دوره هشتم ـ سال اول
شماره چاپ: ۱۲۲
تاریخ چاپ: ۱۳۸۷/۴/۹
شماره ثبت: ۱۲۱

اظهارنظر کارشناسی درباره:

«لایحه جرائم رایانه‌ای»

(گزارش ۱)

کد موضوعی: ۲۸۰
شماره مسلسل: ۹۱۳۸
آبان ماه ۱۳۸۷

به‌نام خدا

فهرست مطالب

اظهارنظر کارشناسی درباره:
«لایحه جرائم رایانه‌ای»

گزارش کنونی مرکز، نسخه بازنگری شده پیشنهادهای گذشته است که در آن پیشرفت‌های فنی، دانش ارتقا یافته حقوق کیفری مرتبط با رایانه و دیدگاه‌های صاحب‌نظران و مسئولان بیشتری لحاظ شده است. از جمله مراجعی که صمیمانه در تهیه متن پیشنهادی جدید یاری رسانیده‌اند عبارتند از: دادستانی کل کشور، دفتر اینترنت دادستانی تهران، شورای عالی اطلاع‌رسانی، وزارت دادگستری، وزارت ارتباطات و فناوری اطلاعات ـ مرکز تحقیقات مخابرات (پژوهشکده امنیت)، وزارت فرهنگ و ارشاد اسلامی و معاونت امنیت عمومی نیروی انتظامی، همچنین لازم می‌دانیم از حمایت‌ها و همکاری‌های معاونت حقوقی و توسعه قضایی قوه قضائیه که در این کار پژوهشی نقش مؤثری داشته‌اند، تشکر و قدردانی نماییم.

مقدمه

باور به اینکه «قانون ایجاد می‌شود تا اجرا نشود» یا اینکه «قانون ایجاد می‌شود تا نقض شود»، هر دو روی یک سکه برای توجیه قانون‌گذاری درباره مسائل و پدیده‌های جدید است. لایحه «**جرائم رایانه‌ای**» که با هدف ضابطه‌مند کردن فضای سایبر تدوین شده است، از یک‌سو به دنبال این آرمان است که از طریق رعایت مقرراتش توسط شهروندان هیچ‌گاه به اجرا درنیاید و ازسوی دیگر، در پی این واقعیت است که اگر توسط افراد نقض شد، ماهیت وجودی‌اش را به تدبیر کیفر به رخ همگان کشد. این لایحه بیش از هر چیز حکایت از تسخیر دنیای انسان‌ها با امکانات خیره‌کننده فضای سایبر دارد و این فضا چنان با مرزها و محدودیت‌ها بیگانه است که به راحتی نمی‌توان حضورش را در میهنمان نادیده انگاشت. بنابراین، چنین فضایی که بیش از پیش در خدمت فعالیت‌های انسانی قرار گرفته، جز با ضابطه‌مندی نمی‌تواند از دام هرج‌ومرج رهایی یابد و لایحه جرائم رایانه‌ای نخستین طلیعه فراگیر قاعده‌مندسازی فضای سایبر با صبغه کیفری است تا نظاره‌گر محیطی جدید و بیکران، اما سالم باشیم.

شاید در این مقطع زمانی، که کلیات لایحه جرائم رایانه‌ای از سوی مجلس شورای اسلامی به تصویب رسیده، بحث راجع به ضرورت اینچنین قانونی بی‌فایده باشد. اما تصریح به این نکته نیز حائز اهمیت است که مهم‌ترین و جامع‌ترین اقدام تقنینی در حوزه حقوق کیفری مرتبط با رایانه به‌شمار می‌آید. هرچند اذعان می‌شود به‌رغم جامعیت نسبی، تمامی شاخه‌های کیفری رایانه‌ای ـ

سایبری را دربرنمی‌گیرد و قانون‌گذار ایرانی باید با جدیت بیشتری به رفع خلأها و نارسایی‌های این حوزه بپردازد. البته نبود قوانین مادر برای شاخه‌های کیفری، دلیل اصلی این نقیصه است. برای مثال، تا زمانی که قانون جامعی راجع به «**حمایت از داده‌ها و حریم خصوصی**»[1] به تصویب نرسد، تقنین جامع مسائل کیفری ناظر به آن محملی ندارد. همچنین است قوانین راجع به «**حق نشر**»[2] یا «**نشر الکترونیکی**» که هریک در جای خود قوانین مستقلی می‌طلبند.

