جرایم سایبری و پزشکی قانونی دیجیتال

اثری از:

Thomas J. Holt, Adam M. Bossler, and
Kathryn C. Seigfried-Spellar

مترجمین:

دکتر محمد سعید شفیعی	استاد دانشگاه آزاد اسلامی مرکز اصفهان (خوراسگان)
دکتر مهرنوش ابوذری	استادیار دانشکده حقوق دانشگاه تهران
فرسیما خامسی‌پور	مدرس دانشگاه و عضو باشگاه پژوهشگران جوان و نخبگان دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)

سرشناسه	: Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar
عنوان و نام پدیدآور	: جرایم سایبری و پزشکی قانونی دیجیتال/ اثری از امون کربین... [و دیگران]؛ مترجمین: محمدسعید شفیعی و دیگران...
مشخصات نشر	: تهران، کتاب آوا، ۱۳۹۷
مشخصات ظاهری	: ۴۵۶ ص
شابک	: ۹۷۸-۶۰۰-۳۴۶-۴۹۵-۷
وضعیت فهرست نویسی	: فیپا
یادداشت	: Cybercrime and Digital Forensics
یادداشت	: مهرنوش ابوذری ۱۳۶۷، فرسیما خامسی‌پور ۱۳۷۱
شناسه افزوده	: کارابن، ایمون
شناسه افزود	: شفیعی، محمدسعید، ۱۳۴۸، مترجم
رده‌بندی کنگ	: HV ۱۳۹۷۶۷۷۳ ۴د۹/
رده‌بندی دیویی	۲۵۹۶۸/۳۶۳
شماره کتابشناسی ملی	: ۵۵۵۸۰

انتشارات کتاب آوا

جرایم سایبری و پزشکی قانونی دیجیتال

مؤلفین:	Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar
مترجمین:	محمدسعید شفیعی – مهرنوش ابوذری – فرسیما خامسی پور
ناشر:	کتاب آوا
نوبت چاپ:	اول- زمستان ۱۳۹۷
شمارگان:	۱۰۰۰
قیمت:	۵۵,۰۰۰ تومان
شابک:	۹۷۸-۶۰۰-۳۴۶-۴۹۵-

نشانی مراکز پخش: تهران، خیابان انقلاب، خیابان ۱۲ فروردین، بن‌بست حقیقت، پلاک ۴، واحد ۴

شماره های تماس: ۶۶۹۷۴۱۳۰ - ۶۶۴۰۷۹۹۳ - ۶۶۹۷۴۶۴۵ دورنگار: ۶۶۴۶۱۱۵۸

www.avabook.com Email: avabook_kazemi@yahoo.com

نشانی فروشگاه: اسلامشهر، خیابان صیاد شیرازی (خیابان دانشگاه)، داخل کوچه فرمانداری

شماره تماس: ۵۶۳۵۴۶۵۱

فهرست مطالب

مقدمه: [1]

امروزه فناوری اطلاعات صرف نظر از موقعیت جغرافیایی، در تمامی شئون زندگی وارد شده است و هریک از افراد، بسته به نیاز خود از مزایای این علم بهره مند می شوند. گرچه فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیده بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نماند است دنیای ارتباطات و فضای سایبر، فرصتهای جدید و بسیار پیشرفته ای را برای قانون شکنی در اختیار کاربران خود قرار داده که امکان رفتارهای ضد اجتماعی و مجرمانه مهیا شده است.

به طور کلی، آنچه امروزه تحت عنوان جرم سایبر قرار می‌گیرد، دو طیف از جرائم است: گروه اول جرائمی هستند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه‌شان، با امکاناتی که در اختیار مجرمان قرار می‌دهد، ارتکابشان را تسهیل می‌کند. جرائم تحت شمول این حوزه بسیار گسترده‌اند و از جرائم علیه امنیت ملی و حتی بین‌المللی نظیر اقدامات تروریستی گرفته تا جرائم علیه اموال و اشخاص را در برمی‌گیرند. اما طیف دیگر جرائم سایبر، به سوء استفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرائمی نظیر دسترسی غیرمجاز به داده ها یا سیستمها یا پخش برنامه‌های مخرب نظیر ویروسها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرائم سایبری محض نیز گفته می‌شود.

