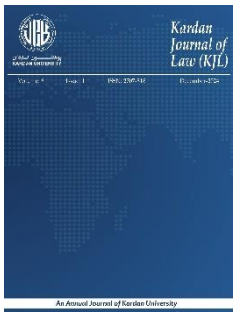

Kardan Publishing

Kardan Journal Law (KJL)

ISSN: 2707-3181 (Print and Online), Journal homepage: https://kardan.edu.af/KJL

Protecting Privacy of Data and Systems: A Comparative Study of the Criminal Laws of Afghanistan and Iran

Dr. Mohammad Ali Rezayee
Ehsanullah Faisal

To cite this article: Rezayee, Mohammad Ali, and Ihsanullah Faisal "Protecting Privacy of Data and Systems: A Comparative Study of the Criminal Laws of Afghanistan and Iran", *Kardan Journal of Law*, 6, no. 1 (2024): 27-46.
DOI: 10.31841/KJL.2024.27

To link to this article: http://dx.doi.org/ 10.31841/KJL.2024.27

Published online: 30 December 2024

Article

Protecting Privacy of Data and Systems: A Comparative Study of the Criminal Laws of Afghanistan and Iran

Kardan Journal of Law
6 (1) 27 – 46

Kardan Publications
Kabul, Afghanistan
http://dx.doi.org/10.31841/KJL.2024.27
https://kardan.edu.af/KJL

Received: 30 Sep 2024
Revised: 30 Oct 2024
Accepted: 30 Nov 2024
Published: 30 Dec 2024

Dr. Mohammad Ali Rezayee
Ihsanullah Faisal

حمایت از محرمانگی اطلاعات و سیستم: بررسی مقایسوی نظام جزایی افغانستان و ایران

چکیده

مداخله حقوق جزا در حمایت از محرمانگی اطلاعات و سیستم با چالشِ ناسازگاری فراگیری و نسبیت همراه است. از یک سو به جهت بنیادی بودن محرمانگی برای فضایی‌که مبتنی بر اطلاعات است، از محرمانگی اطلاعات و سیستم همه اشخاص حقیقی و حقوق حمایت می‌شود، ولی از سوی دیگر، این حمایت مطلق نیست تا همراه با خواست دارندگان اطلاعات و سیستم باشد و این خواست خود را در اقدامی پیشینی در قالب حفاظت از اطلاعات یا سیستم از دیگران، ایجاد ارتباط غیرعمومی یا طبقه‌بندی کردن اطلاعات اعلام کنند. در اینجا مداخله حقوق جزا بر اساس عدالت جزایی و استحقاق در مجازات کردن رفتارهای سرزنش پذیر نیست بلکه بر اساس یک رابطه طولی از تلفیق عدالت ترمیمی و عدالت جزایی است. در واقع محرمانگی ارزشی چند دستی در فضای سنتی به جهت محوری شدن در فضای‌سایبر به نخستین ارزش مورد حمایت تبدیل شده است ولی همچنان مفهوم و شاخص‌های آن با دارندگان اطلاعات و سیستم گره خورده است و این نسبیت و فردیت را از فضای سنتی وام گرفته است. مقاله حاضر با استفاده از منابع کتابخانه‌ای و با روش توصیف و تحلیل در پی پاسخ به پرسشی بنیادین درباره حدود مداخله حقوق جزا در حمایت از محرمانگی اطلاعات و سیستم است. با لحاظ اوصاف بنیادین حقوق جزا و ویژگی‌های فضای‌سایبر، به این نتیجه رسیده است که مداخله حقوق جزا بر اساسی رویکرد سودانگارانه و نیز رهیافت مبنی بر عدالت ترمیمی، می‌کوشد تا اراده شهروندان در حفاظت از محرمانگی خود را به اراده قانونگذار پیوست کند و در همان حال آنها را به تدبیر بازدارنده برای پاسداری از محرمانگی اطلاعات و سیستم فرابخواند.

کلمات کلیدی: محرمانگی اطلاعات و سیستم، حقوق جزا، اعلام پیشینی محرمانگی

مقدمه

محرمانگی اطلاعات و سیستم، مهم‌ترین مؤلفه امنیت کمپیوتر و بنیادی‌ترین ارزش برای زیست سایبری است. دلیل این امر نیز ابتنای فضای سایبر بر اطلاعات و معلومات است. در واقع آنچه که بایسته اطلاعات و معلومات است، محرمانگی آن‌ها است. اگر در زندگی بیرونی و فیزیکی، ارزش‌های گوناگونی از جان و مال گرفته تا نظم عمومی و محیط زیست مطرح می‌شوند و در این میان، حریم اطلاعات شخصی ناپدید یا کم‌رنگ می‌شوند؛ ولی در فضای سایبر این موضوع در صدر فهرست ارزش‌های مورد حمایت قرار می‌گیرد و همین ویژگی نقطه آغازین برای بررسی مسأله این نوشتار است که می‌توان از دو زاویه به آن نگریست:

از یک سو محرمانگی اطلاعات و سیستم دنباله ارزشی به نام حریم خصوصی افراد است که در نظام حقوق کشورها مطرح بوده است. حقوق اساسی شهروندان و حمایت بی‌پیشینه از محرمانگی حریم خصوصی اشخاص در قوانین اساسی هر دو کشور «افغانستان و ایران» دلیل محکم و متقن برای اثبات این ادعا است. بنابراین، محرمانگی بیشتر نقش حفاظتی و مصونیت بخشی به حریم خصوصی افراد را دارا است و از فراهم شدن زمینه‌ها و فرصت‌های تاخت و تاز بر این حریم خاص در جهت برملا نمودن جلوه‌های خصوصی زندگی فردی که فرد علاقه به فاش شدن آن نداشته و باعث سلب آرامش روحی، تنزل جایگاه اجتماعی و حتی در برخی موارد منجر به پایان دادن حیات فزیکی متضرر توسط خودش در اعتراض علیه وضعیت موجود می‌شود؛ جلوگیری می‌کند.

البته محرمانگی در این فضا به دلایلی چون دسترسی همگان به فضای سایبر و با در نظرداشتن ابعاد وسیع و گسترده آن و عدم موجودیت زمینه‌های بازدارنده، بیشتر آسیب‌پذیر است. نقض محرمانگی زمینه سوءاستفاده از اطلاعات و سیستم را فراهم می‌کند. اگر این اطلاعات متعلق به اسرار نظامی باشد، نقض محرمانگی و دسترسی به آن جاسوسی محسوب می‌شود که ممکن است از این ناحیه، امنیت ملی و تمامیت ارضی کشور مربوط به مخاطره افتد. البته فارغ از بحث‌های امنیتی، در خیلی از موارد دیگر نیز نقض محرمانگی می‌تواند آسیب‌های جدی و حیاتی غیرقابل جبرانی به‌بار آورد. مثلاً به نقل از صفحات خبری تسنیم و اصلاحات پرس «هکرها به اطلاعات واکسن کرونا ساخت شرکت داروسازی آمریکایی فایزر و شریک آلمانی آن شرکت بایو ان تک دسترسی پیدا کرده و مسئولان شرکت نامبرده تائید نموده‌اند که اسناد مربوط به ساخت واکسن کوید19 این شرکت در جریان یک حمله سایبری به رگولاتری دارویی اروپا به سرقت برده شده است.»[1] در واقع در چنین زمان حساسی که حیات بشری در سراسر دنیا با تهدید مرض مهلک کوید19 دچار است، نقض محرمانگی داده‌ها و اطلاعات حساس مربوط به ساخت واکسن کرونا به مراتب مهم‌تر از اسرار نظامی و دفاعی یک کشور و در حقیقت بیانگر اهمیت محرمانگی اطلاعات و معلومات در فضای سایبر است که هر آن امکان دستبرد به آن وجود دارد.

از سوی دیگر، حریم خصوصی یا محرمانگی داده‌ها و سیستم‌های اشخاص حقیقی و حقوق متفاوت با حریم خصوصی محیط فیزیکی می‌باشد. به‌عبارت دیگر محرمانگی داده‌ها و سیستم‌ها در فضای سایبر به منزله یک ارزش بسیط به اندازه حریم خصوصی در محیط فیزیکی نیست؛ بلکه خود تجمع همه ارزش‌هایی است که از فضای بیرونی به فضای سایبر منتقل شده‌اند. وقتی سخن از محرمانگی اطلاعات و سیستم می‌شود، نمادی از همه اطلاعات مرتبط با ارزش‌های بنیادینی چون جان، امنیت و محیط زیست و ارزش‌های دیگری چون مالکیت فکری و اطلاعات تجاری است و همین امر حدود مداخله حقوق جزا را برای حمایت فراگیر از محرمانگی اطلاعات و سیستم‌های همه اشخاص توجیه می‌کند. البته

[1] Tasnim News and Eslahaat Press, Telegram post, December 10, 2020.

برخلاف محیط بیرونی که حقوق جزا تنها بخشی از حریم خصوصی اشخاص را مورد حمایت قرار می‌دهد؛ این فراگیری همراه با نقش‌دهی به حمایت‌شدگان در اعلام اهمیت محرمانگی از دید آن‌ها است و اگر اشخاص حقیقی یا حقوق، حفاظت از محرمانگی را اعلام نکنند، حمایت حقوق جزا از داده‌ها و سیستم‌های آن‌ها انجام نمی‌شود. همین امر مداخله جزایی فراگیر را نسبی می‌کند که بر اساس آن، رفتارهای ضد محرمانگی اطلاعات و سیستم، ضرورتاً سرزنش‌پذیر نیست؛ مگر اینکه دارنده اطلاعات یا سیستم با اقداماتی اعلام کند که محرمانگی از نظر وی دارای اهمیت است. از این رو، حدود مداخله حقوق جزا در زمینه حمایت از محرمانگی اطلاعات و سیستم با تضاد فراگیری از یک سو و نسبیت از سوی دیگر مواجه می‌گردد و در این نوشتار به آن پرداخته می‌شود. در این راستا، ابتدا ارزش‌های مورد حمایت معرفی و سپس چالش‌های مداخله حقوق جزا در حمایت از این ارزش‌ها بررسی می‌شوند و در نهایت نظم حقوق جزا ایران و افغانستان به صورت مقایسه‌ای مورد بررسی قرار می‌گیرد.

1. مفهوم محرمانگی اطلاعات و سیستم

در بحث محرمانگی اطلاعات و سیستم بیشتر به مصونیت آن‌ها پرداخته می‌شود که شامل جلوگیری از هرگونه دسترسی، رویت و اطلاع‌یابی از اطلاعات قرار گرفته در سیستم یا مداخله و اثرگذاری بر فعالیت سیستم در پردازش اطلاعات است. به‌عبارت دیگر اهمیت و کاربرد مطلوب اطلاعات و سیستم وابسته به مصونیت آن‌هاست. در این راستا ضرورت شناخت موضوع و اطلاع از مفاهیم و تعاریف کلمات ایجاب می‌کند که پیش از ورود به اصل بحث، اصطلاحات مهمی چون محرمانگی، اطلاعات و سیستم از نظر مفهومی به‌صورت ریشه‌ای توضیح داده شود تا زمینه برای ورود به اصل بحث فراهم شود.

1.1 محرمانگی

تعریف متفاوت حقوق‌دانان از محرمانگی، بیانگر برداشت‌های متفاوت از این اصطلاح است و به‌خوبی نقش اثرگذاری عرف جامعه را در توصیف این واژه به تصویر می‌کشد. عده‌ای محرمانگی را یکی از ارکان مهم و اساسی حریم خصوصی می‌دانند.[2] به باور برخی دیگر محرمانگی پوشش مناسب برای حفظ اطلاعات و سیستم و عدم دسترسی افراد غیرصالح به آن است[3] و عده‌ای هم آن‌را استثنایی بر آزادی اطلاعات می‌شمارند.[4] اما آنچه مهم است «محرمانگی اطلاعات و سیستم‌های کمپیوتری از مصالح مورد اتفاق برای استفاده صحیح و تقویت اعتماد و گسترش کاربرد کمپیوتر در امور روزمره مردم است و بر همین اساس اقدام به جرم‌انگاری نقض آن شده است.»[5]

بعضاً این پرسش مطرح می‌شود که وقتی ما، اطلاعات و سیستم را برخوردار از محرمانگی می‌دانیم و از سوی دیگر از آن به چتر حمایتی وسیع تعبیر می‌کنیم و ادعایی داریم که گویا اطلاعات و سیستم به هیچ وجه از محدوده حمایتی آن

---

[2]. حریم خصوصی نیز، که بارها به تعریف آن اشاره شده، متشکل از سه رکن اصلی است: ۱- محرمانگی، ۲- گمنامی، ۳- تنهایی، به نقل از فرید محسنی، David Banisar, *Privacy and Human Rights: An International Survey of Privacy Law and Developments* (Washington, DC: Electronic Privacy Information Center, 1st ed., 2000), 2.

