واکاوی و بررسی ابعاد امنیتی و حقوقی قانون جرایم رایانه ای

علی حسن بابایی[1]

چکیده

در این مقاله با آسیب شناسی و بررسی مشکلات قانون جرایم رایانه ای مصوب (۱۳۸۸/۳/۵) مجلس شورای اسلامی به روش مطالعات کتابخانه ای و سپس تعمیم و کارایی آن به جرایم و مشکلات موجود در جامعه و سیستم های رایانه ای مشخص گردید این قانون دارای ایرادات و مشکلات تخصصی است؛ از جمله عدم توجه کافی به حریم خصوصی و حفظ داده های رایانه ای کاربران خصوصی با شخصیت حقیقی، مشخص نبودن دقیق جرایم و تخلفات مالی، اقتصادی و تجاری در فضای سایبری، عدم جرم انگاری علیه محصولات فرهنگی رایانه ای و کاستی هایی در خصوص قانون حمایت از کودکان آنلاین، عدم توجه قانونگذار در زمینه تعیین قضات متخصص و محاکم ویژه رسیدگی به جرایم رایانه ای، در نظر گرفتن جزای نقدی برای جرایمی همچون جاسوسی رایانه ای و اقدام علیه امنیت ملی، عدم توجه به همکاری های بین المللی و قانون کپی رایت و مالکیت محصولات و تولیدات رایانه ای، عدم تصویب ماده قانونی در رابطه با ارسال و انتشار ویروس های رایانه ای و یا کدهای مخرب و داده های ضد امنیتی در سیستم های رایانه ای، عدم جرم انگاری در خصوص اعمالی مانند ارسال و انتشار هرزنامه ها و پیغام های الکترونیکی و تبلیغاتی ناخواسته از موارد مشکلات و نتایج تحقیق می باشد. همچنین تعریفی از قانون امضای دیجیتال در مکاتبات و یا فعالیت های مالی و اقتصادی رایانه ای و ارزش و اعتبار آن نشده است که این موضوع باعث بروز مشکلاتی در اجرای قانون مذکور شده و یا راه های سوء استفاده از آن را برای سودجویان باز می گذارد.

واژگان کلیدی: *قانون جرایم رایانه ای، حقوق شهروندان مجازی، رویکرد انتظامی سایبر.*

---

[1] معاون دادسرای عمومی و انقلاب همدان، کارشناسی ارشد حقوق

مقدمه

با توجه به تصویب قانون جرایم رایانه ای در مجلس شورای اسلامی، این قانون به دلیل گستردگی دامنه موضوعات مرتبط و تغییرات پیوسته و سریع سیستم های رایانه ای و مخابراتی و فضای مجازی دارای نواقص و کاستی هایی می باشد که در این پژوهش به بررسی قانون مذکور پرداخته می شود و در ادامه نیز پیشنهاداتی برای اصلاح این قانون ارایه می گردد. سوء استفاده های رایانه ای با انگیزه مالی آغاز شده (دزیانی، محمدحسین، ۱۳۸۴) و با پیدایش سایبر، این انگیزه قوت بیشتری یافته است، زیرا علاوه بر امکان انواع سوء استفاده ها از داده های واجد ارزش مالی، مانند سرقت کارت های اعتباری، میزان ارتکاب جرایم مالی در دنیای فیزیکی نیز به نحو قابل توجهی افزایش یافته است (جلالی فرهانی، امیرحسین و باقری اصل، رضا، مجلس و پژوهش: ۵۵). با توجه به گسترش امکانات رایانه ای و مخابراتی در سطوح مختلف جامعه، و دسترسی سازمان ها و ارگان های دولتی به فناوری های نوین ارتباطی و رایانه ای، امکان سوء استفاده از این امکانات توسط کاربران عمومی فضای سایبر[۱]، کارکنان و یا شاغلین و یا افراد وابسته به سازمان ها، ادارات، ارگان ها و شرکت های حقوقی وجود دارد. جرایم و تخلفات رایانه ای در سطوح مختلف سازمانی می تواند با استفاده از آدرس ها و دامنه های ثبت شده اینترنتی در فضای مجازی و یا پست الکترونیکی[۲] شخصیت حقوقی، سوء استفاده از خطوط مخابراتی و یا دسترسی و افشای داده های رایانه ای محرمانه صورت پذیرد. همچنین در حالی که بسیاری از کشورهای جهان شرایط استفاده از امضای دیجیتال را فراهم نموده اند، در ایران بحث ها درباره ارگان اداره کننده یعنی مرکز گواهی ریشه (یکی از عناصر مهم زیر ساخت کلید