جرائم رایانه‌ای ـ سایبری را در قالب سه نسل مورد بررسی قرار می‌دهند که قابل توجه می باشد:

نسل اول جرائم رایانه‌ای: همانگونه که از عنوان پیداست، این نسل به ابتدای ظهور سیستمهای رایانه‌ای، به ویژه زمانی که برای اولین بار در سطح گسترده‌ای در دسترس عموم قرار گرفتند، مربوط می‌شود. در آن زمان، عمده اقدامات غیرمجاز، به ایجاد اختلال در کارکرد این سیستمها و به تبع آن دستکاری داده‌ها مربوط می‌شد.

---

[1] مهرنوش ابوذری- استادیار و عضو هیات علمی دانشگاه تهران- گروه حقوق جزا و جرم شناسی

نسل دوم جرائم رایانه‌ای: این نسل از جرائم پل ارتباطی میان نسل اول و سوم بوده و دلیل بارز آن هم عمر بسیار کوتاه این نسل است که به سرعت با ظهور نسل سوم منتفی شد. این رویکرد که از اواخر نسل اول زمزمه‌های آن شنیده می‌شد، به دلیل محوریت یافتن داده‌ها اتخاذ گردید. دلیل آن هم این بود که در دوران نسل اول، سیستمهای رایانه‌ای به تازگی پا به عرصه گذاشته بودند و عمدتاً به شکل سیستمهای شخصی یا رومیزی بوده و به همین دلیل به تنهایی مورد توجه قرار گرفته بودند. اما به تدریج با توسعه و ارتقای فناوری رایانه و به کارگیری آن در بسیاری از ابزارها و به عبارت بهتر رایانه‌ای شدن امور، به تدریج ابزارهای رایانه‌ای جایگاه خود را از دست دادند و محتوای آنها یعنی داده‌ها محوریت یافت. بدیهی است در این مقطع مباحث حقوقی و به تبع آن رویکردهای مقابله با جرائم رایانه‌ای نیز تغییر یافت، به نحوی که تدابیر پیشگیرانه از جرائم رایانه‌ای با محوریت داده‌ها و نه وا بسته‌ها تنظیم شدند. حتی این رویکرد در قوانینی که در آن زمان به تصویب می‌رسید نیز قابل مشاهده است.

به این ترتیب، سیستمهای رایانه‌ای در صورتی در دوران نسل دوم، ایمن محسوب می‌شدند که داده‌های موجود در آنها از سه مولفه برخوردار بودند: ۱. محرمانگی: داده‌ها در برابر افشا یا دسترسی غیرمجاز حفاظت شده باشند؛ ۲. تمامیت: داده‌ها در برابر هرگونه تغییر یا آسیب حفاظت شده باشند؛ و ۳. دسترس‌پذیری: با حفظ کارکرد مطلوب سیستم، داده‌ها همواره در دسترس مجاز قرار داشته باشند.

هم اکنون، این سه مولفه در حوزه ی جرائم نسل سوم از جایگاه ویژه‌ای برخوردارند و حتی در اسناد قانونی به صراحت به آنها اشاره شده است.

برای مثال، عنوان اول از بخش اول فصل دوم کنوانسیون جرائم سایبر بودا پست، ۲۰۰۱)، به جرائم علیه محرمانگی، تمامیت و دسترس‌پذیری داده‌ها و سیستمهای رایانه‌ای اختصاص دارد. در ذیل این عنوان، پنج ماده به طور مفصل جرائم این حوزه را برمی‌شمرند که عبارتند از: دسترسی غیرقانونی، شنود غیرقانونی، ایجاد اختلال در سیستم و سوء استفاده از دستگاهها.

این دوره با وجود عمر کوتاه خود، تاثیر بسزایی در تحول نگرش به جرائم رایانه‌ای داشت. حتی می توان گفت، تقریباً از این زمان بود که اصطلاحاتی نظیر جامعه ی اطلاعاتی یا حقوق کیفری اطلاعات به طور رسمی در اسناد قانونی وارد شد.