[3]. محرمانگی به معنی کسب اطمینان خاطر از غیرقابل‌نفوذ بودن اطلاعات و عدم دسترسی غیر به آن است .طاهره میرعمادی، *مبانی حقوق ملی و شهروندی در فضای تبادل اطلاعات* (تهران: مؤسسه تحقیقات و توسعه علوم انسانی، ۱۳۸۷)، ۳۱۶.

[4]. حفظ حریم خصوصی افراد از جمله استثناهای آزادی اطلاعات به شمار می‌رود؛ زیرا از یک‌سو حفظ محرمانگی شخصی ممکن است مانع شود که اطلاعات مربوط به زندگی خصوصی به ابزاری برای درهم‌شکستن آزادی و استقلال انسان‌ها تبدیل شود.]لازم به ذکر است[محرمانگی اطلاعات یعنی حق خودداری از ارائه اطلاعات به دیگران .محسن نوکاریزی و سیدمهدی نارمنجی، *آشنایی با اطلاعات و ارتباطات* (تهران: انتشارات سمت، ۱۳۹۲)، ۱۳۵.

[5]. غلام‌رضا محمدنسل، *حقوق جزای اختصاصی جرایم رایانه‌ای در ایران* (تهران: نشر میزان، ۱۳۹۵)، ۲۵.

خارج نیست؛ آیا محرمانگی میان اطلاعات و سیستم مشترک است یا جدای از هم است؟ همچنین وضعیت حامل‌های اطلاعات چه می‌شود که از آن‌ها در کنار اطلاعات و سیستم نام برده نشده است؟ در واقع با توجه به این‌که حامل اطلاعات، سیستم نیست تا از این حمایت برخوردار شود؛ آیا این مسأله خود یک تناقض آشکار در جهت ادعای فوق نیست؟ حقوق‌دانان با تفسیر شیوا توضیح لازم را برای رفع ابهام موجود ارائه کرده و بر این نگرانی نقطه پایان گذاشته و معتقدند که «اطلاعات بیشتر در درون سیستم یا سیستم جای می‌گیرد و شکستن محرمانگی سیستم، شکستن محرمانگی اطلاعات را نیز به همراه دارد ولی گاه اطلاعات بر روی داده برها (حامل‌های داده) مانند دیسک فشرده (سی‌دی) است که در سنجش با کمپیوتر یا گوشی همراه به سختی می‌توان داده‌برها را سیستم دانست و در اینجا خود اطلاعات می‌تواند موضوع بزه قرار گیرد؛ بدون آن‌که به سیستم یورش برده شود.»[6]

2.1 اطلاعات و سیستم

لازم به ذکر است که اطلاعات (data) در قانون جرایم کمپیوتری ایران همان «داده»، سیستم (Computer System) همان «سامانه» و اطلاعات (Information) همان «معلومات» است که در بخش جرایم سایبری کود جزای افغانستان نیز به این عناوین شناخته می‌شود. اطلاعات و سیستم از اهمیت فوق‌العاده در جرایم کمپیوتری برخوردار است و در این راستا برخی آن را به خون و رگ‌های پیکره فضای سایبری تعبیر کرده و گفته‌اند، «پیکره فضای سایبر هم‌چون بدن آدمی است که اطلاعات نقش خون و سیستم‌ها و شبکه‌ها نقش رگ‌ها را دارند. وجود هر یک بدون دیگری امکان‌پذیر نیست و در واقع بدون وجود یکی از این دو، فضای تبادل اطلاعات شکل نمی‌گیرد.»[7] اطلاعات کمپیوتری می‌توانند به اقسام مختلف وجود داشته باشد. «داده‌ها ممکن است به‌صورت برنامه رایانه ای[8] یعنی نرم‌افزار (Software) یا این‌که به‌صورت متن، صوت و تصویر که از آن به عنوان داده محتوا (Data Content) یاد می‌شود، باشند.»[9]

در باب معرفی و شناسایی اطلاعات در منابع مختلف به تعاریف متفاوت برخوردیم که برخی از آن‌ها کلی[10] و برخی هم مبهم[11] است. اما برای وضوح بیشتر باید گفت که «داده در لغت به معنی اطلاعات، مفروضات، دانسته‌ها و سوابق آمده است.»[12] و در اصطلاح به «اطلاعات خاصی که وارد رایانه می‌شوند تا پردازشی روی آن‌ها صورت گیرد، داده اطلاق می‌شود.»[13] اطلاعات در معنای فنی «علایم، نمادها و سیگنال‌هایی است که قابلیت ورود (Input) به یک سیستم رایانه ای، پردازش (Process)، ذخیره (Storage)، انتقال و خروج (Output) را داشته باشد. داده می‌تواند به شکل آنالوگ، دیجیتال و یا موج (نوری یا الکترومغناطیسی) موجود باشد؛ مثلاً اطلاعات ثبت شده روی یک کاست، داده‌های آنالوگ

---

6. حسن عالی‌پور، *حقوق کیفری فناوری اطلاعات* (تهران: خرسندی، ۱۳۹۵)، ۱۶۴.

7. عالی‌پور، *حقوق کیفری فناوری اطلاعات*، ۱۴۹.

8. نرم‌افزار، دستورالعمل‌های دقیقی است که عملیات سیستم رایانه‌ای را کنترل می‌کند .کنت سی. لاودن و جین پی. لاودن، *فناوری اطلاعات و ارتباطات؛ مفاهیم و کاربردها*، ترجمه حمید محسنی (تهران: نشر کتابدار، ۱۳۹۲)، ۱۰۳.

9. مهدی فضلی، *مسوولیت جزایی در فضای سایبر* (تهران: انتشارات خرسندی، ۱۳۹۶)، ۷۷.

10. مجموعه دانسته‌هایی که سیستم رایانه‌ای روی آن پردازش انجام می‌دهد تا نتیجه مورد نظر حاصل شود .به نقل از جواد بابایی؛ مجید سبزعلی گل و سیدعلی موسوی، *مفاهیم پایه فناوری اطلاعات* (تهران: شرکت چاپ و نشر کتاب‌های درسی ایران، ۱۳۹۲)، ۱۸.

11. داده، مجموعه‌ای از واقعیات خام است که هنوز به شکل سازماندهی و منسجم نشده که افراد آن را درک و مورد استفاده قرار دهند. محمدرضا زندی، *تحقیقات مقدماتی در جرایم سایبر* (تهران: انتشارات جنگل، ۱۳۹۳)، ۲۷.

12. به نقل از ابراهیم اسلامی؛ سلیمان حییم، *فرهنگ کوچک انگلیسی - فارسی* (تهران: انتشارات فرهنگ معاصر، چاپ پانزدهم، ۱۳۳۷)، ۸.

13. ابراهیم اسلامی؛ کامران شیرزاد، *جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و بین‌الملل* (تهران: نشریه بهینه فراگیر، چاپ اول، ۱۳۸۸)، ۷۹-۸۰.

است. اطلاعات ارسالی از سوی یک ماهواره داده‌هایی است که به صورت موج ارسال می‌شود و داده‌های دیجیتالی به صورت توالی نمادهایی از الفبای دودویی (Binary Alphabet) به شکل صفر و یک ظهور می‌یابد.»[14]

در مورد تعریف سیستم برخلاف نظر پیش‌گفته، برخی از حقوق‌دانان برنامه کامپیوتری را جز سامانه یا سیستم می‌دانند؛[15] نه اطلاعات. اما برخی دیگر بدون اینکه از نرم‌افزار نام ببرند، سیستم را دستگاهی دارای حافظه و قابل برنامه‌ریزی معرفی می‌کنند.[16] هر یک از تعاریف موجود به‌نحوی یک بخش از سیستم را واضح ساخته؛ ولی تعریف نسبتاً قابل قبول را کنوانسیون جرایم سایبر ارائه کرده است که بر اساس آن «سیستم رایانه ای، هرگونه ابزار یا مجموعه‌ای از ابزارهای مرتبط و متصل به هم است که مطابق با یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهد.»[17] این تعریف برنامه کامپیوتری را نه اطلاعات دانسته و نه سیستم؛ بلکه آن را یک نظم‌دهنده معرفی کرده است که به‌وسیله آن سیستم قادر می‌شود تا پردازش خودکار اطلاعات اخذ شده را انجام دهد و طی فرآیندی که انسان در آن هیچ دخالتی ندارد به اطلاعات[18] تبدیل کند. هم‌چنین سیستم را ابزار معرفی کرده و به‌نحوی دامنه شمول آن را به هر نوع ماشین الکترونیکی که توانمندی فعالیت خودکار را دارا باشد؛ مثل ماشین‌های خودپرداز بانکی (ATM) و همانند آن گسترش اطلاعات است.

3.1 ارزش محرمانگی

محرمانگی از ارزش فوق‌العاده‌ای برخوردار است. محرمانگی اعتماد، آرامش و اطمینان به‌بار می‌آورد. ارزش و اعتبار اطلاعات نه‌تنها به محرمانگی آن وابسته است، بلکه هرگاه محرمانگی از آن سلب شود ممکن است اطلاعات کارایی خود را از دست بدهد. محرمانگی اطلاعات می‌تواند یا نسبت به حریم خصوصی فرد19 و دارای ارزش فردی یا در مورد اطلاعات مهم مرتبط با امنیت ملی20 کشور و متعلق به یک جغرافیای خاص و یا نه فردی و امنیتی بلکه در رابطه با یک موضوع حساس،21 مانند اطلاعات واکسن بیماری کوید19 متعلق به شرکت‌های داروسازی باشد که از اهمیت حیاتی جهانی برخوردار است. هم‌چنین باید گفت محرمانگی اطلاعات و سیستم می‌تواند در کارکرد و پاسخگویی آن به نیازهای موجود اثرگذار باشد. به‌هر اندازه که اطلاعات و سیستم دارای ارزش حیاتی و کارایی بیشتر باشد، به همان اندازه محرمانگی آن از اهمیت بیشتری برخوردار خواهد بود. عرف حاکم جامعه، اطلاعات و سیستم را ارزش‌گذاری می‌کند و

---

[14]. مهدی فضلی، *مسوولیت جزایی در فضای سایبر* (تهران: انتشارات خرسندی، ۱۳۹۶)، ۷۸.

[15]. سیستم رایانه‌ای مورد نظر این کنوانسیون، دستگاهی است که از نرم‌افزار و سخت‌افزاری که برای پردازش خودکار داده‌های دیجیتال طراحی شده، تشکیل یافته است. امیرحسین جلالی فراهانی، *کنوانسیون جرایم سایبر و پروتکل الحاقی آن* (تهران: انتشارات خرسندی، ۱۳۹۵)، ۱۹.

[16]. <<دستگاهی دارای حافظه و قابل برنامه‌ریزی که قادر است عملیات ریاضی و منطقی را با سرعت بالا، انجام و نتیجه را ارائه نماید. به‌عبارت دیگر، دستگاهی است که بتواند سه عمل را انجام بدهد؛ ۱- دریافت اطلاعات ۲- پردازش اطلاعات ۳- اعلام نتیجه پردازش یعنی اطلاعات >>. سبزعلی گل و موسوی، *مفاهیم پایه فناوری اطلاعات*، ۱۷.

[17]. کنوانسیون سایبر، ۲۰۰۱: بند الف ماده ۱.

[18]. محتوای اطلاعات به شمار می‌آید که با سیستم کمپیوتری تولید شده و برای پردازش و ارسال مناسب است. ابراهیم اسلامی، *حقوق جزای اختصاصی جرایم رایانه‌ای ایران؛ با تأکید بر کنوانسیون جرایم رایانه‌ای بوداپست و آرای صادره محاکم قضایی* (تهران: انتشارات جنگل، ۱۳۹۷)، ۲۶.

[19]. حوزه‌هایی از اطلاعات که مشمول حمایت قانونی اسرار قرار می‌گیرند، تقریبا نامحدود هستند. مواردی هم‌چون اطلاعات مربوط به زندگی جنسی، معالجات بهداشتی و پزشکی، موضوعات خانوادگی، امور منزل، محتوای دفترچه یادداشت، نامه‌ها و نامه‌های الکترونیکی، عکس‌های مراسم ازدواج و تصاویر موجود در منزل مربوط به این حوزه می‌شود. پیترکری جوساندرز، *حقوق رسانه*، ترجمه حمیدرضا ملک محمدی (تهران: نشر میزان، ۱۳۸۶)، ۱۶۹.

