامی باشـد، ذخیـره، پـردازش و توزیـع داده پیام‌های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:

الف: اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند.(اصـول تحصـیل، نگهداری و پردازش محدود و مرتبط)

ب: داده پیام باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمـع آوری برای شخص موضوع داده پیام شرح داده شده جمع آوری گردد و تنها برای اهداف تعیـین شده مورد استفاده قرار گیرد.(اصول تحصیل و پردازش محدود و مرتبط)

ج: داده پیام باید صحیح و روزآمد باشد.(اصل درستی یا صـحت داده هـای گـردآوری شده)

د: شخص موضوع داده پیام باید به پرونده های رایانه ای حاوی داده پیام‌های شخصـی مربوط به خود دسترسی داشته و بتواند داده پیام‌های ناقص و یا نادرست را محو یا اصـلاح کند.(اصل حق اطلاع و دسترسی به اطلاعات برای سوژه)

ه: شخص موضوع داده پیام باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه ای داده پیام شخصی مربوط به خود را بنمایـد.(اصـل حـق امحـاء برای سوژه)

ماده ۶۰: ذخیره، پردازش و یا توزیـع «داده پیـام» هـای مربـوط بـه سـوابق پزشـکی و بهداشتی تابع آیین نامه ای است که در ماده ۷۹ این قانون خواهد آمد.

ماده ٦١: سایر موارد راجع به دسترسی موضوع «داده پیام» از قبیل استثنائات، افشای آن برای اشخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسئول دیدبانی و کنترل جریان «داده پیام» های شخصی به موجب مواد مندرج در باب چهارم این قانون و آیین نامه مربوطه خواهد بود.

ماده ٦٤: به منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبادلات الکتریکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسسات برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم محسوب و مرتکب به مجازات مقرر در این قانون خواهد رسید.(اصول تحصیل مشروع و مجاز داده‌ها و افشاء و انتقال مشروع و مجاز داده‌ها)

ماده ۷۱: هرکس در بستر مبادلات الکترونیکی شرایط مقرر در مواد (۵۸) و (۵۹) این قانون را نقض نماید مجرم محسوب و به یک تا سه سال حبس محکوم می‌شود.

ماده ۷۲: هرگاه جرایم راجع به «داده پیام» های شخصی توسط دفاتر خدمات صدور گواهی الکترونیکی و سایر نهادهای مسئول ارتکاب یابد، مرتکب به حداکثر مجازات مقرر در ماده (۷۱) این قانون محکوم خواهد شد.

ماده ۷۳: اگر به واسطه بی مبالاتی و بی احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرایم راجع به «داده پیام» های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل ۵۰ میلیون ریال محکوم می‌شود.

ماده ۷۵: متخلفین از ماده (٦٤) این قانون و هرکس در بستر مبادلات الکترونیکی به منظور رقابت، منفعت و یا ورود خسارت به بنگاه های تجاری، صنعتی، اقتصادی و خدماتی با نقض حقوق قراردادهای استخدام مبنی بر عدم افشای اسرار شغلی و یا دستیابی غیر مجاز، اسرار تجاری آنان را برای خود تحصیل نموده و یا برای اشخاص ثالث افشا نماید به حبس از شش ماه تا دو سال و نیم و جزای نقدی معادل ۵۰ میلیون ریال محکوم خواهد شد.(اصول تحصیل مشروع و مجاز داده‌ها و افشاء و انتقال مشروع و مجاز داده‌ها)

ماده ۷۸: هرگاه در بستر مبادلات الکترونیک در اثر نقص یا ضعف سیستم مؤسسات خصوصی و دولتی، به جز در نتیجه قطع فیزیکی ارتباط الکترونیکی، خسارتی به اشخاص وارد شود مؤسسات مزبور مسئول جبران خسارت وارده می‌باشند مگر اینکه خسارات وارده ناشی از فعل شخصی افراد باشد که در این صورت جبران خسارات بر عهده این اشخاص خواهد بود.(اصل حق بهره‌مندی از جبران خسارت)