نسل سوم جرائم رایانه‌ای: از اوایل دهه نود، با جدی شدن حضور شبکه‌های اطلاع‌رسانی رایانه‌ای در عرصه بین‌الملل و به ویژه ظهور شبکه جهانی وب که به فعالیت این شبکه‌ها ماهیتی تجاری بخشید، بحث راجع به ابعاد گوناگون فضای سایبر به ویژه مسائل حقوقی آن، وارد مرحله جدیدی شد. زیرا تا آن زمان شبکه‌های رایانه‌ای در ابعاد منطقه‌ای، محلی و در حوزه‌های محدودی نظیر سیستمهای تابلوی اعلانات که عمدتاً جهت بارگذاری و پیاده‌سازی برنامه‌ها، پیامها و همچنین ارتباطات پست الکترونیک به کار می‌رفتند به فعالیت می‌پرداختند.

بنابراین می توان گفت فضای سایبر، فرصت های تازه و بسیار پیشرفته‌ای را برای قانون شکنی در اختیار انسان می‌گذارد، هم‌چنین توان بالقوه ارتکاب گونه‌های مرسوم و کلاسیک جرایم را به شیوه‌های غیر مرسوم و بسیار جدید سوق می‌دهد تا مجرمان سایبری بتوانند در این کهکشان صفر و یک، هرآنچه می‌خواهند در آن اندیشه دارند، به منصه ظهور برسانند. این امر، علوم مختلف و از جمله جرم‌شناسی را با تحول روبرو ساخت.

لذا با گسترش فرصت های فعالیت مجرمانه در فضای سایبر و نگرانی مردم از این جرایم، توجه اختصاصی حقوقدانان و جرم شناسان به جرایم ارتکابی در این فضا جلب شد و منجر به ایجاد حوزه مطالعاتی جرم شناسی سایبری گردید.

گرچه عده ای معتقدند حوزه سایبری وسیله ای نوین برای ارتکاب جرایم سنتی(جرایم ارتکابی در فضای واقعی) هستند و لذا آورده جدیدی نیستند که برایشان قائل به قانون جدید و مباحث نظری جدید باشیم اما عقیده غالب که با گذشت زمان و توسعه جرایم سایبری از حیث کمی و کیفی و تنوع انواع و اشکال، بر آن صحه گذاشته شده، قائل است اینترنت فضای جدیدی با ماهیتی کاملا متفاوت از فضای واقعی (جرایمی مانند هک کردن) خلق کرده است.

از این رو جرایم سایبری به علت مزایایی که مجرمان در آن می بینند، رو به گسترش است. ویژگی های مطلوب و مزایای حضور مجرمانه در فضای سایبر این است که از یک سو ارتکاب آنها آسان بوده و با کمترین ریسک از جهت احتمال دستگیری یا عدم موفقیت و شناسایی، به نتیجه مطلوب خود می رسند که با هویت و مکان ناشناس و چه بسا غیرقابل شناسایی، در دنیایی شناور و سیال به فعالیت مجرمانه و حیات خود ادامه می دهند که در اغلب موارد بزهدیده بر بزهدیدگی خود مطلع نمی شود یا بسیار دیر بر آن آگاهی می یابد و حتی در اغلب موارد غیرقانونی بودن آنها روشن نمی باشد. یک ویژگی خاص جرایم سایبری این است که وقوع می یابند بدون آنکه صحنه جرم داشته

باشند. به علاوه، مجرمان به دلیل عدم رویت فوری آثار و نتایج رفتار مجرمانه شان، راحت تر مرتکب جرم می شوند. این امر باعث سهولت از بین بردن آثار جرم می گردد. سرعت بالای ارتکاب جرم و قابلیت تکرار فراوان نیز از ویژگی های دیگر این جرایم می باشد. جرایم سایبری غالبا بسیار سریع به وقوع می پیوندند و از شروع جرم تا اجرای آن فاصله ای وجود ندارد. گاهی فاصله، تنها به اندازه فشردن یک کلید است. از سوی دیگر، جرایم سایبری معمولا ماهیت سریالی دارند و با یک بار ارتکاب، مجرم به اعمالش خاتمه نمی دهد. هم چنین این امر به ویژگی خاص این فضا نیز برمی گردد که داده ها در این فضا به سادگی گسترش یافته و به طور خودکار تکرار می گردند و محو آن به سادگی ممکن نیست. تعطیل ناپذیر بودن و امکان وقوع جرم در هر زمان شبانه روز و هر روز هفته، وجه دیگر این جرایم است که زمینه گستردگی وقوع آن و افزایش رغبت افراد در ارتکاب این جرایم را فراهم می آورد.