---

[۱] Cyber space

[۲] E-Mail

عمومی) به پایان نرسیده است. چنین مرکزی در رأس مجموعه های سلسله مراتبی قرار گرفته و مراجع فرعی را تصدیق می کند. شناخت ماهیت و نقش این مرکز در ایجاد اعتماد نسبت به تراکنش های الکترونیکی، قضاوت آگاهانه درباره نهاد اداره کننده آن را ممکن می سازد (مصطفی بختیاروند، ۱۳۸۶، ۱۹۳). از جمله راهکارهای امنیتی درباره پیغام های الکترونیکی، استفاده از مکانیسم های معروف به امضاهای الکترونیکی[۱] است. امضای الکترونیکی به کاربران کمک می کند هنگام دریافت پیغام در اینترنت پدید آورنده آن را شناخته و از اصالت آن اطمینان یابند. از جمله نکات قابل توجه که ضرورت تصویب جرایم رایانه ای و سایبری را توسط قانونگذار ایجاب نموده می توان به موارد زیر اشاره کرد:

۱- اقدام علیه امنیت ملی، تهدیدات جنگ نرم و جاسوسی رایانه ای.
۲- ترویج ابتذال جنسی، فساد و فحشا و رفتار های غیر اخلاقی و هرزه نگاری جنسی.
۳- جرایم علیه کودکان آنلاین و افراد صغیر زیر ۱۸ سال، سوء استفاده های جنسی و اغفال کودکان.
۴- نشر اکاذیب و اخبار کذب، کلاهبرداری های مالی و اینترنتی، جعل اسناد.
۵- جرایم علیه دامنه های سطح بالای کشور و نفوذ غیرمجاز به حریم سایبری حقوقی و خصوصی.
۶- دسترسی غیرمجاز به داده ها یا حامل های داده رایانه ای.

با توجه به اینکه در مباحث حقوقی تعریف جرم از اهمیت ویژه‌ای برخوردار است، تعاریفی در مورد جرم رایانه‌ای از سوی سازمان ها و کشورهای دیگر انجام شده است. از جمله سازمان‌هایی که تعاریف را ارایه کرده‌اند می‌توان به سازمان همکاری و توسعه اقتصادی شورای اروپا، سازمان

---

[۱] Digital Signature

ملل متحد، انجمن بین الملل حقوق جزا و کنوانسیون جرایم محیط سایبر اشاره نمود که گاهاً تفاوت‌هایی هم با یکدیگر دارند. در حقوق ایران تا پیش از تصویب قانون جرایم رایانه ای توسط مجلس شورای اسلامی، تعریف مشخصی از جرم رایانه‌ای وجود نداشت و در رسیدگی به جرایم رایانه‌ای به قوانین مختلف از جمله قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای استناد می گردید[۱]. در قانون مصوب ۱۳۸۸ جرایم رایانه ای نیز تعریفی از جرم رایانه ای به عمل نیامده و صرفاً به مصادیق این گونه جرایم پرداخته شده است. در تصویب قوانین و مقررات کیفری، لازمه ایجاد امنیت و فراهم آورنده شرایط توسعه هر حوزه تکنولوژیکی محسوب می شود و حوزه فناوری اطلاعات و ارتباطات نیز از این قاعده مستثنا نیست. اما برای تهیه قانونی مناسب که حقوق و تکالیف دست اندرکاران این حوزه را تعیین کند، ایجاد زبان مشترک میان حقوق دانان و متخصصین رایانه ای و نگاه قانونگذار به موضوعات مختلف از زاویه دید متخصصین و کاربران آن حوزه، ضرورتی انکار ناپذیر است.

بیان مساله

در دنیای امروز با روند روبه گسترش استفاده از فناوری های نوین و رایانه با مسایل و مشکلات جدیدی مواجه هستیم. سازمان ها و دستگاه های دولتی به منظور ارایه خدمات بهتر به مراجعین و افزایش سرعت ارایه خدمات و کاهش هزینه ها اقدام به استفاده از فناوری اطلاعات و ابزارهای رایانه ای در سطح وسیعی نموده اند. همچنین شمار رشد کاربران فناوری اطلاعات در ایران به سرعت در حال افزایش است. استفاده از فناوری های نوین ارتباطی و رایانه ای دارای مزایای بی شماری است و لیکن علوم رایانه و فناوری اطلاعات مشکلات خاص خود را به همراه

[۱] حسین، علی بای و بابک، پورقهرمان؛ بررسی فقهی و حقوقی جرایم رایانه ای، پژوهشگاه علوم و فرهنگ اسلامی، قم. ۱۳۸۸