همان‌گونه که ملاحظه می‌شود مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی در زمینه داده های شخصی، برخی از اصول ناظر بر حمایت از حریم خصوصی داده‌ها و اطلاعات شخصی در محیط الکترونیکی را مورد توجه قرار داده است. از آن جمله می‌توان به اصل تحصیل قانونی و مبتنی بر رضایت سوژه یا شخص موضوع گردآوری و پردازش (ماده ۵۸)، اصل تحصیل مضیق و مرتبط (بند های الف و ب ماده ۵۹)، اصل درستی یا صحت داده های گردآوری شده(بند ج ماده ۵۹)، اصل دسترسی (بند د ماده ۵۹) و اصل امحا (بند ه ماده ۵۹) اشاره کرد. با این حال، برخی از اصول دیگر که از جمله در حقوق اروپایی و مقررات برخی کشورها به آن‌ها تصریح شده، در حقوق ایران مورد توجه قانون گذار قرار نگرفته است. از آن جمله می‌توان به اصل انتخاب، اصل امنیت، اصل شفاف سازی، اصل ممنوعیت افشاء، اصل پردازش مرتبط و اصل عدم انتقال اشاره کرد. هر چند، قانون گذار ایرانی برخی از اصول حاکم بر داده های شخصی را مورد تصریح قرار داده است، با این حال گاه همه مقتضیات آن اصل در مقررات موضوع مواد ۵۸ تا ٦١ قانون تجارت الکترونیکی پیش بینی نشده است. به عنوان مثال، در خصوص اصل قانونی بودن و لزوم تحصیل رضایت سوژه، هر چند ضرورت آن در ماده ۵۸ به صراحت ذکر شده است ولی مستثنیات آن پیش بینی نشده و با توجه به ماده ٦١ آن قانون به آیین نامه واگذار شده است. ارجاع مستثنیات حمایت از داده های شخصی به آیین نامه جای تأسف دارد، زیرا این مستثنیات هم به اندازه خود اصل از اهمیت برخوردار هستند و باید در قالب قانون پیش بینی شود تا از هر گونه سوءاستفاده احتمالی جلوگیری شود. همچنین توجه به مفاد بند اخیر ماده ۵۹ مبین آنست که صرف نظر از انشاء ناصواب و غیر حقوقی ماده، با توجه به اطلاق و عموم عبارات به کار رفته در قانون که مفید شمول آن نسبت به همه مؤسسات و نهادها (حتی دولتی و عمومی) می‌باشد، این حکم به هیچ وجه توجیه و حتی امکان اجرا ندارد و از مصادیق افراط و تفریط قانونگذار در امر حمایت از داده می‌باشد. در مورد ماده ۷۳ این قانون نیز نکاتی قابل ذکر است: ۱- مجازات مقرر در این ماده تنها اختصاص به فرضی دارد که جرم ارتکابی ناشی از بی مبالاتی و بی احتیاطی دفاتر خدمات صدور گواهی الکترونیکی باشد نه مطلق اشخاصی که داده های شخصی افراد را در اختیار دارند. ۲- مجازات مقرر در این ماده تنها ناظر بر فرضی است که به واسطه بی مبالاتی و بی احتیاطی مؤسسات مورد بحث، جرمی راجع به داده پیام‌های شخصی روی دهد و در هر مورد که نقض حقوق سوژه یا اصول حاکم بر قانون صورت پذیرد کارایی ندارد.

در مقابل، قانون فدرال حمایت از داده آلمان، مقررات صریح و روشنی را در قالب قانون در خصوص وظایف و اختیارات و نیز مسئولیت‌های اشخاصی که به گـردآوری و پـردازش داده های شخصی می‌پردازند وضع نموده و به این ترتیب روابط حقـوقی تمـامی اشـخاص دست‌اندرکار و ذینفع را مشخص کرده است. حقوق ایران متأسفانه از این حیـث نیـز دارای ایراد است، زیرا بر اساس ماده ٦١ قانون تجارت الکترونیک در این زمینه هـم بـه آیـین نامـه ارجاع شده است. بدیهی است امکان پیش بینی مقررات آمره و ضمانت اجراها اعم از حقوقی و کیفری در چارچوب آیین نامه وجود ندارد.