اهم قوانین و سیاست‌های دارای صبغه کیفری که تاکنون راجع به این حوزه تصویب شده‌اند عبارتند از:

۱. قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای، مصوب ۱۳۷۹،

۲. قانون اصلاح قانون مطبوعات (الحاق تبصره «۳» به ماده (۱) راجع به نشریات الکترونیکی)، مصوب ۱۳۷۹،

۳. مصوبه شماره ٤٨٨ شورای عالی انقلاب فرهنگی در سال ۱۳۸۰ راجع به نحوه استفاده از شبکه‌های اطلاع‌رسانی رایانه‌ای (پالایش محتوای مجرمانه)،

٤. قانون تجارت الکترونیکی، مصوب ۱۳۸۲،

٥. قانون جرائم نیروهای مسلح، مصوب ۱۳۸۲ (ماده (۱۳۱))،

٦. قانون اصلاح قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز می‌نمایند، مصوب ۱۳۸٦ (به‌ویژه ماده (۱۰)).

تقریباً مصادف با نخستین تحرکات تقنینی این حوزه، یعنی در نیمه نخست سال ۱۳۸۱، مسئولیت تدوین لایحه‌ای قضایی به «شورای عالی توسعه قضایی» وقت قوه قضائیه که اکنون به «معاونت حقوقی و توسعه قضایی» تبدیل شده واگذار شد. در آنجا با تشکیل «**کمیته جرائم رایانه‌ای**» گروهی از کارشناسان حقوقی، قضایی و فنی به بررسی خلأهای قانونی و تجربیات کسب شده توسط کشورهای پیشرو این عرصه و همچنین اسناد بین‌المللی و منطقه‌ای، به‌ویژه کنوانسیون جرائم سایبر شورای اروپا،[3] مصوب ۲۰۰۱/۱۱/۲۳ پرداختند. تدوین پیش‌نویس حدود یک سال به‌طول انجامید و پس از آن در فرایند ملاحظات نهایی مقامات ارشد قوه، به‌ویژه شخص ریاست محترم قوه قضائیه قرار گرفت و پس از تأیید و تصویب نهایی، در ۲۵ تیرماه ۱۳۸٤ از سوی هیئت دولت تقدیم مجلس شورای اسلامی شد.

پس از اعلام وصول این لایحه از سوی مجلس شورای اسلامی، مرکز پژوهش‌ها با هدف تقویت جنبه‌های مثبت لایحه و رفع نواقص و نارسایی‌های احتمالی آن، دوباره گروهی متشکل از

1. Data Protection - Privacy
2. Copy Right
3. European Convention on Cyber Crime

تدوین‌کنندگان لایحه و کارشناسان و صاحب‌نظران حقوقی، قضایی و فنی را گردهم آورد تا در مدت زمان اندکی که در اختیار داشت، پیشنهادهای ضروری را طی گزارشی کارشناسی به اطلاع نمایندگان محترم برساند که خوشبختانه گزارش تهیه شده، از سوی کمیته‌ای که برای بررسی لایحه در کمیسیون حقوقی و قضایی مجلس تشکیل شده بود، با اقبال مواجه شد.[۱]

با این حال، به دلایل نامعلومی تصویب نهایی این لایحه مسکوت ماند تا اینکه در خردادماه ۱۳۸۷، هیئت وزیران تصویب کرد این لایحه مجدداً در دستور کار مجلس قرار گیرد که متعاقب آن مجلس در شهریورماه کلیات آن را تصویب کرد.

همان‌طور که ملاحظه می‌شود، این لایحه طی سال‌های اخیر فراز و نشیب‌های زیادی را پشت سر گذاشته و درعین‌حال از آنجا که طی این مدت جامعه ما فرایند الکترونیکی شدن را ولو با شتابی نامطلوب طی کرده، اما هر روز خلأ چنین قانونی بیشتر احساس می‌شود و عملاً مسئولان قضایی و انتظامی را در برخورد قانونی با هنجارشکنی‌های مرتبط با رایانه با مشکل مواجه ساخته است.