[20]. امنیت ملی در فضای سایبر منوط به امنیت اطلاعات است و در واقع تا زمانی که امنیت اطلاعات مخدوش نگردد، امنیت ملی نیز تهدید نمی‌شود. عالی‌پور، *حقوق کیفری فناوری اطلاعات*، ۴۵.

[21]. اطلاعاتی که دارای ویژگی محرمانه هستند، ضرورتاً در ردیف اسرار جای می‌گیرند، جوساندرز، *حقوق رسانه*، ۱۶۸.

قانون‌گذار در قالب قانون به ارزش‌های تعیین شده رسمیت می‌بخشد؛ لذا می‌توان گفت محرمانگی یک اصل22 و ارزش‌گذاری آن اعتباری23 است.

قبل از اینکه اطلاعات و سیستم مورد استفاده قرار گیرد و فناوری اطلاعات پیشرفت‌های چشم‌گیر امروزی را داشته باشد، حریم خصوصی و محرمانگی آن کمتر مورد تعرض قرار می‌گرفت و در این خصوص، مصونیت نسبی وجود داشت. به سخن دیگر، محرمانگی محیط فیزیکی نسبت به محرمانگی در فضای سایبر از ثبات و پایداری بیشتر برخوردار بود؛ چون در محیط فیزیکی یک نظارت عمومی بر مبنای اخلاق جمعی و هنجارهای هدایت‌گر اجتماعی، شکل گرفته که در کنار نهادهای مجری قانون و تأمین کننده نظم، در کنترل جامعه نقش مهمی دارد. در این فضا، فرد با هویت واقعی است و در صورت ارتکاب جرم، اغلب شناسایی و ردیابی می‌شود و در واقع اتخاذ تصمیم به ارتکاب جرم با پذیرفتن بیشترین ریسک ممکن است و هزینه سنگینی را در پی دارد؛ از این رو می‌توان گفت حریم خصوصی اشخاص در فضای فیزیکی از مصونیت بیشتر برخوردار است و در واقع محرمانگی در این محیط ارزش است، ولی مهمترین ارزش به حساب نمی‌آید. این در حالی است که قابل تغییر بودن هویت و مخفی بودن فضای سایبر یک فرصت بی‌بدیل را برای مجرمین فضای سایبر فراهم ساخته است تا با خاطر آسوده در این فضا، آنارشیسم و هرج و مرج را به‌وجود آورند. فقدان حاکمیت و در دسترس بودن امکانات لازم، زمینه نقض محرمانگی را فراهم ساخته و سبب شده است تا در فرصت اندک از لحاظ زمانی، قربانی موردنظر را به دام جرمی‌شان بیاندازند؛ لذا جرم کمترین هزینه ممکن را برای مرتکبین آن دارد و محرمانگی در یک شرایط شکننده قرار گرفته است و از این رو مهمترین ارزش به حساب می‌آید. تجربه به اثبات رسانده هر قدر وابسته به فناوری شویم،[24] به همان اندازه حریم خصوصی ناامن‌تر[25] و نقض محرمانگی بیشتر می‌شود.

2. مبانی مداخله حقوق جزا در حمایت از محرمانگی اطلاعات و سیستم

اهمیت محرمانگی به‌خاطر قابلیت سوءاستفاده از اطلاعات و سیستم است. محرمانگی اطلاعات و سیستم یعنی همه قابلیت دسترسی به آن را ندارند و در واقع سیستم و اطلاعات جزء حریم خاص پنداشته می‌شود که متعلق به یک فرد یا افراد مجاز است که می‌توانند به آن ورود و دسترسی داشته باشند. ممکن عده‌ای برخلاف اصول اخلاق و با نادیده گرفتن محرمانگی اطلاعات و سیستم، اقدام به نقض محرمانگی و سوءاستفاده از آن کنند که در چنین وضعیتی ناگزیریم به‌خاطر حمایت از اطلاعات و سیستم و حفظ محرمانگی آن به قوانین جزا به‌عنوان آخرین گزینه مراجعه کنیم.

---

[22]. اصل بودن حریم خصوصی می‌تواند باعث تضمین گردش آزاد اطلاعات در مجاری قانونی و صحیح آن باشد. اما عکس این قضیه صادق نیست. بدین معنی که مبنا قرار دادن آزادی اطلاعات هیچ تضمینی برای حریم خصوصی ایجاد نمی‌کند؛ زیرا در بسیاری موارد آزادی اطلاعات، راه تجاوز به حریم خصوصی را هموار می‌سازد. فرید محسنی، *حریم خصوصی اطلاعات؛ مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه* (تهران: انتشارات دانشگاه امام صادق، ۱۳۹۴)، ۲۷۵.

[23]. اطلاعات محرمانه در بعد اطلاعات خصوصی که موضوع افشای اسرار قرار می‌گیرد با اطلاعاتی که به معنای خاص محرمانه خوانده می‌شوند و موضوع جاسوسی قرار می‌گیرد متفاوت است. مهدی فضلی، *مسوولیت جزایی در فضای سایبر*، ۱۹۹.

[24]. کشورهای که در آن‌ها فناوری اطلاعات به عنوان بستر اصلی فعالیت‌ها در آمده، آسیب‌پذیری‌هایی را نیز پیدا کرده‌اند. این آسیب‌پذیری‌ها بیشتر ناشی از وابستگی سایر بخش‌ها به فناوری اطلاعات و سهولت استفاده از فناوری اطلاعات توسط گروه‌ها و افراد تهدید کننده فضای مجازی است. ابراهیم حسن بیگی، *حقوق و امنیت در فضای سایبر* (تهران: انتشارات ابرار معاصر، ۱۳۸۴)، ۷۹.

[25]. مرز میان حریم خصوصی و امنیت قابل تشخیص است «حریم خصوصی در فضای سایبر» یک حق است و امنیت، اقداماتی است که برای محافظت از این حق (و سایر منافع) انجام می‌شود. محسنی، *حریم خصوصی اطلاعات؛ مطالعه جزا در حقوق ایران، ایالات متحده آمریکا و فقه امامیه* (تهران: انتشارات دانشگاه امام صادق، ۱۳۹۴)، ۵۳۵.

1.2 پیوند اخلاق و محرمانگی

اخلاق، معیار درستی و نادرستی مفاهیم روزمره است که ما با آن سروکار داریم و یک گستره وسیعی از هنجارهای مهمی که در زندگی فردی و جمعی ما اثرگذار است را شکل می‌دهد. یقیناً محرمانگی نیز یکی از این ارزش‌ها و حق انسانی هر فرد است که در جامعه قابل طرح و بررسی است. در این باره باید گفت که «ارزش‌های اخلاق همان ارزش‌های اجتماعی‌اند و در خارج از ظرف اجتماع، بسیاری از مفاهیم اخلاق، بلکه هیچ یک از آن‌ها معنای محصلی ندارند. ایثار، صبر و استقامت، راست‌گویی، عدالت‌ورزی، محبت و امثال آن همگی ارزش‌هایی هستند که جامعه به ما معرفی می‌کند.»[26]

حال ما مکلف[27] هستیم از محرمانگی اطلاعات و سیستم یا به‌عنوان یک ارزش یا به سبب پیامدهای[28] ناگوار اجتماعی که نقض آن در پی دارد، حفاظت کنیم. اگر صرفاً دید ارزشی محض به محرمانگی داشته باشیم، اهمیت و کارایی آن کاهش می‌یابد و تبدیل به یک هنجار می‌شود که نقش آن در تعاملات اجتماعی کم‌رنگ خواهد شد. پیامدگرایی صرف نیز کارساز نیست؛ زیرا ممکن است زمینه بی‌حدوحصرِ نادیده گرفتن محرمانگی را به‌عنوان یک ارزش اجتماعی پذیرفته شده با هر توجیه پیش‌پاافتاده‌ای تحت عنوان نتیجه مفید و دلخواه فراهم کند. به‌عبارت دیگر از یک سو، نباید آنقدر وابستگی بی‌چون‌وچرا به محرمانگی اطلاعات و سیستم پیدا کنیم که در برابر هیچ پیامدی آن را قابل معاوضه ندانیم؛ چرا که در این صورت ممکن است بدخواهان جامعه به حصار امنی دست یابند. از سوی دیگر میان پیامدهای حمایت یا نادیده گرفتن محرمانگی باید سبک و سنگین صورت گیرد؛ چون محرمانگی یک ارزش اجتماعی است و از این رو عرف جامعه به عنوان معیار در قوانین مربوط مشخص خواهد کرد که در چه صورتی محرمانگی از سوی چه کسی یا چه نهادی و در برابر چه پیامدی قابل نقض خواهد بود. در این چارچوب محرمانگی به‌عنوان یک ارزش اخلاق و اجتماعی مورد حمایت قانون خواهد بود؛ لذا نقض آن جرم پنداشته و مجازات می‌شود. این موضوع شبیه عنوانی است که در فلسفه اخلاق از آن به غایت‌نگری قانونی[29] تعبیر می‌کنند.

2.2 پیوند مذهب و محرمانگی

اسلام دین رأفت، صلح، محبت، صفا، آرامش، صمیمیت و همدلی است. در آن تجسس، بدون اجازه به خانه‌ای دیگری داخل شدن، سرک کشیدن به حیاط خلوت افراد، بدگمانی نسبت به دیگران، نسبت دادن اعمال ناروا به دیگری، خیانت در امانت، سوءاستفاده از اعتماد دیگران، پرده‌دری از عیوب مردم و غیبت کردن منع شده است. فلسفه این دستورات در دین مبین اسلام، حفظ آبروی فرد، تأمین آرامش او و احترام به‌مقام انسان است. از این رو می‌توان گفت نه‌تنها میان محرمانگی و آموزه‌های اسلامی پیوند وجود دارد، بلکه محرمانگی از دل آموزه‌های اسلامی برخواسته است.

---

[26]. محمدتقی مصباح یزدی، *فلسفه اخلاق* (تهران: شرکت چاپ و نشر بین‌الملل، چاپ خانه سپهر، چاپ اول، ۱۳۸۱)، ۱۱۳.

[27]. ناپیامدگرایی که بر اساس آن برخی از انواع کارها (مثل کشتن بی‌گناهان) فی نفسه نادرست است، نه به خاطر پیامدهای بدی که به‌بار می‌آورد. هری جی گنسلر، *درآمدی جدید به فلسفه اخلاق*، برگردان حمیده بحرینی، (تهران: نشر آسمان خیال، چاپ اول، ۱۳۸۵)، ۲۵۲.

[28]. پیامدگرایی که بر اساس آن باید کاری را انجام داد که بیشترین پیامدهای خوب را به‌بار می‌آورد. خود این مسئله که چه نوع کاری انجام می‌دهیم فی نفسه اهمیتی ندارد. گنسلر، *درآمدی جدید به فلسفه اخلاق* (تهران: نشر آسمان خیال، چاپ اول، ۱۳۸۵)، ۲۵۲.

[29]. «غایت‌نگری قانونی: عملی درست است که اگر و تنها اگر به‌وسیله یک قانون طلبیده شود که خودش عضوی از مجموعه قوانینی است که پذیرش آن‌ها می‌تواند به یک خیر و بهره بزرگ‌تر برای جامعه منتهی شود تا به‌هر گونه احتمال دیگر» لوپی پویمان، *درآمدی بر فلسفه‌ی اخلاق؛ شناسایی درست و نادرست*، ترجمه شهرام ارشد نژاد (تهران: انتشارات گیل، چاپ اول، ۱۳۷۸)، ۱۳۵.