۳-۲- قانون جرایم رایانه ای مصوب ۱۳۸۸

ماده ۱ این قانون، نقض اصل تحصیل مشروع و مجاز را جرم انگاری کرده و مقرر می‌دارد: «هر کس به طور غیر مجاز به داده‌ها یا سامانه های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است، دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جـزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد».ایـن ماده با هدف حمایت همه جانبه از اقدام اشخاص در اتخاذ تدابیر امنیتی برای سیستم یا داده های خود، دسترسی غیر مجاز را به صورت ساده جرم انگاری کرده است. در این راسـتا از آنجایی که هکرها و کراکرها دارای امکانات هستند و جزای نقدی صرف قدرت پیشـگیری ندارد مجازات حبس نیز پیش بینی شده است.

ماده ۲ این قانون نیز نقض اصل تحصیل منصفانه داده‌ها را جرم انگاری نمـوده و مقـرر می‌دارد: «هر کس به طور غیر مجاز محتوای در حال انتقال ارتباطات غیر عمومی در سامانه های رایانه ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا چهل میلیـون ریـال یـا هـر دو مجـازات محکوم خواهد شد».

شنود در فضای سایبر به معنای دریافت داده هـای در حـال انتقـال یـا بـه هـر نحـوی دسترسی به آن‌هاست. منظور از داده نیز در قانون فوق هـر نمـادی از واقعـه اطلاعـات یـا مفاهیم قابل پردازش در سیستم رایانه ای یا مخابراتی اسـت و گسـتره مصـادیق آن بسـیار وسیع است. منظور از ارتباطات غیر عمومی ارتباطی است که در مرئی و منظر عموم نباشـد و همگان از محتوای داده های در حال انتقال اطلاع نیابند(گزارش تـوجیهی لایحـه جـرایم رایانه ای، ص ٦، همان: ۱۹۷).

جرم ماده ۱۶ این قانون با نقض عامدانه اصل کیفیت داده های شخصی در مرحله پردازش و اصل پردازش صادقانه با تغییر داده های درست یا تولید داده های نادرست صورت می‌گیرد. بنابراین این تصاویر یا فیلم‌ها یا صداها ممکن است واقعی باشند و از روی نسخه واقعی به این شکل درآمده باشند یا غیر واقعی بوده ولی کاملاً شبیه به تصویر فیلم و صدای یک یا چند شخص معین باشند و اگر صدا یا تصویر یا فیلم با یکدیگر جمع شوند، تغییر یا تحریف یکی از آن‌ها برای تحقق موضوع مجرمانه با تحقق سایر شرایط کافی است(عامل نجف آبادی، همان: ۸۶). البته این جرم یک جرم مقید به نتیجه است و این عمل حتماً باید به صورت عرفی موجب هتک حیثیت شخص بشود تا قابل مجازات باشد. هرچند عموماً ناظران این صحنه‌ها این محتویات را به صاحبان اصلی آن‌ها منتسب نمی‌دانند اما این گونه محتویات موجب اهانت به اشخاص و تزلزل حرمت شخص می‌شود. فضای سایبر در این زمینه به اندازه ای مساعد است که اکنون هر تصویری را که در ذهن انسان می‌گنجد می‌توان در آن یافت. این ماده مقرر می‌دارد: «هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که صرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره: چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.»

ماده ۱۷ این قانون نیز نقض اصول راجع به افشاء و انتقال داده‌ها را جرم انگاری کرده و مقرر می‌دارد: «هر کس به وسیله سامانه های رایانه ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفا موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.»