در این گزارش، اهم مباحث جدیدی که مورد توجه قرار گرفته‌اند، عبارتند از:

- ویرایش فنی ـ ادبی مواد لایحه،
- تفکیک برخی رفتارهای مجرمانه و مدرج کردن کیفرها،
- متناسب کردن مجازات‌های پیشنهادی با جرائم،
- جرم‌انگاری سرقت رایانه‌ای،
- اتخاذ رویکرد جامع در مبارزه با محتوای مستهجن رایانه‌ای، به‌ویژه با هدف حمایت کیفری از کودکان،
- پیش‌بینی مسئولیت کیفری برای اشخاص حقوقی،
- اتخاذ رویکرد جامع نسبت به مسئولیت کیفری ارائه‌دهندگان خدمات (اینترنتی)،
- اصلاح و تکمیل کیفیات مخففه و مشدده جرائم رایانه‌ای،
- پیش‌بینی اقدامات تأمینی در مورد جرائم رایانه‌ای،
- الحاق فصل و مواد راجع به استنادپذیری ادله الکترونیکی،
- تعیین تکلیف راجع به تجهیزات سخت‌افزاری و نرم‌افزاری رایانه‌ای و مخابراتی اختصاص‌یافته به ارتکاب جرائم رایانه‌ای.

---

۱. مرکز پژوهش‌های مجلس شورای اسلامی، گزارش کارشناسی درباره لایحه جرائم رایانه‌ای، شماره ۷۵۵۲، مهرماه ۱۳۸۴.

گزارش توجیهی اصلاحیه لایحه جرائم رایانه‌ای

عنوان لایحه: جرائم رایانه‌ای

عنوان «**جرائم رایانه‌ای**» از آن رو برای لایحه در نظر گرفته شده که:

اولاً این لایحه درصدد جرم‌انگاری رفتارهای سرزنش‌آمیز مرتبط با رایانه، اینترنت و مخابرات بوده که مقررات کیفری فعلی در ارتباط با آن مبهم یا ساکت‌اند. در این میان، ضرورتی نداشت قبل از اصطلاح «**جرائم رایانه‌ای**»، واژه «**مجازات**» آورده شود، زیرا هر جرمی قانوناً به استناد ماده (۲) قانون مجازات اسلامی، مصوب ۱۳۷۰ به این دلیل جرم است که با قید مجازات منع شده است و طبعاً ذکر مجازات در عنوان لایحه لغو است.

ثانیاً هرچند در لایحه، قسمت «**آیین دادرسی**» نیز ذکر شده است؛ اما نمی‌توان ادعا کرد که عنوان «**جرائم رایانه‌ای**» صرفاً جنبه ماهوی دارد، زیرا قسمت شکلی لایحه کلاً پیرامون نحوه رسیدگی به جرائم رایانه‌ای است و از این حیث مقوله‌ای تبعی نسبت به جرائم رایانه‌ای محسوب می‌شود و به‌تبع طرح این عنوان خودبه‌خود مطرح می‌شود. به‌عبارت دیگر، بخش یکم به مباحث ماهوی جرائم رایانه‌ای و بخش دوم به مباحث شکلی جرائم رایانه‌ای می‌پردازد که در هر حال هر دو در ذیل عنوان «**جرائم رایانه‌ای**» قابل جمع هستند.

ثالثاً جرائم رایانه‌ای به جرائمی اطلاق می‌شود که با شرایط و اوصاف و کیفیات متفاوتی در فضای سایبر ارتکاب می‌یابند و چنان نیست که رایانه در حد وسیله برای ارتکاب جرائم سنتی تلقی شود. در این صورت، محمل عقلایی ندارد تا با تغییر وسیله جرم، عنوان جرم تغییر یابد. در فضای سایبر، یا اصولاً جرائم جدید با اقتضای این فضا ارتکاب می‌یابند یا اینکه جرائمی هستند که شرایط و کیفیات تحقق آنها با شرایط و کیفیات جرائم مشابه در قوانین کیفری فعلی متفاوت است. از این رو، به ناگزیر باید طبقه‌بندی جدید «**جرائم رایانه‌ای**» را به رسمیت شناخت. «**رایانه‌ای**» نیز معادل «**کامپیوتری**» است که در راستای استعمال الفاظ فارسی و براساس ماده واحده قانون ممنوعیت به‌کارگیری اصطلاحات بیگانه، مصوب ۱۳۷۵ و با التفات به اینکه یکی از مخاطبان این ماده واحده مراجع قانون‌گذاری هستند، انتخاب شده است.