لذا نکته قابل توجه، نقاط در حال وقوع جرایم سایبری و ضرورت توجه چندجانبه به این جرایم است. از همین رو، برنامه هایی که به منظور پیشگیری از جرایم سایبری ارائه می‌شوند باید به این امر توجه داشته باشند. نکته دیگر، قابلیت اعمال برخی نظریات جرم‌شناسانه مربوط به جرایم فضای سنتی بر جرایم این فضای نوین و جستجوی نظریه های جدید در تبیین جرایم سایبری است.

شکل گیری جرم شناسی سایبری یک تبیین میان رشته ای از جنبه های عملی و مباحث نظری در باب جرایم سایبری را با شناخت علوم رایانه ای فراهم می سازد. به دلیل رشد روزافزون اینترنت و علوم کامپیوتری فناوری اطلاعات، باعث شده جرم شناسی سایبری به تدریج از یک مطالعه حاشیه ای به یک شاخه اصلی و با اهمیت در جرم شناسی تبدیل شود.

بحث جرم شناسی سایبری در سال ۲۰۰۷ توسط جایشانکار مطرح شد. در سال ۲۰۰۸ ایشان نظریه ای را در تبیین منسجم جرم شناسی سایبری به نام « نظریه جابجایی مکانی» مطرح کرد و در این نظریه جرایم در فضای سایبری را توضیح داد. جرم شناسی سایبری مطالعه عوامل ایجاد جرم در فضای مجازی و تاثیرات آن بر دنیای حقیقی و راهکارهای پیشگیری از حدوث اینگونه جرایم می باشد.نظریه جابجایی مکانی یا انتقال فضا، تفسیری درباره ماهیت رفتار اشخاصی است که رفتار هنجار و ناهنجار خود را در فضای فیزیکی و سایبری نشان می دهند. این نظریه اختصاصا برای جرایمی که با استفاده از اینترنت واقع می شوند، شکل گرفته است و بیان می دارد که مردم هنگامی که به دنیایی با ویژگی های مطلوبشان وارد می شوند، ممکن است به گونه متفاوتی رفتار کنند که سبب گرایش افراد به ارتکاب جرم و همچنین بزهدیدگی آنان گردد.

لازم به ذکر است در بحث جرم شناسی جرایم سایبری مطالعات اندکی صورت گرفته است که این امر می تواند به دلیل سرعت تغییرات فناوری و نیاز به مشارکت و حضور فعال در فضای سایبری برای تبیین آن و دشواری هایی در رسیدن به یک توافق جامع در هنجارهای رفتاری فضای سایبر است. کمااینکه رقم سیاه بزهکاری در این جرایم نیز بسیار بالا می باشد. در اثر عواملی همچون عدم آگاهی و شناخت کامل بزهدیدگان این جرایم، ترس از لطمه به اعتبار شرکت و از دست دادن اعتبار سرمایه گذاران، عدم تخصص ضابطان قضائی در شیوه کشف و تعقیب این جرایم و فقدان امکانات کافی در این خصوص، مشکلات فنی خاص در کشف و اثبات آنها رقم سیاه در جرایم سایبری بسیار بالاست. لذا متخصصان، اطلاعات موجود در زمینه جرایم سایبری را مانند کوه یخ می دانند.