لازم به ذکر است که در پیش نویس های لایحه این قانون، دامنه مصادیق اسرار شخصی گسترده تر بود ولی در متن قانون از شمول حمایت خارج شده‌اند و فقط صوت، تصویر و فیلم مشمول مواد فوق قرار گرفته‌اند. از نص این ماده بر می‌آید که شخص منتشر کننده بایستی رضایت شخص را قبل از انتشار صوت یا تصویر یا فیلم خصوصی یا خانوادگی

وی به دست آورد و این رضایت بایستی در زمان انتشار یا افشاء حاصل شده باشد و این تکلیف بر عهده منتشر کننده اطلاعات فوق است و نباید تصور شود که صاحب اسرار باید عدم رضایت خود را در انتشار یا در دسترس قرار دادن اسرار خصوصی به منتشر کننده اعلام نماید. این جرم نیز جرمی مقید است و باید ایراد ضرر یا هتک حیثیت عرفی در آن صورت گیرد(محسنی، همان: ۵۷۸). در حقیقت می‌توان گفت که این ماده، از حریم خصوصی به عنوان حریم خصوصی حمایت نکرده است، بلکه در صورتی که اعمال مذکور منجر به ضرر یا هتک حیثیت عرفی شخص گردد از حقوق وی حمایت می‌کند.

۳-۳- آیین نامه دفاتر خدمات حضوری اینترنت (Coffee net)

این دفاتر محلی برای ارائه خدمات دسترسی حضوری به شبکه های اطلاع رسانی (اینترنت و اینترانت) می‌باشند و مطابق بند ۷ آن، تجاوز به حریم خصوصی اطلاعاتی شهروندان، شنود و دسترسی غیرمجاز به داده‌ها از سوی آن‌ها ممنوع می‌باشد.

بند ۷: تولید و عرضه موارد زیر توسط شبکه‌های اطّلاعات رایانه‌ای ممنوع می‌باشد:

۱۵-۷- افشای روابط خصوصی افراد و تجاوز به حریم اطّلاعات شخصی آنان.

۱٦-۷- انتشار اطّلاعات حاوی کلیدهای رمز بانک‌های اطّلاعاتی، نرم‌افزارهای خاص، صندوق‌های پست الکترونیکی و یا روش شکستن آن‌ها.

۱۹-۷- هرگونه نفوذ غیر مجاز به مراکز دارنده اطّلاعات خصوصی و محرمانه و تلاش برای شکستن قفل رمز سیستم‌ها.

۲۱-۷- هرگونه تلاش برای شنود و بررسی بسته‌های اطّلاعاتی در حال گذر در شبکه که به دیگران تعلق دارد.

در مواد مذکور، نقض اصولی از قبیل اصل تحصیل مشروع و مجاز، اصل تحصیل منصفانه و اصول راجع به در دسترس قرار دادن داده‌ها جرم انگاری شده است.

۳-٤- آیین نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنت (ISP)[۲]

یک رسا(ISP)، اتصال به شبکه اطلاع رسانی و اینترنت را فراهم می‌آورد و جزء ضروری دسترسی و اتصال افراد به شبکه اینترنت می‌باشد. رساها با داشتن امکانات ویژه می‌توانند راحت‌تر از دیگران حریم خصوصی اطلاعاتی شهروندان را نقض کنند. از طرف دیگر

فعالیت نظام‌مند آن‌ها مبتنی بر تدابیر امنیتی می‌تواند از ارتکاب بسیاری از جرایم علیه داده های شخصی پیشگیری کند. رساها موظف به حمایت فنی (رویکرد حمایتی) از حقوق کاربران نیز شده‌اند. ضمن اینکه رساها موظفند که حقوق کاربران را به ایشان اطلاع دهند و نحوه حفاظت از حریم خصوصی اطلاعات و ارتباطات را به ایشان آموزش دهند. این تکالیف با یک رویکرد حمایتی درصدد پیشگیری از تجاوزات به حقوق کاربران و مخصوصاً حریم خصوصی ایشان است.