قرآن به عنوان بزرگ‌ترین کتاب آسمانی مسلمان‌ها را از تجسس منع کرده و آن را یک کار ناروا دانسته و فرموده است که در زمینه چنین صراحت دارد (یا أَیُّهَا الَّذینَ آمَنُوا اجتَنِبُوا کَثیراً مِنَ الظَّنِّ إِنَّ بَعضَ الظَّنِّ إِثمٌ وَ لا تَجَسَّسُوا)[30] ترجمه «ای کسانی که ایمان آورده اید! از بسیاری از گمانها بپرهیزید، چرا که بعضی از گمانها گناه است؛ و هرگز در کار دیگران تجسس نکنید» هر کدام از آیات قرآن، حکمت‌های زیادی دارد. یکی از حکمت‌های این آیه، بحث پرده‌پوشی و حمایت از محرمانگی است. پیامبر اسلام (صلی الله علیه وسلم) به‌عنوان مبلغ و پیام‌آور دین نیز جستجو در اسرار دیگران را در قالب یک حکم عام، حرام دانسته است؛[31] یعنی هرکسی در پی کشف اسرار دیگران باشد، وعده خداوند است که او را رسوا خواهد کرد. حضرت علی(کرم الله وجهه) نیز در زمان حکومت خود به مالک اشتر در مصر به عنوان یک مقام حکومتی دستور دادند که از کسانی‌که در پی عیب‌جویی مردم‌اند، دوری جوید و در پی امور پنهان مردم نباشد. در واقع حتی یک مقام ارشد حکومتی به‌عنوان امین و محرم راز مردم برای انجام برنامه‌های حکومتی که در رابطه با نظم جامعه و آسایش عموم مردم است؛ حق دسترسی به امور پنهان آن‌ها را ندارد که این موضوع نشانگر آن است که اسلام تا چه اندازه برای محرمانگی ارزش قائل است و از آن حمایت می‌کند.

3.2 پیوند سوداجتماعی و محرمانگی

محرمانگی در جامعه معنی و مفهوم می‌یابد. به سخن دیگر اطلاعات و سیستم و نهایتاً معلومات، در جامعه کارایی لازم را دارد و هرگاه جامعه‌ای نباشد، دیگر بحث و جدال در مورد محرمانگی بی‌معناست. حقیقت این است که اطلاعات برای سهولت و پیشرفت‌های مورد نیاز جامعه بشری شکل گرفته است؛ ولی واقعیت چیزی برخلاف این حقیقت است و می‌توان گفت که امروزه اطلاعات در خیلی از موارد به‌نحوی زندگی اجتماعی را به سمت دشواری‌های غیرقابل پیش‌بینی سوق داده است. «اطلاعات در عصر فناوری اطلاعات و ارتباطات، موضوع مهمی است که قلمرو زندگی انسان‌ها را دربرگرفته است و هر روز بر دامنه آن افزوده می‌گردد. دسترسی ساده عموم به اطلاعات دیگران و تسهیل در نظارت‌های گوناگون بر زندگی اشخاص، موجب دشواری زندگی انسان‌ها شده است.»[32]

در دنیای جدید اطلاعات، دیگر از رمزورازهای زندگی خبری نیست. زندگی به‌سان کف دست هر فرد گشته که هر کف‌شناسی به راحتی خطوط ناهمگون آن را نظاره می‌کند. از مسئولیت‌پذیری خبری نیست و مصونیت و آرامش روحی تبدیل به یک رویا شده است که در نرسیدن شهروندان به این رویا هیچ‌کس بی‌تقصیر نیست. فرد عادی جامعه با توجیه آزادی اطلاعات از برهم زدن این آرامش، کوچک‌ترین احساس ندامت ندارد و حکومت‌ها گاهی با توجیه مباحث مرتبط به امنیت ملی[33] و تروریسم[34] هیچ مانعی را در مقابل خویش نمی‌پذیرند. در واقع کنترل زندگی شهروندان و سرک کشیدن به حیاط خلوت مردم کم‌کم در حال عادی شدن است. عده‌ای دیگری بنابر مقاصد متعدد مانند خودخواهی،

---

[30]. (حجرات / ۱۲)

[31]. اسحاق بن عمار از امام صادق روایت می‌کند که پیامبر فرمودند: ای تمام کسانی که به زبان اسلام آورده‌اید و ایمان به قلبتان رسوخ نکرده است، مسلمانان را مذمت نکنید، در جست‌وجوی اسرارشان (معایبشان) نباشید؛ زیرا هر شخصی که به دنبال کشف اسرار دیگران باشد، خداوند اسرار او را آشکار خواهد ساخت و خداوند اسرار هر کسی را هویدا سازد، او را رسوا خواهد ساخت، هرچند در منزلش باشد .به نقل از (بای و پورقهرمانی، ۱۳۸۸: ۲۰۶) از «محمدبن یعقوب کلینی، *الاصول من الکافی*، ج۲، ص۳۵۴ و ۳۵۵».

[32]. محسنی، *حریم خصوصی اطلاعات؛ مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه*، ۱۵.

[33]. یکی از عوامل مؤثر در مبهم ماندن تعریف و مفهوم امنیت تمایل صاحبان قدرت می‌باشد تا از این طریق بتواند جهت توجیه اعمال خلاف قاعده مورد استفاده قرار گیرد «.به نقل از فرید محسنی؛ محسن اسماعیلی، «امنیت و شریعت»، *فصل‌نامه کتاب نقد* ۱۴ و ۱۵ (۱۳۷۹)، ۲۶۳.

[34]. امروزه، شنود تلفنی و رهگیری اطلاعات و داده‌ها یکی از برجسته‌ترین راه‌های کنترل شهروندان است و بیشتر دولت‌ها چه مردم‌سالار و چه نامردم‌سالار این شیوه را آزموده‌اند و بهانه آن را یا پیکار با تروریسم دانسته‌اند یا پاسداشت امنیت ملی .عالی‌پور، *حقوق کیفری فناوری اطلاعات*، ۱۷۹.

قهرمان‌تراشی، ارضای حس انتقام‌جویی، رسیدن به منفعت شخصی، دلایل سیاسی و امنیتی و مواردی از این دست در پی آسیب رساندن[35] به فضای سایبر و اطلاعات‌اند و حتی گاهی سیستم‌ها نیز از چنین آسیب‌هایی در امان نیستند.

شاه بیت هر آنچه که در مورد جامعه گفته شد، محرمانگی است. به رسمیت شناختن محرمانگی و تلاش برای محفوظ ماندن و تأمین آن به‌صورت خودکار منجر به سود اجتماعی می‌شود و نادیده گرفتن و نقض آن هزینه‌های اجتماعی[36] در پی دارد. امروزه بیشتر از هر وقت و زمان دیگر فضای تبادل اطلاعات به‌دلیل نبود محرمانگی آشفته است. میان سود اجتماعی و محرمانگی نه‌تنها پیوند بلکه یک رابطه دوسویه وجود دارد. به سخن دیگر محرمانگی سود اجتماعی را به‌دنبال دارد و سود اجتماعی در پی حفظ و حمایت از محرمانگی است. چنین رابطه‌ای در استحکام این پیوند و بقای آن نقش اساسی دارد.

اطلاعات، برنامه کمپیوتری، سیستم و معلومات، همه حاصل تلاش فکری دانشمندان عرصه فناوری اطلاعات است[37] که به‌سان موتور محرک در فضای سایبر نقش ایفا می‌کند. نسخه اصلی که دانشمندان این عرصه برای جامعه پیچیده‌اند در تأمین امنیت و برآورده شدن نیازها، نقش مهم و حیاتی دارد؛ مثلاً امروزه اطلاعات کاربرد بی‌پیشینه و بی‌بدیل در عرصه پیشرفت و خود کفایی اقتصادی و در جهت شکوفا شدن جامعه انسانی دارد که نمونه مهم آن بانک‌داری اینترنتی[38] و تجارت الکترونیک[39] است. اما اگر محرمانگی وجود نداشته باشد، تلاش‌های فکری دانشمندان و اقدامات انجام شده در این عرصه به ثمر نخواهد نشست. در این صورت اطلاعات آلت دست بدخواهان جامعه قرار می‌گیرد، کارایی لازم خود را از دست می‌دهد و به یک تهدید مرموز مبدل می‌شود. بر این اساس «از منظر باهمادگرایان امروزین، شخص در چارچوب اجتماع و با توسل به ارزش‌های مشترک جمعی می‌تواند آرمان‌های خویش را تعقیب کند. فرد خارج از اجتماع، آن‌سان که فردگرایان می‌گویند جز در عالم انتزاع، قابل تصور نیست. بنابراین تحمیل هرگونه قیود اجتماعی بر افراد به‌خاطر خیر و صلاح آنان صورت می‌گیرد و نمی‌توان آن را امری خلاف اصل تلقی کرد.»[40]

3. چالش‌های مداخله حقوق جزا در حمایت از محرمانگی اطلاعات و سیستم

برخورد موردی حقوق جزا در حمایت از محرمانگی اطلاعات و سیستم یکی از چالش‌های عمده و اساسی است که نمایانگر عدم ثبات آن در این راستا است. امری که به این چالش‌ها افزوده، بیشتر برخورد به‌ظاهر مصلحتی حقوق جزا

---

[35]. طی تخمینی که توسط کارشناسان ارائه شده است خسارت وارده به سیستم‌های کمپیوتر از طریق انتشار ویروس I Love You در سطح جهان بالغ بر یازده بلیون دلار بوده است .به نقل از مهدی فضلی؛ Kumar Katyal, Neal, *Criminal Law in Cyber Space*, p. 3 (http://www.nealkatyal.com).

[36]. مراد از هزینه اجتماعی، زیان‌هایی است که روابط متعارف شهروندان را دست‌خوش تغییر می‌سازد و بی‌هنجاری را در فضای عمومی جامعه دامن می‌زند و بستر مناسب برای گسترش فساد و ناهنجاری اجتماعی فراهم می‌کند .مجتبی فرح‌بخش، *جرم‌انگاری فایده‌گرایانه‌ای؛ جستاری در فلسفه حقوق جزا* (تهران: نشر میزان، چاپ اول، ۱۳۹۲)، ۳۲۸.

[37]. اکنون نرم‌افزارهایی که حاصل تلاش فکری دانشمندان بسیار در حوزه کامپیوتر است به زحمت و با صرف هزینه‌های مالی و زمانی تولید می‌شود و گاهی به بهای زیادی توسط کاربران خریداری می‌شود. اهمیت اطلاعات همچنین بستگی به میزان وابستگی جوامع به اطلاعات دارد؛ در واقع هر قدر جامعه‌ای اطلاعاتی‌تر باشد، همان قدر اطلاعات در آن جامعه بیشتر اهمیت می‌یابد .فضلی، *مسئولیت جزایی در فضای سایبر*، ۱۹۴.

[38]. کاربرد فناوری‌های اطلاعات در امور مالی و بانک‌داری این امکان را فراهم می‌کند که به سرعت پول را به صورت الکترونیکی از یک مکان به مکان مجازی دیگر در هر نقطه از جهان منتقل کرد .مرتضی نورمحمدی، *گسترش فناوری‌های اطلاعات و ارتباطات و تحول امنیت* (تهران: نشر میزان، ۱۳۹۰)، ۱۷۳.

[39]. انجام عملیات بانکی از طریق شبکه، بارزترین مصداق فعالیت‌های مبتنی بر فناوری نوین است که حریم خصوصی نقش کلیدی در آن ایفا می‌کند و وارد شدن کوچک‌ترین خدشه‌ای بر آن، عرصه تجارت الکترونیک را با تمام حساسیت و مقبولیتش با شکست روبه‌رو خواهد ساخت . محسنی، *حریم خصوصی اطلاعات؛ مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه*، ۲۷۲.

[40]. فرح‌بخش، *جرم‌انگاری فایده‌گرایانه‌ای؛ جستاری در فلسفه حقوق جزا*، ۲۲۰.

است که از محرمانگی اطلاعات به‌صورت عام حمایت نمی‌کند. در واقع تنها عده‌ای از ناقضین محرمانگی اطلاعات و سیستم با واکنش حقوق جزا مواجه می‌شوند؛ نه همه ناقضین محرمانگی. اما عده‌ای به این چالش‌های حقوق جزا بسنده نکرده و ضعف و عدم کارایی حقوق جزا را در برابر فضای سایبر نیز از چالش‌های آن قلمداد نموده‌اند. به باور این عده، فضای سایبر از لحاظ محرمانگی به ذهن آدمی می‌ماند؛[41] آیا می‌توان ذهن آدمی را خواند، کنترل کرد و به بند کشید؟[42] پاسخ به این پرسش مجال دیگر و فرصت لازم می‌طلبد.