در واقع این واقعیت را باید پذیرفت که هنوز برداشت عمل مجرمانه در بسیاری از فعالیت‌های سایبری که فی‌الواقع جرم هستند، نمی‌شود. لذا نقش فرهنگ‌سازی در اینجا پررنگ می‌گردد. می‌توان گفت برای ارتقای امنیت و کاهش جرایم در فضای سایبر، سه مولفه قابل توجه هستند: حاکمیت، پلیس، مردم. در جرایم سایبری، نقش حاکمیت به دو دلیل عمده بسیار برجسته می‌گردد. نخست آنکه، مجرمان بابت اعمالشان احساس شرمساری نمی‌کنند زیرا عملشان را جرم نمی‌دانند. در برخی موارد، مشاهده شده فرد به دلیل احساس میهن پرستانه اش اقدام به برخی جرایم سایبری نموده است، مانند هک کردن سایت‌های دشمن یا ویروس‌های متخاصم . این امر، می تواند نتایج بسیار مخرب و خطرناک برای کلیت جامعه و امنیت ملی به بار آورد و چه بسا دامنه جنگی گسترده را فراهم نماید.

عامل دیگر، مباحث مربوط به تبادلات مالی و گسترده شدن بانکداری الکترونیک بدون توجه به فراهم آوردن بسترهای فرهنگی در این زمینه و آگاهی رساندن مناسب به مردم می‌باشد.

لذا حتی گاه مردم از اینکه بزهدیده یک جرم سایبری شده‌اند، ناآگاه هستند. این ناآگاهی، دامن خانواده ها را نیز می گیرد. فقر علمی خانواده‌ها در این زمینه و پیشرو بودن فرزندانشان امری است که منجر به عدم نظارت شایسته والدین بر فعالیت فرزندانشان در این فضا می گردد. این خانواده‌ها که با سفر چندروزه فرزندانشان با دوستان خود مخالفند، به یک‌باره فرزند خود را برای سفری جهانی در کنار هزاران غریبه در دنیای سایبر رها می سازند که این امر می تواند افزایش جرایم سایبری – خواه در بزهکاری این نوجوانان و خواه در بزهدیدگی آنان- را در پی داشته باشد.

ویژگی های خاص این فضا و ناآگاهی مردم و نبود زیرساختهای فرهنگی لازم برای حضور در این فضا، عنصری تشویق کننده برای مجرمین گشته است که علاوه بر مجرمان خاص فضای سایبر، مجرمان

فضای واقعی نیز دامنه جرایمشان را از فضای واقعی به دنیای سایبر انتقال داده اند و به نوعی پدیده « کوچ مجرمانه » شکل گرفته است. ارتقاء سطح اطلاعات جامعه نسبت به فضای مجازی و اطلاع رسانی در زمینه جرایم سایبری و راههای مقابله با آن، ارتقاء سطح باورهای اخلاقی خصوصا در بین نوجوانان و جوانان نمونه‌هایی از پیشگیری از شکل گیری جرایم در فضای مجازی است.

هم چنین از آنجا که خسارات وارده بر اثر جرائم سایبری به مراتب گسترده‌تر و جبران ناپذیرتر درمقایسه با جرائم سنتی است، و با توجه به تهدیدات و آسیب های این محیط علیرغم مزایای فراوان آن، لازم است به خوبی بر آن اشراف داشته و این تهدیدات مستمرا شناسایی شوند تا بتوان در عصر حاضر با افزایش ادراک از تأثیر و کاربرد فضای سایبر بر ماهیت جرم و انحراف، بهتر مقابله نموده و از بروزسازی پیشگیری نمود.

کتاب حاضر از آثار نویسنده ارزشمند در حوزه تبیین جرایم سایبر از منظر جرم شناختی و نقش آن در دستاوردهای علمی علوم جنایی مدرن می باشد که پیرامون ماهیت جرایم سایبری و بررسی اقسام آن شامل هک کردن، خدمات اتصال تکنیک کامپیوتری و آسیب رسانی بدافزارها، دزدی دیجیتالی، کلاهبرداری اینترنتی، جرایم جنسی رایانه ای، آزار و اذیت آنلاین و مزاحمت سایبری، ترور سایبری، نقش ادله اثبات و جرم یابی دیجیتال و چشم انداز آینده جرایم سایبری مباحثی ارزشمند و بسیار جدید و به روز را مطرح نموده است که قطعا اثار قابل استناد و ارجاع در حوزه شناسایی جرایم سایبری و جرم شناسی سایبری می باشد.