این آیین نامه ضمن تاکید بر مصونیت حریم خصوصی کاربران در بندهای ۵-۳-۱۵ و ٦، در بند ۹، تجاوز به حریم خصوصی کاربران را مقید به یک سری ضمانت اجراهای اداری کرده است. ضمن اینکه این ضمانت اجراها مانع طرح مورد در دادگاه‌ها و اعمال حقوق کیفری نخواهد بود. این بند آیین نامه فاقد شفافیت و وضوح کافی در تعیین ضمانت اجراهاست. ضمن اینکه در بند ٦ مصادیق مهمی از تجاوز به حریم خصوصی مانند شنود یا دسترسی غیر مجاز تخلف شمرده شده‌اند درحالی‌که هنوز این موارد غیر از ضمانت اجراهای اداری این ماده مشمول هیچ حکم کیفری نمی‌شوند. بندهای مذکور به قرار ذیل می‌باشند:

۱۵-۳-۵- حریم اطلاعات خصوصی کاربران از مصونیت برخوردار بوده و هرگونه دسترسی غیرقانونی توسط رساها و هر مرجع دیگر به فعالیت‌های اینترنتی کاربران ممنوع می‌باشد.

بند ٦- تولید و عرضه موارد زیر توسط رساها و کاربران ممنوع می‌باشد:

۱۳-٦- افشاء روابط خصوصی افراد و تجاوز به حریم اطلاعات شخصی آنان

١٤-٦- انتشار اطلاعات حاوی کلیدهای رمز بانک‌های اطلاعاتی، نرم افزارهای خاص، صندوق‌های پست الکترونیکی و یا روش شکستن آن‌ها

۱۸-٦- هرگونه نفوذ غیرمجاز به مراکز دارنده اطلاعات خصوصی و محرمانه و تلاش در جهت شکستن قفل رمز سیستم‌ها

۲۰-٦- هرگونه تلاش برای انجام شنود و بررسی بسته های اطلاعاتی در حال گذر در شبکه که به دیگران تعلق دارد

بند ۹- در صورت تخطی از موارد مندرج در این مصوبه، مجازات‌های اعمال شده شامل تذکر، قطع موقت مجوز، لغو پروانه و طرح در دادگاه‌ها و محاکم قانونی بسته به نوع

تخلف بر اساس قوانین و ضوابط ذی‌ربط بر عهده کمیسیون راهبردی می‌باشد که بر اساس گزارش نظارتی وزارت پست، تلگراف و تلفن بررسی و اعلام نظر می‌نماید.

همان طور که ملاحظه می‌شود، در مواد مذکور نیز نقض اصولی از قبیل اصل تحصیل مشروع و مجاز، اصل تحصیل منصفانه و اصول راجع به در دسترس قرار دادن داده‌ها مورد جرم انگاری قرار گرفته است.

۴- نتیجه‌گیری

برای درک صحیح از جرم انگاری‌های صورت گرفته و نیز پایه ریزی یک ارزش گذاری کیفری منطقی در مورد حمایت از حریم خصوصی در برابر نقض الزامات اساسی حمایت از داده‌ها در فضای سایبر، لازم است ابتدا اصول و مبانی حاکم بر جمع آوری، نگهداری، پردازش و انتقال و افشاء اطلاعات شخصی تبیین شوند و سپس حقوق اشخاص موضوع داده معین شوند. آن گاه می‌توان موارد شدید نقض و تجاوز به این اصول و حقوق را جرم انگاری نمود و یا در مقام تفسیر و اجرای جرم انگاری‌های صورت گرفته، از چهارچوب مشخصی بهره‌مند شد. نقض این اصول و حقوق ناشی از آن‌ها، طبقات عمده جرایم علیه حریم خصوصی در فضای سایبر را پدید می‌آورند. ضمن اینکه تبیین دقیق اصول و حقوق مبتنی بر واقعیت‌های اجتماعی، سیاسی و فرهنگی موجود، می‌تواند در پیشگیری از جرایم در این زمینه و نیز رعایت منطق و انصاف در جرم انگاری بسیار مهم و اثربخش باشد.