بخش نخست ـ کلیات

ماده (۱) ـ تعاریف لایحه

الف) داده رایانه‌ای: هر نمادی از واقعه، اطلاعات یا مفهوم به شکلی مطلوب برای پردازش در یک سیستم

رایانه‌ای یا مخابراتی است که باعث می‌شود سیستم‌های ذکر شده کارکرد خود را به مرحله اجرا گذارند.

ب) داده محتوا: هر نمادی از موضوع‌ها، مفهوم‌ها یا دستورالعمل‌ها نظیر متن، صوت یا تصویر، چه به‌صورت در جریان یا ذخیره شده که به‌منظور برقراری ارتباط میان سیستم‌های رایانه‌ای یا پردازش توسط شخص یا سیستم رایانه‌ای به‌کار گرفته شده و به‌وسیله سیستم رایانه‌ای ایجاد شود.

ج) داده حاصل از مبادله داده محتوا: هرگونه داده‌ای که توسط رایانه‌ها در زنجیره ارتباطات تولید می‌شود تا ارتباطی را از مبدأ تا مقصد مسیریابی کند و شامل مبدأ ارتباط، مقصد، مسیر، زمان، تاریخ، اندازه، مدت، زمان و نوع خدمات اصلی و نظایر آن خواهد بود.

د) اطلاعات: عبارت است از داده‌های پردازش شده قابل فهم برای انسان یا سیستم‌های رایانه‌ای یا مخابراتی.

هـ) اطلاعات کاربر: هرگونه اطلاعاتی که در اختیار ارائه‌کننده خدمات باشد و مربوط به مشترک آن خدمات بوده و شامل نوع خدمات ارتباطی و پیش‌نیازهای فنی و دوره استفاده از آن خدمات، هویت مشترک، آدرس جغرافیایی یا پستی یا IP، شماره تلفن و سایر مشخصات شخصی وی است.

و) سیستم رایانه‌ای: هر نوع دستگاه با مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری ـ نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار داده عمل می‌کند.

ز) سیستم مخابراتی: هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکی اطلاعات میان یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکارساز نوری از طریق یک یا چند مسیر ارتباطی به‌وسیله قراردادهایی که برای گیرنده قابل فهم و تفسیر باشد.

ح) ارائه‌دهنده خدمات دسترسی: هر شخص حقیقی یا حقوقی است که امکان ارتباط یا اتصال به اینترنت را برای کاربران فراهم می‌کند و عبارتند از:

۱. **ایجادکننده نقطه تماس بین‌المللی**: ارائه‌دهنده خدمات دسترسی است که امکان ارتباط یا اتصال پرظرفیت به اینترنت را از طریق سیستم‌های ارتباطی برای کاربران فراهم می‌کند.

۲. **ارائه‌دهنده خدمات دسترسی کم‌ظرفیت**: ارائه‌دهنده خدمات دسترسی است که به‌عنوان واسط میان ایجادکننده نقطه تماس بین‌المللی و کاربران عمل می‌کند و امکان ارتباط یا اتصال به اینترنت را برای آنان فراهم می‌کند.

۳. **ارائه‌دهنده خدمات دسترسی حضوری**: ارائه‌دهنده خدمات دسترسی است که امکان استفاده کاربران از اینترنت را به‌صورت حضوری در محلی معین فراهم می‌کند.