1.3 نسبیت محرمانگی

محرمانگی یک واژه آشنا، مهم و حساس اما در عین حال نسبی است. از نظر هر فرد محرمانگی یک ارزش است، ولی حساسیت افراد در برابر این ارزش متفاوت است. این تفاوت اغلب وابسته به اهمیت موضوعی است که محرمانگی‌اش نقض شده است. اگر موضوع مهم باشد بیشتر حساسیت‌آفرین و واکنش‌برانگیز خواهد شد، اما اگر موضوع خیلی اهمیت کلیدی نداشته باشد ممکن است نقض محرمانگی آن حساسیت شدیدی را در پی نداشته باشد که یک امر طبیعی است. البته گاهی در یک موضوع مشخص بسته به طرز دید فرد نسبت به محرمانگی آن موضوع که جامعه نیز در این ارزش‌گذاری فرد نقش دارد؛ واکنش‌ها متفاوت است. برای نمونه ممکن است در جوامع غربی پخش عکس شخصی یک شخص خیلی حساسیت‌زا نباشد و فرد متضرر در حد یک اعتراض یا شکایت به نهادهای مربوط علیه آن اقدام و بسنده کند. اما در جامعه دیگر نشر آن حیثیتی و از ارزش حیاتی برخوردار باشد. مثلاً «در ایران برخی از کسانی که به هر طریق به فیلم‌ها و عکس‌های خصوصی دیگران دست پیدا می‌کردند با تهدید به انتشار آن در اینترنت مبالغ سنگینی باج‌خواهی می‌نمودند. اشخاص متعددی به دلیل انتشار فیلم‌های شخصی دست به خودکشی زدند و یا زندگی آن‌ها به طلاق منتهی گردید و یا حتی برخی قتل‌های ناموسی رخ داد.»[43] علاوه‌براین ممکن است حتی در یک جامعه دو فرد نسبت به نقض محرمانگی یک موضوع معین واکنش‌های متفاوت داشته باشند که بیانگر آن است که محرمانگی یک ارزش پذیرفته شده نسبی است، اما ثابت نیست.

در دو کشور ایران و افغانستان نیز، برخورد متفاوت نسبت به محرمانگی اطلاعات و سیستم وجود دارد. قانون‌گذار هر دو کشور دسترسی غیرمجاز،[44] شنود غیرمجاز[45] و جاسوسی سایبری[46] را ناقض محرمانگی اطلاعات و سیستم می‌داند. عناوین یاد شده در هر دو کشور جرم بوده و برای مرتکبین آن مجازات تعیین شده است. چنین اقدامی به‌صورت رسمی بیانگر حمایت حقوق جزا از محرمانگی اطلاعات و سیستم است. اما وقتی در قانون هر دو کشور جاسوسی صرف به اطلاعات سری تعلق می‌گیرد و اطلاعات صنعتی و تجاری را شامل نمی‌شود، یعنی عملاً محرمانگی آن‌ها از دایره حمایت هر دو قانون خارج است؛ لذا بازهم به نکته قبلی که نسبیت محرمانگی است بر می‌گردیم. در حقیقت قانون‌گذار تعیین می‌کند که بر چه مبنایی، در چه زمانی، بر اساس چه شرایطی از محرمانگی چه نوع اطلاعات و سیستم‌ای حمایت قانونی کند.

---

[41]. فضای سایبر از جهت محرمانگی همچون ذهن آدمی است. در ذهن آدمی تعداد بی‌شماری از قضایا یا مطلوب‌هایی نهفته است که اگر عیان شود سبب تحیر دیگران یا نقض مکرر قانون یا هنجارها می‌گردد. ابراهیم اسلامی، *جرم سایبری و بزه‌دیده سایبری* (تهران: انتشارات افروز، ۱۳۹۵)، ۲۳.

[42]. فضای سایبر به جهت افسارگسیختگی و کنترل‌ناپذیری با دنیای بیرونی قابل مقایسه نیست و باز باید گفت به هر میزان که می‌توان ذهن انسان‌ها را دید و آن‌ها را به بند کشید و کنترل کرد، می‌توان در فضای سایبر نیز صادق باشد .اسلامی، *جرم سایبری و بزه‌دیده سایبری*، ۲۵.

[43]. محسنی، *حریم خصوصی اطلاعات؛ مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه*، ۵۸۸.

[44]. ماده ۹۵۰ قانون مجازات اسلامی ایران و مواد ۸۵۲ و ۸۵۵ کود جزا افغانستان.

[45]. ماده ۹۵۱ قانون مجازات اسلامی ایران و ۸۵۶ کود جزا افغانستان.

[46]. مواد ۹۵۲، ۹۵۳ و ۹۵۴ قانون مجازات اسلامی ایران و ماده ۸۶۴ کود جزا افغانستان.

در برخی از کشورها نه‌تنها محرمانگی همه اطلاعات از حمایت قانونی برخوردار نیست؛ بلکه حتی گاهی تحت عناوینی چون امنیت ملی و مصالح دیگر نقض محرمانگی را به‌طور قانونی مستوجب مجازات ندانسته‌اند. به سخن دیگر مواردی وجود دارد که نقض محرمانگی را قانونی دانسته و جز وظایف مجریان قانون قلمداد کرده‌اند. «طبق ماده 6 قانون امنیت هوایی آلمان، مأموران برای کشف اقدامات تروریستی اختیار گشودن داده‌های شخصی را دارند. بر پایه ماده 7 قانون امنیت انسانی فیلیپین، مأموران دولتی با وجود قانون ضد استراق سمع با مجوز کتبی دادگاه پژوهش می‌توانند با به‌کارگیری هر حالت، شکل، نوع یا سنخ از ابزار و تسهیلات الکترونیکی، ارتباطات، پیام‌ها، مکالمات، مباحثات و گفت‌وشنودها و نوشته‌های سازمان‌های تروریستی از قبل اعلام شده یا سازمان‌ها و افراد مشکوک به ارتکاب تروریسم یا تبانی برای ارتکاب آن را شنود یا دریافت یا ضبط کنند. البته این ماده شنود یا دریافت اطلاعات از کسانی که بسته به شغل‌شان باید اطلاعات‌شان پنهان بماند مثل پزشکان و بیماران یا وکیلان و موکلان را استثنا کرده است. بر پایه قانون تنظیم اختیارات بازپرسی انگلستان مصوب 2000 نیز مأموران دولت به بهانه بایسته‌های امنیت ملی، می‌توانند به فراگیری یا افشای داده‌های ارتباطی ماده 2، خبرگیری از داده‌های در حال تراکنش ماده 28 و انجام جاسوسی‌های سرزده دست زنند.»[47]

2.3 اعلام محرمانگی

محرمانگی اصطلاح خیلی کلی و عام است که اگر تمام امکانات جامعه برای حمایت از آن بسیج شود، ممکن حمایت لازم از آن به‌صورت شایسته و بایسته صورت نگیرد. البته عام بودن نباید توجیه عدم حمایت قانون از محرمانگی تمام اطلاعات و سیستم‌ها محسوب شود. بنابراین راه‌حل این است که قانون به قدر ضرورت و نیاز، حمایت‌های لازم را داشته باشد. در این راستا ضروری است چند شرط را در نظر بگیریم تا بر اساس آن، هر اطلاعات و سیستم‌ای که شرایط معین را تکمیل کرد از حمایت قانون برخوردار شود. به‌عبارت دیگر وقتی محرمانگی به معنی وسیع آن قابل حمایت قانون نباشد، نیاز است تا موارد حمایت شده به‌صورت فنی- حقوقی از سوی قانون‌گذار اعلام و مشخص شود.

مثلاً شرط رعایت تدابیر امنیتی[48] یا حفاظت‌شدگی در دسترسی غیرمجاز، اطلاعات و سیستم‌هایی را که مورد حمایت قانون قرار می‌گیرد از بقیه اطلاعات و سیستم‌ها تفکیک می‌کند. بنابراین «چنان‌چه رایانه دزدیده شده دارای گذرواژه یا دیگر تدابیر حفاظتی نباشد، که بیشتر رایانه‌های شخصی این چنین هستند، موضوع ماده یک قانون جرایم رایانه‌ای نخواهد بود حتی اگر رباینده به سامانه وارد شود؛ مگر اینکه رفتارهای دیگری مانند تخریب داده یا پخش محتوای خصوصی انجام شود که در این‌صورت بزه جداگانه‌ای رخ می‌دهد.»[49] با تفکیک اطلاعات و سیستم‌های یادشده محدوده مورد حمایت قانون مشخص می‌شود؛ بنابراین هر اطلاعات و سیستم که شرایط و حمایت قانونی را داشته باشد، محرمانه است و نقض محرمانگی آن‌ها برخورد سخت قانون را در پی دارد. حقیقتاً مقنن با اعلام شرط حفاظت‌شدگی در دسترسی غیرمجاز در پی اعلام محرمانگی بوده است.

یکی از موضوعات مهم دیگر ارتباطات افراد در سطح جامعه است. موضوع یک رابطه، مشمولین آن را تعیین می‌کند. مثلاً گاهی موضوع یک رابطه، عام است و این ارتباطات عمومی همه افراد حق دارند از مشمولین آن باشند یا به محتوای آن دسترسی داشته باشند؛ یعنی چیزی پنهانی وجود ندارد تا عده‌ای از دسترسی به آن منع شوند. اما گاهی موضوع یک

[47]. عالی‌پور، حقوق کیفری فناوری اطلاعات، ۱۸۰.

[48]. تدابیر امنیتی همان تدابیر فنی و کمپیوتری است که به شیوه‌های گوناگون مانند نصب باروی آتشین، نصب گذرواژه، رمزنگاری و حتی پنهان‌گذاری انجام می‌شود. عالی‌پور، حقوق کیفری فناوری اطلاعات، ۱۷۱.

[49]. عالی‌پور، حقوق کیفری فناوری اطلاعات، ۱۶۸.

رابطه، مشمولین آن را محدود می‌سازد که به آن ارتباط خصوصی[50] گفته می‌شود و هر کسی غیر از مشمولین آن حق ورود به این رابطه و اطلاع از موضوع آن را ندارد و قانون‌گذار ورود و دسترسی به محتوا را از سوی هر کسی به‌جز مشمولین رابطه و بدون اجازه آن‌ها را غیرمجاز اعلام کرده است. ندادن جواز به چنین ورودی از سوی قانون به‌معنی محرمانه بودن آن است و مقنن حمایت خود را از چنین رابطه محرمانه‌ای اعلام می‌کند.

اگر هر فردی هم به‌صورت شخصی[51] و هم به‌صورت عمومی محدوده‌های محرمانگی را در جامعه مشخص نماید، محرمانگی به اصل فراگیر مبدل خواهد شد که خلاف اصل بودن، آزادی است. لذا معیارهای تعیین‌کننده محدوده محرمانگی باید از سوی یک نهاد معتبر به‌صورت رسمی اعلام شود تا از یک سو برای اکثر اعضای جامعه قابل قبول باشد و از سوی دیگر تضمینی برای حفظ این محدوده وجود داشته باشد. با سنجه قانون تعدادی از اطلاعات و سیستم‌ها با در نظرداشتن اهمیت آن سری[52] اعلام می‌شود و در طبقه حمایت شده قانون[53] قرار می‌گیرد و دسترسی همگان نسبت به آن‌ها منع می‌شود. ممنوعیت اعلام شده دسترسی به اطلاعات و سیستم‌های مشخص، محرمانه بودن آن‌ها را واضح می‌سازد. اعلام منع دسترسی همگان به آن‌ها به یقین اعلام محرمانگی آن‌ها به‌حساب می‌آید.

این که چرا محرمانگی به عنوان هشداری از قبل اعلام می‌شود می‌تواند توجیهات زیاد و متفاوتی داشته باشد. لیکن فلسفه آن ایجاب می‌کند موارد محرمانه از غیر محرمانه تفکیک شود. با اعلام موارد محرمانه از یک سو شهروندان حامی قانون از محرمانه بودن آن حمایت می‌کنند و از سوی دیگر آنان که در پی نقض محدوده محرمانه هستند با برخورد قانون در حمایت از محرمانگی اعلام شده مواجه می‌شوند.