مقایسه بین قانون فدرال حمایت از داده آلمان با قوانین ایران در زمینه داده های شخصی نشان می‌دهد که حقوق ایران به لحاظ فقدان برخی از اصول حاکم بر داده های شخصی، کامل نبودن اصول پیش بینی شده و ارجاع برخی دیگر به آیین نامه های مختلف دارای نقایص جدی است که باید از سوی مقنن مورد بازنگری قرار گیرد. از سوی دیگر، فقدان مقررات جامع در زمینه حمایت از حریم خصوصی مانع از درک و اجرای صحیح حمایت از داده در دادگاه‌ها و مراجع اداری می‌گردد. «لایحه حریم خصوصی» که برای ارائه به مجلس شورای اسلامی تدوین شده، این ایراد را تا حدودی برطرف نموده است که در صورت رفع ایرادات و تصویب آن، خلأ موجود تا حدی مرتفع می‌گردد. علاوه بر آن چه گفته شد، مقررات حقوق ایران ناظر بر حمایت از داده های شخصی، از حیث مصادیق داده های مورد حمایت و ضمانت اجراهای کیفری نیز دارای نواقص و ایرادتی است که بحث و بررسی‌های مفصل و مستقلی را می‌طلبد.

پی‌نوشت‌ها

۱. ماده (۳)۴۳ قانون فدرال حمایت از داده آلمان مقرر می دارد کـه جـرایم اداری مـذکور در مـاده (۱)۴۳، قابل مجازات با جزای نقدی حد اکثر تا ۲۵ هزار یورو است.

۲. (ISP) برگرفته از کلمه Internet Service Provider یعنی شرکت خدمات سرویس های اینترنـت است. یک ISP توسط یک خط تلفن از شرکت مخابرات و یا امکانـات مـاهواره ای مـی توانـد اینترنت را به User خود سرویس دهد.

منابع

اصلانی، حمیدرضا (۱۳۸٤). «اصول حاکم بر حمایت از داده»، مندرج در *مجموعه مقاله های همایش بررسـی جنبه های حقوقی فناوری اطلاعات*، چاپ اول، تهران: معاونت حقوقی و توسعه قضایی قوه قضاییه، مرکز مطالعات توسعه قضایی.

اصلانی، حمیدرضا(۱۳۸٤). *حقوق فناوری اطلاعات*، چاپ اول، تهران، نشر میزان.

باستانی، برومند(۱۳۸٦). *جرایم رایانه ای و اینترنتی جلوه ای نوین از بزهکاری*، چاپ دوم، تهران، نشر میزان.

حسنی، جعفر(۱۳۸۵). «حمایت کیفری از حریم خصوصی در فضای سایبر»، دانشگاه شهید بهشتی، دانشکده حقوق، پایان نامه جهت اخذ درجه کارشناسی ارشد گرایش حقوق جزا و جرم شناسی.

دزیانی، محمد حسن(۱۳۷٦). *جرائم کامپیوتری*، جلد اول، تهران، دبیرخانه شورای عالی انفورماتیک.

دزیانی، محمد حسن(۱۳۷۸). *جزوه آموزشی حقـوق سـایبر و جـرایم سـایبری*، جلـد اول، چـاپ محـدود، معاونت آموزش قوه قضاییه.

زرکلام، ستار(۱۳۸٦). «حریم خصوصی ارتباطات اینترنتی(مطالعه در حقـوق ایـران و اتحادیـه اروپـا)»، *مجلـه معارف اسلامی و حقوق*، سال هشتم، شماره اول، ۱۷۳-۱۹٦.

زیبر، اولریش(۱۳۸۳). *جرایم رایانه ای*، ترجمه نوری، محمد علی و نخجوانی، رضا و بختیاروند، مصـطفی و رحیمی مقدم، احمد، چاپ اول، تهران، کتابخانه گنج دانش.

عامل نجف آبادی، محمد(۱۳۸۷). «جرم انگاری در فضای مجازی»، دانشگاه شهید بهشتی، دانشکده حقـوق، پایان نامه جهت اخذ درجه کارشناسی ارشد گرایش حقوق جزا و جرم شناسی.

محسنی، فرید(۱۳۸۹). *حریم خصوصی اطلاعات: مطالعه تطبیقی در فقه امامیه، حقوق کیفری ایران و ایالات متحده آمریکا*، تهران، انتشارات دانشگاه امام صادق.

David H. Flaherty, (1989). Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.

Kelleher D & Murray K. (1999). IT Law in the European Union, Sweet & Maxwell, London.

Kabay M. E. (2002). Anonymity and Identity in Cyberspace, in “Computer security handbook”, forth edition, John Wiley & sons Inc, United States of America, New York.