ط) ارائه‌دهنده خدمات میزبانی: هر شخص حقیقی یا حقوقی است که فضای لازم را برای ذخیره داده کاربران فراهم می‌کند. ذخیره‌گذاری اطلاعات یا ذخیره موقت اطلاعات در راستای ارائه خدمات

دسترسی، خدمات میزبانی محسوب نمی‌شود.

ی) تدبیرهای حفاظتی: عبارت است از به‌کارگیری روش‌های نرم‌افزاری یا سخت‌افزاری یا ترکیبی از آن دو، متناسب با نوع و اهمیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی، به‌منظور جلوگیری از دسترسی به آنها بدون مجوز مرجع قانونی.

به‌کار بردن لفظ عام «**کلیات**» در مورد «**تعاریف**» بدون ذکر مقرره‌ای دیگر که عمومات و کلیات لایحه را بیان کند، نامناسب است. این قسمت شامل یک ماده مشتمل بر سیزده تعریف از واژگان است که با توجه به دلایل ذیل، پیشنهاد می‌شود به کلی حذف و بخش نخست با عنوان «**جرائم و مجازات‌ها**» جانشین آن شود:

- این واژگان جنبه فنی دارد و نمی‌توان به‌طور جامع و مانع از آنها تعریفی ارائه داد. زیرا با توجه به توسعه حیرت‌انگیز فضای سایبر و ظهور دستاوردها و ابزارها، نرم‌افزارها و عناوین جدید، در عالم اعتبار نیز مفهوم واژگان فنی در حال تغییر و نوسان است. برای مثال، هنوز رابطه بین «اطلاعات رایانه‌ای»، «داده رایانه‌ای» و «محتوای رایانه‌ای» مشخص و معلوم نیست در آینده نزدیک مفهوم و مصادیق آنها به چه میزان در نوسان باشد.
- تعریف نکردن این قبیل واژگان، این حسن را دارد که مقنن بدون محدود کردن این اصطلاحات در قالب الفاظی مبهم و قابل تفسیر که هر لحظه ممکن است نقص آن هویدا شود، قاضی را با ارجاع امر به کارشناس مربوط یاری خواهد کرد تا تعریف و مفهوم روزآمد مورد نظر را درک کند.
- بیشتر تعاریف ارائه شده به‌گونه‌ای در ماده (۲) قانون تجارت الکترونیکی، مصوب بهمن‌ماه ۱۳۸۲ انعکاس یافته‌اند و ضرورتی ندارد تکرار شوند. اصطلاحات «**داده‌رایانه‌ای**»، «**داده‌محتوا**» و «**اطلاعات**»، مشابه «**داده‌پیام**» قانون مذکور (بند «الف» ماده (۲)) تعریف شده‌اند. تعاریف «**داده حاصل از مبادله داده محتوا**» و «**اطلاعات کاربر**» در قالب تبصره در ذیل ماده مربوط به خودشان آمده‌اند و نیازی به اختصاص بخش مجزایی با عنوان «**کلیات**» به آنها نیست. کما اینکه مواردی چون محتویات مستهجن در لایحه تعریف شده، ولی در اینجا نیامده است. «**سیستم رایانه‌ای**» دقیقاً در بند «و» ماده (۲) قانون مذکور تعریف شده است. «**سیستم مخابراتی**» نیز برای قانون‌گذار ایرانی بیگانه نیست و برای مثال تعریفی که حتی قانون‌گذار در سال ۱۳۵۰ در باب تأسیس شرکت مخابرات ایران در ماده (۱) خود ارائه داده، هنوز با مقتضیات کنونی سازگار است.[1] «**ارائه‌دهنده خدمات دسترسی**» نیز با توجه به شقوقی که برای آن ذکر شده، اکنون محملی از اعراب ندارد و

---

۱. البته در تبصره «۱» این ماده، «مخابرات» به‌طور کلی و نه «سیستم مخابراتی» تعریف شده، ولی به اذعان متخصصان این حوزه، همچنان جامعیت خود را حفظ کرده است: *«مقصود از مخابرات در این قانون عبارت است از انتقال و ارسال علائم و نوشته‌ها و تصاویر و صداها و هرگونه اطلاعات دیگر به‌وسیله سیم یا بی‌سیم و یا نور و یا هر رویه الکترومغناطیسی».*