3.3 هم‌پوشانی محرمانگی

یکی از چالش‌های دیگری که حقوق جزا در حمایت از محرمانگی اطلاعات و سیستم به آن مواجه است، هم‌پوشانی محرمانگی است. این چالش تنها فراروی حقوق جزا ایران نیست، بلکه کنوانسیون جرایم سایبر بوداپست نیز چنین وضعیتی دارد. به‌عبارت دیگر چالش هم‌پوشانی محرمانگی ابتدا متوجه کنوانسیون جرایم سایبر بوداپست بود و قانون جرایم رایانه ای ایران در ارائه دسته‌بندی جرایم این فصل از این کنوانسیون الگوبرداری نمود و با این چالش مواجه شد. به‌همین منظور بود که کود جزای افغانستان در بخش جرایم سایبری از دسته‌بندی جرایم صرف نظر و صرفاً به ماده‌ها اکتفا کرده است. در نقد این دسته‌بندی، گفته شده است که «این تقسیم‌بندی، به نوعی تقسیم به مصداق است تا محتوا؛ هر چند جامعیت لازم را دارد اما مانع از ورود یک جرم در چند طبقه نیست.»[54]

اطلاعاتی که بر اثر نقض محرمانگی به‌دست آمده باشد، فاقد اعتبار، غیرقانونی و غیرقابل استناد است. لذا هرگونه تغییر نسبت به اطلاعات غیرمعتبر، جرم پنداشته نمی‌شود؛ چون حمایت قانون را ندارد. لازم به ذکر است هم‌چنین

---

[50]. حریم خصوصی، قلمرویی از زندگی اشخاص است که انسان نوعی و متعارف با درک نیازهای جامعه در هیچ وضعیتی تجاوز به آن را مجاز نمی‌داند. محمدعلی نوری و رضا نخجوانی، حقوق حمایت از داده‌ها، (تهران: گنج دانش، ۱۳۸۳)، ۲۲.

[51]. در مورد اطلاعات خصوصی، ارائه تعریف، کاری مشکل است زیرا تا حدودی به نگاه ذهنی فرد باز می‌گردد یعنی اطلاعات خصوصی در باره یک فرد، ممکن است هیچ‌گونه حساسیت خاصی را برای دیگری نداشته باشد. جوساندرز، حقوق رسانه، ۱۶۸.

[52]. اطلاعات سری: داده‌هایی است که افشای آن‌ها بدون مجوز مرجع قانونی می‌تواند امنیت ملی و یا منافع ملی را دچار مخاطره کند. اسلامی، حقوق جزای اختصاصی جرایم رایانه‌ای ایران؛ با تأکید بر کنوانسیون جرایم کامپیوتری بوداپست و آرای صادره محاکم قضایی، ۵۱.

[53]. دلیل پیش‌بینی داده‌های سری نیز بیرون کردن داده‌های محرمانه از تنگنای پشتیبانی جزا است؛ زیرا گستره داده‌های محرمانه به اندازه‌ای است که می‌توان هر اطلاعاتی را در زیر آن قرار داد و چون در رویه نیز برچسب محرمانه بودن بدون نیاز و توجیه بر روی اسناد قرار می‌گیرد، در قانون جرایم کامپیوتری به داده‌های سری بسنده شده است. عالی‌پور، حقوق کیفری فناوری اطلاعات، ۱۹۵.

[54]. مهرنوش ابوذری، جرم‌شناسی سایبری (تهران: نشر میزان، ۱۳۹۵)، ۲۸.

عمل فردی که اقدام به تغییر اطلاعات قابل استناد کرده و بر این اساس مرتکب تقلب شده است یا با علم به تقلبی بودن اطلاعات آن را مورد استفاده قرار داده اطلاعات در عین حال که در مغایرت با صحت و تمامیت داده‌ها است، خلاف محرمانگی آن نیز است.

4. نظم کنونی حدود مداخله حقوق جزا در حمایت از محرمانگی اطلاعات و سیستم

فضای سایبر که از آن به فضای تبادل اطلاعات نیز تعبیر می‌شود، یک فضای با گستره وسیع است. وسعت این فضا برعکس دنیای واقعی، بحث زمان و مکان در تبادل اطلاعات را متحول و دسترسی به اطلاعات در این فضا را تسهیل کرده و در عین حال گسترش فضای سایبر بر اهمیت امنیت اطلاعات و سیستم نیز افزوده است. امروزه بیش از هر زمان دیگری محرمانگی اطلاعات و سیستم به یک ضرورت غیرقابل انکار تبدیل شده است. در واقع اهمیت موضوع در حدی است که پای حقوق جزا را نیز به این عرصه کشانده است تا در حمایت از محرمانگی اطلاعات و سیستم و تحکیم نظم در فضای تبادل اطلاعات مداخله کند.

1.4 دسترسی غیرمجاز

جرم‌انگاری جرایم فنی سایبری در کل و دسترسی غیرمجاز به صورت خاص در هر دو قانون مجازات اسلامی[55] و کود جزا[56] یک اقدام بی‌پیشینه است که همگام با کاربردی شدن کمپیوتر در نهادهای دولتی و خصوصی هر دو کشور یک ضرورت مبرم محسوب گردید. دسترسی غیرمجاز نه‌تنها که زمینه‌ساز[57] جرایم دیگر است، بلکه به‌خاطر این‌که یک اقدام نادرست و خلاف محرمانگی اطلاعات و سیستم است و به جامعه آسیب[58] می‌رساند مورد توجه قانون‌گذار واقع شده است. در عنوان و کلیت دسترسی غیرمجاز یک اجماع میان کشورها شکل گرفته است؛ ولی مصادیق متفاوت آن در قوانین کشورها یک امر طبیعی است و بستگی به دید قانون‌گذاران مربوط دارد. «در قوانین برخی کشورها، صرف دستیابی جرم شناخته شده است، مانند دانمارک، سوئد، فرانسه و آمریکا. اما در برخی کشورهای دیگر، صرف دستیابی به اطلاعات و سیستم‌ها جرم تلقی نشده؛ بلکه کسب اطلاعات و مانند آن شرط تحقق جرم اعلام شده است.»[59] اما در ایران پیش‌شرط دسترسی غیرمجاز اعمال تدابیر امنیتی[60] از سوی متضرر و نقض آن از سوی مجرم است. این در حالی است که قانون‌گذار افغانستان دسترسی به اطلاعات و سیستم دیگری را جرم دانسته و برای وی فرقی نمی‌کند که

---

[55] هرکس به طور غیرمجاز به اطلاعات‌ها یا سیستم کامپیوتری یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (۵،۰۰۰،۰۰۰) ریال تا بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد. (ماده ۹۵۰ قانون مجازات اسلامی).

[56] ۱ -شخصی که به صورت غیرمجاز به سیستم، برنامه یا اطلاعات کامپیوتری متعلق به دیگری، دسترسی حاصل کند، به حبس قصیر محکوم می‌گردد .۲ -شخصی که به اثر ارتکاب جرم مندرج فقره (۱) این ماده، ضرر جسمی، مالی یا معنوی به شخص یا اشخاص وارد کند، علاوه بر جزای مندرج فقره (۱) این ماده به جزای جرم مرتکب نیز محکوم می‌گردد. (ماده ۸۵۲ کود جزا)

[57] بنتام عقیده به جرم دانستن انحرافاتی داشت که زمینه‌ساز جرایم محسوب می‌شوند تا بدین وسیله هزینه‌های ارتکاب جرم افزایش یابد و شخص به سوی عدم ارتکاب آن سوق داده شود. وی از این جرایم به عنوان جرایم فرعی یا جرایم مساعدکننده یاد می‌کند.» علی حسین نجفی ابرندآبادی، محمد جعفر حبیب‌زاده و محمدعلی بابایی، جرایم مانع؛ جرایم بازدارنده، مجله مدرس علوم انسانی، ۳۷ (۱۳۸۳)، ۲۴.

[58] مؤسسه امنیت کامپیوتر و آگاهی فدرال در ایالات متحده، پیمایش سالانه جرم و امنیت کامپیوتری را برگزار و اطلاعات مورد نیاز خود را از بیش از ۷۰۰ شرکت، نهاد دولتی، مؤسسه مالی، خدمات درمانی و دانشگاه‌ها گردآوری می‌کنند. در سال ۲۰۰۵، این پیمایش از این واقعیت پرده برداشت که ۵۶ درصد پاسخگویان، طی ۱۲ ماه گذشته در اثر نقض امنیت کامپیوترشان آسیب دیده‌اند. ماتیو ویلیامز، بزهکاری مجازی؛ بزه، انحراف و مقررات‌گذاری برخط، مترجمین امیر حسین جلالی فراهانی و محبوبه منفرد (تهران: نشر میزان، ۱۳۹۱)، ۶۵.

[59] محمدنسل، حقوق جزای اختصاصی جرایم رایانه‌ای در ایران، ۲۷-۲۶.

[60] منظور از تدابیر امنیتی ایجاد محدودیت در دسترسی افراد غیر مجاز است، امنیت اطلاعات یا سیستم با توجه به نوع سیستم متفاوت است. در خصوص کمپیوترهای شخصی این کار از طریق قرار دادن رمز عبور و در مورد کمپیوترهای متصل به شبکه از طریق تعریف نام کاربری و رمز عبور صورت می‌گیرد. محمدنسل، حقوق جزای اختصاصی جرایم رایانه‌ای در ایران، ۳۰.

سیستم و اطلاعات تدابیر امنیتی داشته یا خیر. برخی از حقوق‌دانان از تدابیر امنیتی در متن این ماده، موضوعیت سامانه یا سیستم را برداشت می‌کنند.[61] لیکن به باور برخی دیگر این تدابیر صرفاً فنی است و عده‌ای دیگر این تدابیر را علاوه بر فنی شامل تدابیر فیزیکی و انسانی[62] نیز می‌دانند.

آوردن شرط تدابیر امنیتی در متن ماده قانون و برداشت‌های حقوق دانان از این اصطلاح می‌تواند در حمایت قانون از محرمانگی اطلاعات و سیستم اثرگذار باشد. اگر محور تدابیر امنیتی را موضوعیت سامانه یا سیستم بدانیم در این‌صورت محرمانگی اطلاعات از حمایت قانون برخوردار نخواهد بود. اگر آن صرفاً تدابیر فنی بدانیم، موارد غیرفنی را از شمول حمایت قانون خارج کرده‌ایم و باز هم دامنه حمایت قانون از محرمانگی اطلاعات و سیستم محدود خواهد شد. لیکن اگر تدابیر امنیتی را فنی و غیرفنی بدانیم در این‌صورت گستره حمایت قانون از محرمانگی وسیع خواهد شد و اگر شرط کود جزا افغانستان را که دسترسی به اطلاعات و سیستم متعلق به دیگری را دسترسی غیرمجاز می‌داند در نظر بگیریم؛ حمایت قانون از محرمانگی وسعت چشم‌گیری خواهد یافت. در نهایت باید گفت که هر دو قانون ایران و افغانستان از محرمانگی حمایت کرده‌اند. قانون جرایم رایانه‌ای ایران معیار را برای حمایت از محرمانگی، اعمال تدابیر امنیتی قرار داده؛ در حالی‌که کود جزای افغانستان اطلاعات و سیستم را به‌طور عام قابل حمایت دانسته است. بر این اساس مطابق قانون ایران کسانی که اطلاعات و سیستم خود را مجهز به تدابیر امنیتی نسازند از این حمایت بهره‌مند نخواهند شد. لیکن قانون جرایم سایبری افغانستان در این خصوص عام است؛ هر چند در مرحله اجرا ممکن است با دشواری‌هایی از این ناحیه مواجه شود.

2.4 شنود غیرمجاز

با شنیدن واژه شنود، ناخودآگاه در ذهن آدم شنیدن به‌شیوه سنتی آن تداعی می‌شود در حالی‌که شنود با شنیدن متفاوت است. حقوق‌دانان برای فهم بیشتر شنود و تفکیک دقیق‌تر آن از شنیدن به‌صورت سنتی یا کلاسیک، در کنار توضیح واژه شنود ویژگی‌های آن را نیز بیان کرده‌اند. «شنود داده‌ها و اطلاعات و نیز امواج الکترومغناطیسی به معنای شنیدن با گوش نیست؛ بلکه به معنای دریافت کردن یا به اختیار گرفتن داده‌ها و اطلاعات است که در این میان واژگان بویش (Sniffing) و رهگیری (Interception) نیز به‌کاربرده می‌شود. بوییدن اطلاعات یا رهگیری اطلاعات هر دو در یک معنی و دقیق‌تر هستند، ولی چون هردو رفتار دربردارنده دانستن محتوا و مفهوم اطلاعات یا داده‌ها است، سرانجام به همان شنود یا دریافت منجر می‌گردد.»[63]

استفاده از اصطلاح رمزگذاری واضح و درست به نظر می‌رسد، البته در شنود علاوه‌بر رمزگذاری ارتباط، خود اطلاعات نیز به‌صورت فنی و کد شده تغییر می‌کند یا به‌عبارت دیگر رمزی یا رمزدار می‌شود؛ لذا به‌کاربردن اصطلاح رمزنگاری دقیق‌تر است. «در شنود اطلاعات، ممکن است که مهاجم بتواند داده‌ها را قطع (Interrupt) نماید، اما نمی‌تواند از مضمون و محتوای آن چیزی بفهمد؛ مگر این‌که رمزشکنی کند. استفاده از یک سیستم رمزنگاری مناسب این احتمال

[61]. گاهی خود سیستم یا سیستم موضوع جرم می‌باشد به‌طوری که فرد به‌صورت غیرمجاز وارد سیستم و سیستم کمپیوتر ای فرد می‌شود. فرق نمی‌کند که در سیستم به داده‌ها دسترسی پیدا کند یا خیر؟ صرف نقض محرمانگی سیستم، خود موضوع جداگانه‌ای است که جرم‌انگاری شده است. اسلامی، حقوق جزای اختصاصی جرایم رایانه‌ای ایران، ۱۰.