آورده است که جامعه و سازمان ها را تحت تاثیر قرار می دهد. جرایم و تخلفات رایانه ای توسط متخصصین فناوری اطلاعات و کاربران رایانه که دارای اطلاعات وسیعی در این زمینه هستند، صورت می پذیرد که وقوع آن در خلاف جهت اهداف مصالح ملی و اجتماعی جامعه است. بنابراین وقوع جرایم و تخلفات رایانه ای با پیچیدگی خاصی صورت می گیرد که شناسایی و کشف این نوع جرایم و تخلفات مستلزم داشتن توانایی استفاده از رایانه و آشنایی تخصصی با فناوری اطلاعات می باشد تا با استفاده از دانش کافی و توانایی لازم در این زمینه به مقابله اصولی و تخصصی با این نوع جرایم و تخلفات پرداخت و از ادامه آن جلوگیری نمود. در این مقاله و پژوهش، قانون جرایم رایانه ای مصوب مجلس شورای اسلامی مورد بررسی و واکاوی قرار می گیرد و میزان کارایی آن مشخص خواهد شد. همچنین پیشنهاداتی در راستای ارتقاء سطح کیفی قانون مذکور و رفع نقایص و کاستی های آن ارایه می گردد. قانون جرایم رایانه ای به لحاظ ساختار با رعایت اصول کنوانسیون جرایم سایبر که در سال ۲۰۰۱ در بوداپست مجارستان به تصویب شورای اروپا رسید، تدوین شده است. بنابر آمارهای رسمی بیش از ۳۵ میلیون کارت الکترونیکی نزد کاربران سامانه های خدمات الکترونیکی بانک ها، ۱۰ میلیون کارت نزد کاربران سامانه هوشمند سوخت و ۵۰ میلیون مشترک تلفن همراه و ثابت و ۱۸ میلیون کاربر اینترنت در کشور وجود دارد[۱]. در سال ۱۳۸۸ در ایران بیشترین جرایم رایانه‌ای و اینترنتی و طرح شکایت در حوزه فناوری اطلاعات مربوط به ثبت دامنه در فضای سایبر و اختلاف بر سر دامنه بین اشخاص حقیقی و حقوقی بوده است و پس از این موضوع اختلاف بین کاربران اینترنت با شرکت‌های سرویس‌دهنده و سپس اختلاف بین شرکت های اینترنتی و سرویس دهندگان با یکدیگر است که بیش از ۸۵ درصد از این دعاوی به سازش و صدور حکم منجر و پرونده

---

[۱] خلاصه گزارش اظهارنظر کارشناسی درباره لایحه جرایم رایانه ای؛ مرکز پژوهش های مجلس شواری اسلامی، ۱۳۸۷/۵/۱۹

مختومه اعلام شده و در برخی موارد که نیاز به کار کارشناسی بوده جهت بررسی بیشتر بسته نشده است[۱]. در سال ۱۳۸۵ تعداد ۷۹ پرونده در خصوص جرایم رایانه ای به سیستم پلیس آگاهی کشور وارد شده است که ۳۳ درصد پرونده‌ها در رابطه با موضوع دسترسی غیرمجاز به سیستم ها و داده‌های رایانه‌ای، بخشی از آن دسترسی های غیرمجاز در حوزه فعالیت های بانکی، ۳۰ درصد پرونده ها با موضوع هتک حیثیت افراد و نشر اکاذیب، ۱۶ درصد پرونده‌ها با موضوع کلاهبرداری های اینترنتی یا تولید و انتشار برنامه ها و کدهای مخرب و فریب سیستم های رایانه ای، ۶ درصد بحث تخریب و اختلال در داده های سیستم و ۵ درصد تکثیر غیرمجاز نرم‌افزارها و محتوای دیجیتال بوده است[۲]. امروزه تولیدکنندگان محتوا به یک سری بنگاه های خاص محدود نیستند و هر فرد می تواند انواع رسانه ها از جمله رادیو اینترنتی، پادکست و برنامه های تصویری ایجاد کند. مهم ترین جرایم اینترنتی در جهان انتشار اخبار کذب، ارسال مطالب، تصاویر و فیلم های مستهجن، آموزش و تبلیغ تروریسم، هتک حرمت افراد، استفاده از فضای متعلق به دیگران، ارسال پیام های مخرب، اخلال دسترسی دیگران در فضای سایبری، دین زدایی، هک و ویروسی کردن سایت ها و ... می باشند. استفاده از فضای سایبر نیز یک فناوری جدید برای ارتکاب جرم است. لذا به دلایل زیر وضع حقوق جزای مستقل برای جرایم رایانه ای ضرورت دارد:

۱- دنیای مجازی به طور سمبلیک، دنیایی جدید است که باید از طریق قانونگذاری مستقل مانند دنیای واقعی آن را به نظم در آوریم.

---

[۱] تارنمای گرداب، مرکز بررسی جرایم سازمان یافته وابسته به فرماندهی پدافند سایبری سپاه پاسداران انقلاب اسلامی ایران

[۲] سرهنگ مهرداد امیدی، معاون مبارزه با جرایم خاص رایانه ای پلیس آگاهی کشور

۲- مجرمان سایبر از لحاظ جرم شناسی از مجرمان عادی متفاوت هستند و قوانین جزایی و مجازات های متفاوتی را نیاز دارند.

۳- ضرر و زیان ناشی از جرایم سایبر بسیار بیشتر از جرایم عادی است.

۴- مشکلات ناشی از شیوه های کشف جرم و تعقیب متهمان و به مجازات رساندن آنها و خصیصه بین المللی این جرایم به آنها ماهیتی متفاوت از جرایم سنتی می بخشد.