مراجع ذی‌صلاح قانونی (کمیسیون و سازمان تنظیم مقررات ارتباطات رادیویی وزارت ارتباطات و فناوری اطلاعات) اصطلاحات دیگری مانند «تأمین، توزیع و عرضه خدمات» استفاده می‌کنند که احتمال دارد اینها نیز تغییر یابند.[۱] همچنین است «**ارائه‌کنندگان خدمات میزبانی**» که تشخیص آن را باید به مراجع ذی‌صلاح قانونی واگذار کرد. زیرا هر روز جلوه‌ها و شاخه‌های نوپدیدی به این عرصه حساس اضافه می‌شود. در نهایت «**تدبیرهای حفاظتی**»، صرف‌نظر از اینکه با «**رویه مطمئن**» تعریف شده در بند «ط» ماده قانون مذکور همپوشانی دارد، مفهوم کاملاً پویایی است و باید احراز آن را متناسب با شرایط پویای این حوزه به قاضی ذی‌صلاح مربوط واگذار کرد.

- همچنین، لایحه جرائم رایانه‌ای صرفاً صبغه کیفری دارد و این اصطلاحات که همگی کلیدی و اساسی و متعلق به کل فضای سایبر است، باید به‌گونه‌ای ریشه‌ای‌تر و منسجم‌تر شناخته شوند.
- معادل‌های فارسی واژگان رایانه‌ای و اینترنتی چندان دقیق و قابل اتکا نیستند تا از ترجمه تعاریف اسناد بین‌المللی یا مقررات سایر کشورها استفاده کرد. برای مثال، لفظ «**محتوا**» در برابر Content که مفهومی شناخته شده برای غربیان است، چندان یقین‌آور نیست، زیرا اصولاً برای ما رابطه مفاهیمی چون «محتوا»، «ماهیت» و «مضمون» شناخته شده نیست و در اینکه آیا به راستی اطلاعات یا حتی داده‌ها، محتوا باشند، جز سکوت و تردید، اقدام یا ادعای دیگری روا نیست.
- تعریف واژگان و معرفی جزء به جزء اصطلاحات به‌کار رفته در قانون، بیشتر به «نظام حقوق عرفی»[۲] اختصاص دارد که تمام تلاش خود را در جزئی‌انگاری قوانین به‌کار می‌بندد، حال آنکه در کشور ما با وجود قواعد تفسیری و اتکا به برداشت قضات، چنین جزئی‌نگری صورت نمی‌گیرد.
- دست آخر اینکه، چندین تعریف در لایحه آمده که در بخش‌های ماهوی و شکلی به‌کار نرفته‌اند، مانند «خدمات دسترسی کم‌ظرفیت و پرظرفیت». اما همان‌طور که اشاره شد، دو مورد از آنها، یعنی «داده ترافیک» (که معادل دقیق‌تر و بهتر اطلاعات حاصل از تبادل داده محتواست) و «اطلاعات کاربران» در قالب تبصره در جای خود منعکس شده‌اند.

پیشنهاد مرکز ـ حذف بخش نخست و ماده (۱) لایحه

---

۱. آیین‌نامه تأمین، توزیع و عرضه خدمات اینترنت و اینترانت ملی، مصوبه جلسه کمیسیون تنظیم مقررات ارتباطات وزارت ارتباطات و فناوری اطلاعات به تاریخ ۱۳۸۵/۵/۱.

2. Common Law System

بخش دوم ـ جرائم و مجازات‌ها

فصل اول ـ جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

مبحث اول ـ دسترسی بدون مجوز

نکات قابل توجه راجع به این عناوین عبارتند از:

الف) در فصل نخست این بخش و همچنین مبحث نخست این فصل، به‌جای لفظ عربی «**اول**» که با شماره پس از خود، یعنی دوم و سوم نیز همخوانی ندارد، از لفظ فارسی «**یکم**» استفاده شده است که البته واژه «**نخست**» نیز می‌توانست جایگزین آن شود، اما ایراد آن این است که با دوم و سوم همخوانی ندارد.