[62]. از آنجا که تدابیر امنیتی نسبت به سیستم، شامل تدابیر فیزیکی و انسانی می‌شود؛ لذا می‌توان گفت اقدام شخصی که با شکستن قفل درب اتاق به‌طور غیرمجاز به سیستم دسترسی می‌یابد مشمول دسترسی غیرمجاز است. مگر این‌که مقصود مقنن را از دسترسی به سیستم دسترسی به کارکرد سیستم بدانیم؛ مثل ماده ۷۳۷ ق.م.ا. جواد بابایی، جرایم رایانه‌ای و آیین دادرسی حاکم بر آن (تهران: مرکز مطبوعات و انتشارات قوه قضائیه، ۱۳۹۷)، ۶۲.

[63]. عالی‌پور، حقوق کیفری فناوری اطلاعات، ۱۷۷.

را بسیار پایین می‌آورد. پیام‌هایی که باید رمزنگاری شوند متن ساده (Plain Text) نام دارند، اما متن خروجی فرآیند رمزنگاری را متن رمزی (Cipher Text) می‌نامند.»[64]

قانون مجازات اسلامی[65] و کود جزا[66] هر دو شنود غیرمجاز را جرم‌انگاری کرده و مرتکبین آن را قابل پیگرد دانسته‌اند. هر دو قانون بر عنوان جرمی توافق نظر دارند ولی نحوه شنود غیرمجاز یا به‌عبارت بهتر، چگونگی انجام شنود در هر دو قانون به‌نحو متفاوتی پیش‌بینی شده است. این تفاوت‌ها میزان و روش حمایت هر دو قانون را از محرمانگی اطلاعات در حال انتقال مشخص می‌سازد. در قانون جرایم رایانه‌ای به صرف شنود میان سیستم‌های متصل بسنده شده است ولی کود جزا، علاوه‌برآن شنودی که در یک سیستم از انتقال اطلاعات از یک پوشه به پوشه دیگر صورت می‌گیرد را نیز جرم دانسته است و عملاً محدوده حمایت قانونی از محرمانگی اطلاعات در حال انتقال را توسعه بخشیده است. بر این اساس در قانون جرایم رایانه‌ای فرد مرتکب به سیستم وارد نمی‌شود بلکه از مسیر انتقال اطلاعات میان دو سیستم این عمل را مرتکب می‌شود؛ ولی برای شنود از انتقال در داخل سیستم، ورود غیرمجاز به سیستم مورد نظر لازم است و در واقع مقدمه آن محسوب می‌شود.

3.4 جاسوسی سایبری

واژه‌های متعددی ذیل عنوان جاسوسی سایبری به‌کاربرده شده است که عبارتند از؛ جاسوسی،[67] جاسوس،[68] خائن‌ملی،[69] خبرگیر[70] و ستون پنجم.[71] جاسوسی مثل دسترسی غیرمجاز عنوان جدیدی نیست، بلکه پیشینه آن به زمان شکل‌گیری حکومت‌ها برمی‌گردد. یکی از بحث‌های عمده و اساسی در قوانین جزایی کشورها را بحث جاسوسی تشکیل

[64]. فضلی، مسوولیت کیفری در فضای سایبر، ۲۱۵.

[65]. ماده ۹۵۱ قانون مجازات اسلامی. هرکس به‌طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سیستم‌های کمپیوتری یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

[66]. ماده ۸۵۶ کود جزا- (۱) شخصی که به‌منظور کسب منفعت برای خود یا دیگری یا وارد نمودن ضرر به دیگری، با استفاده از وسایل تخنیکی یکی از اعمال ذیل را انجام دهد، مرتکب رهگیری غیرمجاز گردیده، به حبس متوسط یا جزای نقدی از شصت هزار تا سه صد هزار افغانی، محکوم می‌گردد :۱ -جلوگیری از انتقال اطلاعات کامپیوتری از سیستم کامپیوتری به سیستم کامپیوتری دیگر یا انتقال آن از یک محل به محل دیگر در عین سیستم کامپیوتری .۲ -جلوگیری از ارسال الکترومغناطیسی از سیستم کامپیوتری که اطلاعات مندرج جزء ۱ فقره (۱) این ماده را انتقال دهد.)۲ (شخصی که از طریق فریب‌کاری، تقلب، یا طرق مشابه دیگر، به‌منظور کسب منفعت برای خود یا شخص دیگری یا وارد ساختن خسارت بر دیگری مرتکب جرم مندرج فقره(۱) این ماده گردد، به حداکثر حبس متوسط، محکوم می‌گردد.

[67]. جاسوسی عبارت است از گردآوری پنهانی و غیرقانونی اطلاعات مرتبط با امور سیاسی، نظامی و سیاسی یک کشور یا اطلاعات متعلق به مردم آن. به نقل از حسن عالی‌پور رالف، دِ سولّا؛ Crime Dictionary, Facts on file, (نیویورک، ۱۹۸۲)، ص.۴۷.

[68]. جاسوس به شخصی اطلاق می‌شود که در پوشش متقلبانه یا مخفیانه و به نفع دشمن درصدد تفحص پیرامون اسرار یا تحصیل اطلاعات یا اشیا یا سایر مدارک و اسناد مربوط به استعداد و توانایی‌های نظامی، اقتصادی و فرهنگی مربوط به یک کشور دشمن باشد. اسلامی، حقوق جزای اختصاصی جرایم رایانه‌ای ایران، ۱۰.

[69]. ماده ۲۳۸ کود جزا- هرگاه تبعه دولت افغانستان مرتکب یکی از اعمال مربوط به جاسوسی گردد، عمل وی خیانت ملی شمرده می‌شود و چنین شخصی خائن ملی خطاب می‌شود.

[70]. جاسوسی یا ستون پنجم که به دلیل مغایرت با امنیت ملی دارای چهره منفی و سرزنش‌آمیز است در چهره‌ای دیگر با تعابیری چون خبرگیر یا کسب اطلاع از کشورهای دیگر برای تأمین امنیت ملی، قابل توجیه و حتی ضروری می‌نماید. عالی‌پور، حقوق کیفری فناوری اطلاعات، ۱۸۷.

[71] در اصطلاح عوامل خرابکار و جاسوسان یک کشور در کشور دیگر یا عوامل گروه مخالف دولت در سازمان دولت را به عنوان ستون پنجم می‌نامند.» به نقل از حسن عالی‌پور؛ داریوش آشوری، دانشنامه سیاسی (تهران: انتشارات سهروردی و انتشارات مروارید، چاپ اول، ۱۳۶۶)، ۱۹۷.

می‌دهد که به تعبیر قانون‌گذاران، فلسفه جرم‌انگاری آن حمایت از امنیت ملی،[72] بقای حکومت‌ها و نظم جامعه عنوان شده است.

در کود جزای افغانستان[73] و قانون مجازت اسلامی،[74] جاسوسی سایبری جرم‌انگاری شده است که این موضوع یک قدم مثبت در راستای حمایت از محرمانگی اطلاعات و سیستم شمرده می‌شود، اما تفاوت‌هایی میان این دو قانون وجود دارد. یکی از این تفاوت‌ها آن است که در قانون مجازات اسلامی اگر مرتکب تبعه ایرانی باشد یا خارجی فرق نمی‌کند و هر دو جاسوس خطاب می‌شوند؛ ولی در کود جزای افغانستان هرگاه تبعه افغانستان مرتکب جرم جاسوسی شود به او خائن ملی و اگر مرتکب، تبعه خارجی باشد به او جاسوس می‌گویند. تفاوت دیگری که وجود دارد آن است که در ماده 954 قانون مجازات اسلامی جاسوسی به‌صورت ترک فعل نیز پیش‌بینی شده در حالی‌که در کود جزا، جاسوسی را به‌موجب ترک فعل قابل تحقق ندانسته است. علاوه‌براین قانون مذکور در بحث مجازات میان جاسوسی سنتی و سایبری تفکیک قائل نشده است.

بحث مهم دیگر، جرم‌انگاری جاسوسی سایبری زیر عنوان محرمانگی در کنار شنود و دسترسی غیرمجاز است. گویا چنین جرم‌انگاری برای حمایت از عام محرمانگی انجام شده است. ولی هنگامی که تبصره قانون مجازات اسلامی، اطلاعات سری را که موضوع جاسوسی است به «داده‌هایی که افشا آن به امنیت کشور لطمه می‌زند تعریف می‌کند» چنین تعریفی عنوان جاسوسی را به اطلاعات که نظامی-امنیتی باشد نه عام اطلاعات محدود می‌کند؛ مثلاً با این تعریف محرمانگی اطلاعات اقتصادی، آموزشی، بهداشتی و دیگر اطلاعات مورد نیاز جامعه از دایره حمایت قانون خارج می‌ماند و در واقع جاسوسی در مورد آن‌ها صدق نمی‌کند یا به‌عبارت واضح‌تر محرمانگی آن‌ها از حمایت قانونی برخوردار نمی‌شود. بنابراین نقض محرمانگی آن‌ها پیگرد قانونی تحت عنوان جاسوسی را در پی ندارد. با چنین وضعیتی متن ماده برخلاف عنوان ماده و عنوان بخش که محرمانگی نام‌گذاری شده و جاسوسی زیر عنوان آن قرار گرفته است؛ خیلی محدود می‌شود و چنین محدودیتی باعث می‌شود تا قانون از محرمانگی اطلاعات محدود و نه عام اطلاعات حمایت کند.

---

[72]. امنیت ملی عبارت است از: حفظ قدرت نظامی، سیاسی، اجتماعی، اقتصادی و فرهنگی و در نتیجه حفظ حکومت و اعمال حاکمیت در امور داخلی و خارجی علیه نفوذ بیگانگان و جلوگیری از هرگونه عملیات غیرقانونی که منظور آن تضعیف و یا انهدام حکومت و ملت باشد. اسلامی، حقوق جزای اختصاصی جرایم رایانه‌ای ایران، ۵۳.

[73]. ماده ۸۶۴ کود جزا) -۱ (شخصی که به‌صورت غیرقانونی نسبت به سیستم، برنامه یا اطلاعات کامپیوتری حاوی اطلاعات سری، مرتکب یکی از اعمال ذیل شود، به جزای جرم خیانت ملی یا جاسوسی مندرج این قانون، محکوم می‌گردد :۱ -دسترسی به اطلاعات سری در حال انتقال یا ذخیره شده در سیستم کامپیوتری یا مخابراتی یا حامل اطلاعات .۲ -در دسترس قرار دادن اطلاعات سری در حال انتقال یا ذخیره شده در سیستم کامپیوتری، مخابراتی یا حامل اطلاعات .۳ -افشاء یا در دسترس قرار دادن اطلاعات سری در حال انتقال یا ذخیره شده در سیستم کامپیوتری یا مخابراتی یا حامل‌های اطلاعات برای دولت، سازمان، شرکت یا گروه خارجی یا عاملان آن‌ها) .۲ (به مقصد فقره (۱) این ماده، اطلاعات سری، عبارت از اسرار مربوط به حاکمیت ملی، تمامیت ارضی یا امنیت ملی کشور می‌باشد که در فصل مربوط به جرایم جاسوسی و خیانت ملی از اسرار دولتی شناخته شده است.

[74]. ماده ۹۵۲ قانون مجازات اسلامی -هرکس به‌طور غیر مجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سیستم‌های کامپیوتری یا مخابراتی یا حامل‌های اطلاعات مرتکب یکی از اعمال زیر شود به مجازات‌های مقرر محکوم خواهد شد :الف) دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون ریال تا شصت میلیون ریال یا هر دو مجازات .ب) در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال .ج) افشاء یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن‌ها، به حبس از پنج الی پانزده سال .تبصره ۱- داده‌های سری داده‌هایی است که افشای آن‌ها به امنیت کشور یا منافع مالی لطمه می‌زند .تبصره ۲- آیین‌نامه نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی و حفاظت از آن‌ها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارت‌خانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیأت وزیران خواهد رسید.