نکته اساسی در جرایم اینترنتی حذف مکان در قلمرو مکان فیزیکی و محدود حاکمیت سیاسی است. ممکن است جرم در خارج از محدوده جغرافیایی و قلمرو حاکمیت کشور انجام شود و جرم انگاری لازمه نادیده گرفتن اصل صلاحیت سرزمینی و توسعه مرزهای جغرافیایی است[1]. در ادامه به واکنش تقنینی کشورها در مورد جرایم رایانه‌ای پرداخته می شود که واکنش نانوشته کشورها در برابر تجاوز و تعدی به ارزش ها در پنج مرحله، سیستم قضایی خود را جهت در برگرفتن قوانین مربوط به جرایم رایانه‌ای اصلاح کردند و این پنج مرحله عبارتند از:

مرحله اول: حمایت از اطلاعات خصوصی.

مرحله دوم: ایجاد و اصلاح قوانین ناظر به جرایم رایانه‌ای.

مرحله سوم: وضع قوانین جدید جهت حمایت از دارایی‌های غیرمادی.

مرحله چهارم: تفکیک قوانین موجود با قوانین و موضوعات جدید.

مرحله پنجم: اصلاح قوانین در مورد جرایم مربوط به محتوا.

همچنین یکی از دغدغه های اصلی امروز در دنیای سایبر، محتوای ناخواسته الکترونیکی یا همان هرزنامه[2] است که ماهیتی تبلیغاتی دارد و با مقاصد تجاری و غیرتجاری برای کاربران سیستم های پیام رسان الکترونیکی ارسال می شود. به طور کلی، اقداماتی که باید در چارچوب

---

[1] ز . رنجبر زواره، کارشناس ارشد حقوق مالکیت فکری

[2] Spam

قانونگذاری انجام شود را می توان در دو محور اساسی گنجانید: ۱- مبارزه با محتوای غیرقانونی، ۲- جرم انگاری علیه محتوای ناخواسته و زیان بار.

سوالات و فرضیه ها

در پژوهش انجام شده و بررسی مشکلات قانون جرایم رایانه ای و طرح فرضیه های آن، به طور کلی سه فرضیه و پرسش مطرح است:

۱- جرایم و تخلفات رایانه ای در سطوح مختلف سازمانی چگونه و از چه طریقی ممکن است صورت پذیرد؟

۲- راه های مقابله با جرایم و تخلفات رایانه ای و پیشگیری از وقوع این جرایم چیست؟

۳- نقاط قوت و ضعف و مشکلات قانون جرایم رایانه ای مصوب مجلس شورای اسلامی چیست؟

به طور کلی جرایم رایانه ای در سطوح مختلف سازمانی می تواند در دو قسمت مورد بحث و بررسی قرار گیرد :

۱- حوزه جرایم و تخلفات رایانه ای در سازمان ها و ادارات دولتی و یا وابسته به قوای سه گانه که با استفاده از امکانات رایانه ای و مخابراتی به انتشار اطلاعات و یا افشای حامل های داده در فضای سایبر و یا سهل انگاری در حفظ امنیت داده ها و اطلاعات رایانه ای می تواند صورت پذیرد و یا با سوء استفاده از امکانات و داده های رایانه ای در جهت بهره برداری مالی و اقتصادی و منافع شخصی، اقدام علیه امنیت و منافع ملی، اقدامات سیاسی بر ضد حاکمیت قابل ارتکاب است. داشتن مشاغل و مسئولیت هایی همچون کارمندان بانک ها، موسسات مالی و یا نهادهای نظامی، انتظامی و یا قضایی

در خصوص ایجاد وقفه و یا تاخیر در پردازش داده های رایانه ای و یا انتقال آنها در فضای سایبری و مخابراتی می تواند منجر به وقوع جرم شود.

۲- جرایم سازمان یافته توسط تیم ها و تشکیلات سازمانی رایانه ای و سایبری که از آن جمله می توان به راه اندازی باندهای فساد و گروه های ضداخلاقی و انتشار تصاویر مستهجن و روابط جنسی در فضای سایبر، ایجاد گروه ها و تشکیلات سازمانی تروریستی در فضای مجازی و یا گروه های سازمان یافته تبلیغات بر علیه حاکمیت نظام و یا نشر اکاذیب و مسموم سازی فضای سیاسی، تشکیل گروه های سازمان یافته سرقت الکترونیکی و نفوذگران به منابع مالی و اخلال گران امنیت بانکداری الکترونیکی، تشکیلات سازمانی تولید و انتشار ویروس ها، بد افزارها و کدهای مخرب و ضد امنیتی رایانه ای اشاره کرد.

معرفی قانون جرایم رایانه ای

قانون جرایم رایانه ای شامل سه بخش اصلی، ۵۶ ماده و ۲۵ تبصره است و در روز سه شنبه مورخ پنجم خرداد ماه یکهزار و سیصد و هشتاد و هشت (۱۳۸۸/۳/۵) در صحن علنی به تصویب مجلس شورای اسلامی و مورخ بیستم خرداد ماه یکهزار و سیصد و هشتاد و هشت (۱۳۸۸/۳/۲۰) به تایید شورای نگهبان رسیده است. این قانون تحت عنوان فصل جرایم رایانه ای به قانون مجازات اسلامی (بخش تعزیرات) تحت مواد ۷۲۹ الی ۷۸۵ اضافه و آورده شده است. قانون مذکور دارای سه بخش اصلی به شرح زیر است :

بخش یکم - شامل ۸ فصل (مواد ۷۲۹ تا ۷۵۵) جرایم و مجازات ها

بخش دوم - شامل ۳ فصل (مواد ۷۵۶ تا ۷۷۹) آیین دادرسی

بخش سوم- شامل (مواد ۷۸۰ تا ۷۸۵) سایر مقررات

یافته ها

ایرادات تخصصی و حقوقی قانون جرایم رایانه ای

با مطالعه و پژوهش در قانون مصوب و مقایسه آن با قوانین جرایم سایبری کنوانسون اروپا و قانون مجازات اسلامی (بخش تعزیرات فصل اول، جرایم علیه امنیت داخلی و خارجی جاسوسی) همچنین تعمیم کارایی آن با مشکلات موجود، مشخص گردید ایرادات و مشکلات موجود در قانون جرایم رایانه ای به شرح زیر می باشد:

۱. در قانون جرایم رایانه ای همانند جرایم سیاسی و تروریستی تعریفی جامع و مانعی از این جرایم به عمل نیامده و صرفاً عناوین و مصادیق جرایم ذکر شده است.
۲. در قانون جرایم رایانه ای مصوب مجلس شورای اسلامی، تنها حفظ تمامیت داده ها و سیستم های رایانه ای و مخابراتی حقوقی، دولتی و وابسته به قوای سه گانه مورد توجه قرار گرفته است و کمتر به حفظ حریم مجازی و داده های الکترونیکی و رایانه ای کاربران خصوصی و اشخاص حقیقی توجه شده است.
۳. عدم جرم انگاری تمامی جرایم رایانه ای و سایبری مانند هرزنامه ها، تبلیغات الکترونیکی و سایبری، فروش اطلاعات هویت فردی کاربران فضای سایبر (آدرس و دامنه اینترنتی، پست الکترونیکی و مشخصات شخصی) به موسسات تبلیغاتی و جاسوسی.

۴. عدم توجه کافی به حریم کاربران عمومی و عدم حمایت از حقوق خصوصی افراد در فضای سایبر همچون حفظ داده های رایانه ای، اطلاعات شخصی و یا آدرس ها و دامنه های اینترنتی.

۵. عدم جرم انگاری و تشدید مجازات جرایم علیه هرزه نگاری کودکان، اطفال و افراد صغیر و ارتباط آنها با محتویات مستهجن در فضای سایبری و رایانه ای.

۶. مشخص نبودن دقیق جرایم و تخلفات مالی، اقتصادی و تجارت شبکه ای (تجارت الکترونیک و شبکه ای) و جرایم علیه تراکنش های مالی و بانکی (بانکداری الکترونیک و اینترنتی).

۷. فقدان ضمانت اجرای مناسب و پشتوانه قوی قانونی در مواردی همچون ضعف مواد قانون در مبارزه با جاسوسی رایانه ای و عدم پیش بینی دادگاه یا شعبه ویژه رسیدگی کننده به جرایم رایانه ای و قضات متخصص.

۸. عدم تفکیک و طبقه بندی لازم و دقیق در برخی جرایم مانند (انتشار ویروس، هرزنامه و برنامه های ضد امنیتی، انتشار کدهای مخرب، نفوذ به رایانه های شخصی و یا دولتی و نظامی، دسترسی به اطلاعات شخصی افراد).

۹. فقدان مجازات های جایگزین متناسب با فضای سایبری و یا تشدید مجازات جرایم سازمان یافته رایانه ای و یا تساهل و تخفیف جزای کیفری و نقدی در برخی از موارد ارتکاب جرایم و تعدیل مجازات های برخی از مواد قانون.

۱۰. عدم توجه به امضاهای دیجیتالی به عنوان ابزار احراز هویت و استناد به آن جهت تصدیق هویت کاربری در فضای سایبر.

۱۱.عدم حمایت از ثبت و نگهداری دامنه های اینترنتی و آدرس های الکترونیکی (اشخاص حقیقی و حقوقی).

۱۲.قانون جرایم رایانه ای دارای ضعف همکاری های بین الملل می باشد، زیرا به مسایل مرتبط با قانون کپی رایت و حفظ حقوق مالکیت فردی در فضای مجازی و رایانه ای و احترام به حقوق تجاری محصولات رایانه ای توجه نگردیده است. به منظور ارتقاء همکاری های بین المللی لازم است ابتدا به این موضوع به صورت قانون نگریسته شود تا از زیان اقتصادی ملی در حوزه تولیدات و محصولات رایانه ای و سرقت آنها جلوگیری شود.

۱۳.عدم جرم انگاری و شفاف سازی جرایم علیه محصولات فرهنگی رایانه ای.