نتیجه‌گیری

در عصر کنونی که فناوری اطلاعات میدان‌دار تمام عرصه‌های سیاسی، اقتصادی، اجتماعی و فرهنگی است و نقش اطلاعات در جامعه کنونی غیرقابل چشم‌پوشی بوده و از اهمیت ویژه برخوردار است؛ اطلاعات و سیستم کلیدی‌ترین نقش را در این چرخه نظام‌مند به عهده دارد. بنابراین محرمانگی این دو حیاتی است و قوانینی در سطح ملی و بین‌المللی لازم است تا از آن حمایت و با ناقضین آن برخورد جدی کند. اهمیت محرمانگی اطلاعات و سیستم فقط به مسائل کلان نظام‌های یاد شده خلاصه نمی شود، بلکه در عصر اطلاعات و در فضای آزاد سایبر آنچه بیشتر آسیب‌پذیر است، حریم خصوصی افراد است که امروزه تحت عنوان حقوق اساسی شهروندی و حقوق بشر یکی از مباحث مهم و داغ جهان است.

محرمانگی اطلاعات و سیستم گاهی از سوی دولت‌ها که خود قوانین را برای حمایت از محرمانگی اطلاعات و سیستم در حیطه خویش تصویب کرده‌اند و تحت عنوان امنیت و نظم عمومی، نقض می‌شود. چنین کاری برخلاف اصل عمومی و همه شمول بودن قوانین صورت می‌گیرد. گاهی هم دولت‌ها به‌خاطر مصلحت‌های کلان جامعه و برای نظارت بر فضای سایبر، محرمانگی را نادیده می‌گیرند و در این راستا حتی اشخاص حقوق غیردولتی موظف می‌شوند تا محرمانگی اطلاعات و سیستم را برای رصد اطلاعاتی که مخالف عقاید و باورهای جامعه است، نقض نماید و گاهی هم محرمانگی از سوی افراد و اشخاص به‌واسطه رخنه‌گری که می‌تواند دلایل متفاوت داشته باشد، نقض می‌شود. چنین اوضاعی شکنندگی محرمانگی را به‌وضوح بیان می‌کند و تصویر واضحی از آن به ما می‌دهد.

ویژگی‌های فضای سایبر و وسعت این فضا زمینه را برای نقض محرمانگی اطلاعات و سیستم فراهم نموده و باعث دل‌چسبی ناقضین محرمانگی اطلاعات و سیستم گردیده است با چنین وضعیتی اطلاعات و سیستم مصون نخواهد بود، لذا لازم است در حوزه قانون‌گذاری چه در سطح ملی و بین‌المللی تجدیدنظر صورت گیرد؛ مثلا در سطح ملی دیگر دارندگان سهل‌انگار اطلاعات و سیستم که تدابیر امنیتی را لحاظ نکرده‌اند نیز از حمایت قانون در برابر نقض محرمانگی اطلاعات و سیستم خود برخوردار شوند و هم در این راستا جاسوسی که یکی از دلایل عمده و اساسی نقض محرمانگی اطلاعات و سیستم به حساب می‌آید و معمولاً از سوی دولت‌ها یا به حمایت دولت‌ها صورت می‌گیرد، جرم شمرده شود تا اطلاعات و سیستم از محرمانگی لازم برخوردار شود.

نقض محرمانگی ممکن است از سوی بدخواهان جامعه یا از سوی دولت صورت گیرد که دلیل هر کدام قبلاً بیان گردید. در برابر بدخواهان باید تدابیر فنی و قانونی لازم اتخاذ گردد ولی دولت بخاطر نظم و امنیت باید راهکار مناسبی را بسنجد که در اثر این راهکار ما شاهد تعادل میان نظم و امنیت جامعه و محرمانگی اطلاعات و سیستم باشیم تا هر دو هم‌زمان از حمایت قانون بهره‌مند باشند و هیچ‌گاه دید افراط‌گونه به مسئله به‌وجود نیاید تا شاهد قربانی یکی به‌خاطر دیگری باشیم؛ مثلاً امروزه ذیل عنوان جاسوسی صرفاً از محرمانگی اطلاعات و سیستم سری حمایت صورت گرفته است در حالی‌که اطلاعات و سیستم‌ای که مستقیم به امنیت ارتباط ندارد، ممکن است به‌طور غیرمستقیم اثرهای انکارناپذیری در این راستا داشته باشد؛ به‌طور نمونه اطلاعات اقتصادی، آموزشی، فرهنگی و اجتماعی باعث تحکیم ریشه‌های امنیت در جامعه می‌شود و عدم رعایت محرمانگی آن‌ها در طولانی مدت، امنیت را متزلزل می سازد.

دستاورد این نوشتار در راستای مسیریابی قضایی در رویارویی با جرایم ضد محرمانگی اطلاعات و سیستم، در اتخاذ رویکرد تلفیقی عدالت جزایی و عدالت ترمیمی است. هم‌چنان‌که باید مرتکب در قبال نقض محرمانگی پیگرد شود، متضرر یا مجنی علیه نیز باید در شکل‌دهی به این جرم نقش فعالی داشته باشد. در واقع برای احراز قضایی جرایم ضد

محرمانگی، اعلام محرمانگی محوری‌ترین عنصر است که قاضی باید احراز کند. این اعلام محرمانگی به‌ویژه برای نهادهای عمومی و دولتی که هم از امکانات بیشتری برخوردارند و هم مکلف به شفاف‌سازی اطلاعات‌اند مگر در موارد مصرح در قانون، باید با حساسیت بیشتری دنبال شود تا هر ادعای نقض محرمانگی از سوی اشخاص حقوق به‌منزله جرم بودن آن در نظر گرفته نشود.

منابع

قرآن کریم (حجرات/12).

ابوذری، مهرنوش .*جرم شناسی سایبری* .چاپ اول. تهران: نشر میزان، 1395.

اسلامی، ابراهیم .*جرم سایبری و بزه دیده سایبری* .چاپ اول. تهران: انتشارات افروز، 1395.

اسلامی، ابراهیم .*حقوق جزای اختصاصی جرایم کامپیوتری ایران (با تأکید بر کنوانسیون جرایم کامپیوتری بوداپست و آرای صادره محاکم قضائی)* .چاپ اول. تهران: انتشارات جنگل، 1397.

اسماعیلی، محسن. "امنیت و شریعت ".*فصل‌نامه کتاب نقد* 14و 15.(1379)

آشوری، داریوش .*دانشنامه سیاسی* .چاپ اول. تهران: انتشارات سهروردی و انتشارات مروارید، 1366.

بابایی، جواد .*جرایم کامپیوتری و آیین دادرسی حاکم بر آن* .چاپ دوم. تهران: مرکز مطبوعات و انتشارات قوه قضائیه، 1397.

بای، حسین علی، پور قهرمانی، بابک .*بررسی فقهی و حقوق جرائم کامپیوتری* .قم: پژوهشگاه علوم و فرهنگی اسلامی، 1388.

پویمان، لویی .*درآمدی بر فلسفه اخلاق؛ شناسایی درست و نادرست* .ترجمه شهرام ارشد نژاد. چاپ اول. تهران: انتشارات گیل، 1378.

پیترکری - جوساندرز .*حقوق رسانه* .ترجمه حمید رضا ملک محمدی. چاپ اول. تهران: نشر میزان، 1386.

جلالی فراهانی، امیرحسین .*کنوانسیون جرایم سایبری و پروتکل الحاقی آن* .چاپ دوم. تهران: انتشارات خرسندی، 1395.

حسن‌بیگی، ابراهیم .*حقوق و امنیت در فضای سایبر* .چاپ اول. تهران: انتشارات ابرار معاصر، 1384.

حییم، سلیمان .*فرهنگ کوچک انگلیسی - فارسی* .چاپ پانزدهم. تهران: انتشارات فرهنگ معاصر، 1337.

زندی، محمدرضا .*تحقیقات مقدماتی در جرایم سایبری* .چاپ اول. تهران: انتشارات جنگل، جاودانه، 1393.

سبزعلی گل، مجید، موسوی، سیدعلی .*مفاهیم پایه فناوری اطلاعات* .تهران: شرکت چاپ و نشر کتاب‌های درسی ایران، 1392.

شیرزدا، کامران .*جرایم کامپیوتری از دیدگاه حقوق جزای ایران و بین‌الملل* .چاپ اول. تهران: نشریه بهینه فراگیر، 1388.

عالی‌پور، حسن .*حقوق جزای فناوری اطلاعات* .چاپ چهارم. تهران: انتشارات خرسندی، 1395.

فرح‌بخش، مجتبی .*جرم‌انگاری فایده ککمپیوتر (جستاری در فلسفه حقوق جزا)* .چاپ اول. تهران: نشر میزان، 1392.

فضلی، مهدی .*مسئولیت جزا در فضای سایبر* .چاپ سوم. تهران: انتشارات خرسندی، 1396.

قانون جزای افغانستان.

قانون مجازات اسلامی ایران.

کانال تلگرامی خبرگزاری اصلاحات پرس@ads_eslahaat_press .

کانال تلگرامی خبرگزاری تسنیم@tasnimnewsadmin .

کنت سی لاودن، جین پی لاودن .*فناوری اطلاعات و ارتباطات؛ مفاهیم و کاربردها* .ترجمه حمید محسنی. ویراست سوم. تهران: نشر کتابدار، 1392.

کنوانسیون جرایم سایبری بوداپست 2001.

گنسلر، هری جی .*درآمدی جدید به فلسفه اخلاق* .برگردان حمیده بحرینی. چاپ اول. تهران: نشر آسمان خیال، 1385.

محسنی، فرید .*حریم خصوصی اطلاعات (مطالعه جزا در حقوق ایران، ایالات متحده آمریکا و فقه امامیه)* . چاپ دوم. تهران: انتشارات دانشگاه امام صادق، 1394.

محمد بن یعقوب کلینی .*الاصول من الکافی* .ج 2، ص 354 و 355.

محمدنسل، غلامرضا .*حقوق جزای اختصاصی جرایم کامپیوتری در ایران* .چاپ دوم. تهران: نشر میزان، 1395.

مصباح یزدی، محمدتقی .*فلسفه اخلاق* .چاپ اول. تهران: شرکت چاپ و نشر بین‌الملل، چاپ خانه سپهر، 1381.

میرعمادی، طاهره .*مبانی حقوق ملی و شهروندی در فضای تبادل اطلاعات* .چاپ اول. تهران: مؤسسه تحقیقات و توسعه علوم انسانی، 1387.

نجفی ابرند آبادی، علی حسین و حبیب‌زاده، محمد جعفر و بابایی، محمدعلی. "جرایم مانع (جرایم بازدارنده) ".*مجله مدرس علوم انسانی* .(1383) 37

نورمحمدی، مرتضی .*گسترش فناوری‌های اطلاعات و ارتباطات و تحول امنیت* .چاپ اول. تهران: میزان، 1390.

نوری، محمدعلی، نخجوانی، رضا .*حقوق حمایت اطلاعات‌ها* .چاپ اول. تهران: کتابخانه گنج دانش، 1383.

نوکاریزی، محسن، نارمنجی، سید مهدی .*آشنایی با اطلاعات و ارتباطات* .چاپ اول. تهران: انتشارات سمت، 1392.

ویلیامز، ماتیو .*بزهکاری مجازی؛ بزه، انحراف و مقررات‌گذاری برخط* .مترجمین امیر حسین جلالی فراهانی و محبوبه منفرد. چاپ اول. تهران: نشر میزان، 1391.

Banisar, David. *Privacy and Human Rights: An International Survey of Privacy Law and Developments.* 1st ed. Washington, D.C.: Electronic Privacy Information Center, 2000, p. 2.

De Sola, Ralph. *Crime Dictionary.* New York: Facts on File, 1982, p. 47.

Katyal, Neal Kumar. *Criminal Law in Cyberspace.* Accessed [date]. www.nealkatyal.com, p. 3.

About the Authors

Dr. Mohammad Ali Rezayee, *Assistant Professor, Criminal Law Department of Law and Political Science Faculty, Kabul University, Kabul, Afghanistan. <mali.rezayee@gmail.com>*
Mr. Ehsanullah Faisal, *Assistant Professor, Criminal Law Department of Law and Political Science Faculty, Kabul University, Kabul, Afghanistan. <fehsanullah@gmail.com>*