۱۴.عدم وجود منع قانونی نگهداری، جمع آوری و انتشار اطلاعات شخصی افراد صغیر در فضای سایبر، حامل های الکترونیکی و داده های رایانه ای بدون آگاهی و کسب اجازه والدین آنها.

۱۵.عدم توجه کافی به حریم خصوصی کودکان و تشدید مجازات علیه جرایم جنسی و هرزه نگاری و سوء استفاده یا انتشار مطالب جنسی افراد کمتر از ۱۸ سال.

استناد پذیری تخصصی و جمع آوری ادله الکترونیکی

در فصل سوم - استنادپذیری ادله الکترونیکی قانون جرایم رایانه ای نواقصی در خصوص استناد به موارد نقض امنیت داده های رایانه ای وجود دارد و این کاستی ها ناشی از غیر تخصصی بودن این فصل از قانون است. بررسی تخصصی و فنی ادله الکترونیک مستلزم شناخت کافی قانون از موارد و اصطلاحات تخصصی رایانه ای و جرایم مرتبط با آن است. با توجه به گستردگی جرایم و

تخلفات رایانه ای و همچنین پیدایش روش ها و ابزارهای جدید برای اقدام به جرم رایانه ای، تعریف و تشخیص کامل این موارد بسیار دشوار است.

نتیجه گیری و پیشنهادها

برای اصلاح کاستی ها و مشکلات قانون جرایم رایانه ای، باید نگاهی میان رشته ای بر این قانون حاکم شود که برای تعیین حقوق و تکالیف یک حوزه تکنولوژیکی نوشته می شود. این قانون باید شامل دیدگاهی باشد که منعکس کننده دغدغه‌ها و مشکلات متخصصین همان حوزه باشد، نه اینکه تنها دیدگاه های حقوقی و غیر فنی را در برگیرد. بنابر ضرورت استفاده از امضای دیجیتال در فعالیت های رایانه ای و تصدیق هویت کاربری، پیشنهاد می گردد ماده قانونی به قانون جرایم رایانه ای با موضوع امضای دیجیتال افزوده شود. امضاهای الکترونیکی به این شرح تعریف شده است: "امضای الکترونیکی عبارت است از هر نوع علامت رایانه ای منظم شده یا به نحو منطقی متصل شده به داده پیام، که برای شناسایی امضا کننده به کار می رود." همچنین پیشنهاد می گردد در ماده هایی از قانون مصوب همچون ماده (۸) که عنوان سیستم های رایانه ای و مخابراتی ذکر شده است، عنوان "فضای مجازی" که بیانگر دنیای مجازی اینترنت و امکانات موجود در فضای سایبری است به آن اضافه شود. پس از جمع بندی بررسی مشکلات قانون جرایم رایانه ای در این پژوهش پیشنهادات اصلاحی جهت رفع مشکلات و تشخیص جرایم رایانه ای در ذیل ارایه می گردد:

۱- انتشار هر نوع ویروس و برنامه مخرب رایانه ای، کدهای مخرب الکترونیکی، برنامه های ضد امنیتی و زیان آور به صورت محصولات رایانه ای در فضای مجازی و پایگاه های داده ای

رایانه ای وابسته به مراکز دولتی و وابسته به قوای سه گانه، خصوصی، اشخاص حقیقی و حقوقی به هر نحو که باعث زیان و خسارت مادی و یا از بین رفتن داده ها، تغییر و تحریف داده ها و یا سرقت دادها شود جرم محسوب شده و شامل مجازات کیفری و حقوقی می گردد.

۲- هر نوع تحریف، تغییر و یا اغفال در ارجاع ارتباطات و لینک های[۱] رایانه ای در فضای مجازی به لینک ها و مطالب غیر واقعی و غیر مرتبط با موضوع مشخص شده به صورت موضوعات ضد امنیتی و انحرافات اخلاقی و یا ایجاد ارتباطات فریبنده به اسناد آلوده به کدهای مخرب و برنامه های زیان آور و یا ویروس های رایانه ای در اینترنت و یا محصولات رایانه ای جرم محسوب می شود.

۳- امضای الکترونیکی به عنوان دلیل در دادگاه پذیرفته شده و از همان قدرت اثباتی امضای سنتی برخوردار خواهد بود.

۴- در انجام امور بانکداری الکترونیکی، تجارت الکترونیکی و فعالیت های اقتصادی رایانه ای در فضای مجازی و سایبری، برای قانونی کردن فعالیت تجاری و اقتصادی استفاده از امضای دیجیتال و گواهی احراز هویت الزامی و ضروری است.

۵- انتشار هرزنامه و هر نوع پیام های تبلیغاتی رایانه ای و ارسال آن به سیستم های رایانه ای و مخابراتی و یا فضای مجازی دولتی و یا وابسته به قوای سه گانه و یا ارسال و انتشار هرزنامه به کاربران خصوصی در صورت عدم تمایل کاربران به وسیله ابزار و یا امکانات رایانه ای و با استفاده از شیوه ها و روش هایی که به طور ناخواسته و خودکار پیغام ها را وارد سیستم و حریم مجازی کاربران می کند و باعث اشغال شدن حجم و فضای حافظه رایانه ای آنها شود، جرم محسوب می گردد.

---

[۱] Link

۶- هرگونه سوء استفاده مالی و کلاهبرداری و صدور وعده های مالی خلاف واقع در فضای مجازی و سیستم های رایانه ای و مخابراتی به منظور بهره برداری اقتصادی و مادی جرم محسوب می شود.

۷- هرگونه سوء استفاده از امکانات رایانه ای و مخابراتی دولتی و یا وابسته به قوای سه گانه که دارای شخصیت حقوقی هستند به هر نحو (استفاده از آدرس اینترنتی، سوء استفاده از IP رایانه ای، استفاده از شماره تلفن ثبت شده و استفاده غیر مجاز از عناوین قانونی) برای فریب افکار عمومی و یا انتشار مطالب خلاف واقع و نشر اکاذیب از این طریق که به نام شخصیت حقوقی انجام می شود جرم محسوب می گردد.

۸- هرگونه کپی برداری، تکثیر و یا انتشار غیر قانونی محصولات رایانه ای و یا مطالب مندرج در سایت های اینترنتی بدون رعایت قانون کپی رایت جرم محسوب می شود.

۹- فروش، افشا و یا در دسترس قرار دادن مشخصات هویت فردی و شخصی کاربران خصوصی و عمومی، حقیقی و حقوقی پست الکترونیکی، فروش آدرس پست الکترونیکی کاربران فضای سایبر، دامنه و آدرس های اینترنتی وبگاه ها (سایت ها) در فضای سایبر توسط ارایه دهندگان خدمات میزبانی و یا مدیران سایت های اینترنتی که به اطلاعات و داده های اشاره شده دسترسی دارند به موسسات تبلیغاتی و یا جاسوسی جرم محسوب می شود.

۱۰- قانون جرایم رایانه ای به طور شفاف به موضوع جرایم علیه محصولات فرهنگی رایانه ای اشاره نکرده است و در این خصوص پیشنهاد می شود ماده ای با عنوان محصولات فرهنگی رایانه ای با محوریت:

۱-۱۰. محصولات صوتی و تصویری (ویدیویی)

۲-۱۰. محصولات بازی و سرگرمی

۳-۱۰. برنامه ها و نرم افزارها

۴-۱۰. آثار هنری و ترسیمی (تجسمی)

۵-۱۰. پویانمایی (انیمیشن و متحرکت سازی) و دیگر محصولات فرهنگی

تصویب و به قانون افزوده گردیده و بدین ترتیب که علاوه بر قوانین موضوعه دیگر، اصلاح قانون مقرر می دارد تولیدکنندگان محتوای رایانه ای و دیجیتالی اعم از نهادهای حکومتی، دولتی یا وابسته به قوای سه گانه، تولیدکنندگان خصوصی داخلی و خارجی باید محصولات خود را در وزارت فرهنگ و ارشاد اسلامی ثبت و پس از انطباق محصول با معیارهای ارزشی و اسلامی و قانونی و احراز هویت پدیدآورندگان محصول، اقدام به تکثیر و انتشار آن نمایند.

۱۱- در جهت حفظ حریم شخصی، امنیت و عفت اطفال و افراد صغیر زیر ۱۸ سال در فضای سایبری و داده های رایانه ای پیشنهاد می شود ماده قانونی به قانون جرایم رایانه ای افزوده گردد که جمع آوری، نگهداری و استفاده یا افشای اطلاعات شخصی کودکان زیر ۱۵ سال در وب سایت های تجاری و غیر دولتی که به آنها اختصاص دارد ممنوع شود، و این ماده قانون مدیران وبگاه های اینترنتی (سایت های اینترنتی) را موظف می کند اطلاعات شخصی افراد زیر ۱۵ سال را با آگاهی کامل و رضایت معتبر والدین و یا سرپرست قانونی آنها جمع آوری و یا نگهداری و منتشر کنند. این ماده قانون از نگهداری یا جمع آوری و انتشار اطلاعات شخصی افراد صغیر بدون رضایت معتبر والدین آنها در فضای سایبری ممانعت به عمل می آورد.

۱۲- یکی دیگر از مشکلات و کاستی هایی که در قانون جرایم رایانه ای وجود دارد، مبحث خرابکاری رایانه‌ای که اصطلاحاً به آن سابوتاژ رایانه‌ای گفته می‌شود اختصاص دارد و به عنصر قانونی اشاره می شود که در قوانین جزایی سنتی ایران جرمی با این عنوان بیان نشده است، اما برخی مواد قانونی ظهور در مفهوم سابوتاژ دارند. در توضیح به این مطلب اشاره می شود که

سابوتاژ مرسوم غیر از سابوتاژ رایانه‌ای می باشد. به طوری که در قانون جرایم رایانه ای خرابکاری علیه عنصر مادی و یا در اصطلاح تخصصی خرابکاری علیه سخت افزار رایانه ای اشاره نشده است و تنها قانون به جرایم و خرابکاری علیه داده های نرم افزاری و دستکاری، تغییر و یا حذف اطلاعات در فضای سایبر اشاره دارد. در مورد سابوتاژ رایانه‌ای باید گفت: در صورتی که اعمال خرابکارانه علیه سیستم و شبکه رایانه‌ای موارد مندرج در ماده ۶۸۷ قانون مجازات اسلامی به منظور مبارزه و معارضه با نظام سیاسی کشور صورت گیرد، سابوتاژ رایانه‌ای تحقق می‌یابد. از آنجا که مجازات یک نوع برخورد شدید و رسمی حاکمیت با مجرم محسوب می شود و تبعات منفی و هزینه های بسیاری را هم برای مجرم و هم برای جامعه به دنبال دارد (برای نمونه، هزینه های نگهداری مجرم در زندان و یا مشکلاتی که برای خانواده مجرم به وجود می آید) امروزه سعی می شود از ضمانت اجرای غیر کیفری که هم سازنده تر و کم هزینه تر از مجازات کیفری به ویژه زندان هستند استفاده شود. با مطالعه قانون جرایم رایانه ای، متوجه می شویم تنها دو شکل از انواع ضمانت اجرا یا همان مجازات وجود دارد:

۱- جریمه نقدی و مجازات کار اجباری.

۲- حبس و زندان.

این مساله نشان می‌دهد که قانونگذار ماهیت فضای مجازی و منطق برگرفته از ماهیت حقوق کیفری، ویژگی های حوزه فناوری اطلاعات، الزامات تجارت در عرصه ملی و بین المللی و شرایط و مقتضیات جامعه کنونی در توجیه چرایی وضع ضمانت اجرای به کار گرفته شده و حتی جرم انگاری ها را به خوبی در نظر نگرفته است. با این توصیف، این پرسش مطرح می شود که اصولاً قانونگذار چه برنامه ای برای کاستن از میزان یا جلوگیری از ارتکاب جرم دارد و همچنین تناسب ضمانت اجرایی تعیین شده توسط چه مرجعی و با چه استدلالی تعیین شده است.

فهرست منابع

- اظهارنظر کارشناسی درباره لایحه جرایم رایانه ای (۱۳۸۴)، مرکز پژوهش های مجلس شورای اسلامی، دفتر ارتباطات و فناوری های نوین: شماره مسلسل ۷۵۵۲.

- انصاری، باقر (۱۳۸۸)، نقد و بررسی مصادیق محتوای مجرمانه، خبرگزاری ایسنا.

- بختیاروند، مصطفی، ماهیت و جایگاه مرکز گواهی ریشه در تراکنش های الکترونیکی. فصلنامه مجلس و پژوهش، سال ۱۴، شماره ۵۵.

- تأملی بر فیلترینگ (۲. مطالعه تطبیقی سایر کشورها)، دفتر مطالعات ارتباطات و فناوری های نوین، تیرماه ۱۳۸۶.

- جلالی فراهانی، امیرحسین و باقری اصل، رضا، پیشگیری اجتماعی از جرایم و انحرافات سایبری. فصلنامه مجلس و پژوهش، سال ۱۴، شماره ۵۵.

- گروه تحقیق (۱۳۸۴)، جهانی شدن ارتباطات و تهدید امنیت ملی ما، فصلنامه راهبرد، شماره ۳۶، ص ۹۰.

- خانزاده، حمید (۱۳۸۸)، بررسی و تحلیل قانون جرایم رایانه ای. وبلاگ دادگستر.

- زرگر، محمود، امنیت در تجارت الکترونیک. فصلنامه مجلس و پژوهش، سال ۱۴، شماره ۵۵.

- علی بای، حسین و پورقهرمان، بابک (۱۳۸۸)، بررسی فقهی و حقوقی جرایم رایانه ای. نشر پژوهشگاه علوم و فرهنگ اسلامی، قم: چاپ اول.

- فاضلی، محمد، مقدمه ای بر سنجش فساد. مرکز پژوهشهای مجلس شورای اسلامی.

- فیروز منش، افشین (۱۳۸۷)، بررسی قانون جرایم رایانه ای. ماهنامه تحلیل گران عصر اطلاعات.

- مانوئل کاستلز (۱۳۸۰)، عصر اطلاعات و ظهور جامعه شبکه ای، ترجمه: عقیلیان، احمد و خاکباز، افشین، انتشارات طرح نو، تهران.

- مدیر بلاگفا. ابهام در قانون جرایم رایانه ای، مدیا نیوز، مهر ۱۳۸۸.

- میسفادین لی پی (۱۳۸۶)، فرهنگ مجازی، بایدها و نبایدها در فرهنگ IT. ترجمه: پاتازیان، کامبیز.

- نقشینه، وحید (۱۳۸۶)، سلامت دیجیتال. روزنامه ایران، شماره ۳۶۳۶.