ب) عنوان مجرمانه «**دسترسی بدون مجوز**» در مبحث یکم به «**دسترسی غیرمجاز**» تبدیل شده است. فارغ از اینکه لفظ «**غیرمجاز**» رساتر و رایج‌تر از «**بدون مجوز**» است، صراحتاً و مؤکداً غیرقانونی بودن رفتار فیزیکی دسترسی را هویدا می‌سازد، اما اصطلاح «**بدون مجوز**»، بیشتر به فقدان نفس مجوز اشاره دارد و حال آنکه مجوز می‌تواند از سوی مرجع قانونی باشد یا مرجع غیرقانونی، یعنی اگر شخصی هرچند بدون مجوز به سیستم رایانه‌ای دسترسی نیافت، اما برای دسترسی از سوی شخص فاقد صلاحیت مجوز داشت، آیا باز هم دسترسی‌اش بدون مجوز محسوب می‌شود؟ این ابهام و کثرت استعمالی که در مقررات گذشته در قبال اصطلاح «**غیرمجاز**» وجود داشت، موجب شد تا این واژه جایگزین «**بدون مجوز**» شود.

پیشنهاد مرکز ـ اصلاح عناوین به:
بخش یکم ـ جرائم و مجازات‌ها
فصل یکم ـ جرائم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی
مبحث یکم ـ دسترسی غیرمجاز

ماده (۲) لایحه

هرکس به‌طور عمدی و بدون مجوز مرجع قانونی، با نقض تدبیرهای حفاظتی داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی، به آنها دسترسی یابد به جزای نقدی از پنج میلیون (۵۰۰۰۰۰۰) ریال تا پنجاه (۵۰۰۰۰۰۰۰) میلیون ریال محکوم خواهد شد.

تغییرات این ماده به‌شرح زیر است:

الف) تعبیر «**به‌طور عمدی**» به‌طور کلی از تمامی مواد لایحه حذف شده است. زیرا اصل بر عمدی بودن

جرائم است و صرف‌نظر از دیدگاه بسیاری از حقوقدانان کیفری که اساساً جرم غیرعمدی وجود ندارد، اگر موارد «**بی‌احتیاطی و بی‌مبالاتی**» را دربرگیرد، قانون‌گذار صراحتاً به آنها اشاره می‌کند. کما اینکه در مواد مربوط، این رویه رعایت شده است. لذا این تعبیر زائد تلقی می‌شود.

ب) تعبیر «**مرجع قانونی**» با سه اشکال اساسی مواجه است. **اولاً** زاید است و واژه «**غیرمجاز**»، عدم صدور از سوی مرجع قانونی را می‌رساند و به‌عبارت بهتر دسترسی غیرمجاز بلافاصله این امر را به ذهن متبادر می‌کند که از سوی مرجع قانونی صادر نشده است. **ثانیاً** مبهم است، زیرا مشخص نیست آیا مرجع قانونی مرجعی است که قانون پیش‌بینی می‌کند یا اینکه شامل هر مرجع صالح از جمله مرجع قضایی نیز می‌شود. **ثالثاً** تفسیربردار است، یعنی مشخص نیست لفظ «**قانونی**» به مرجع برمی‌گردد یا مجوز یا هر دو و اصولاً اگر قانون و مرجع قانونی را مضیق تفسیر کنیم، سخره‌آمیز خواهد بود تا بگوییم برای دسترسی به هر سیستم رایانه‌ای باید سراغ قانون رفت و دید تجویز کرده است یا خیر؟

ج) به‌جای تعبیر «**نقض تدبیرهای حفاظتی**» از «**به‌وسیله تدابیر امنیتی حفاظت شده است**» استفاده شده است. زیرا شرط «نقض تدبیرهای حفاظتی» متضمن این است که مرتکب با به‌کارگیری روش‌های نرم‌افزاری یا سخت‌افزاری یا ترکیبی از آن دو مبادرت به نقض تدبیرهای متناسبی کند که برای سیستم‌ها یا داده‌ها در نظر گرفته شده است و این امر شامل یک‌سری فعل و انفعالات فنی است و حال آنکه دسترسی به سیستم‌های رایانه‌ای با «**اعمال متقلبانه**» یا «**مهندسی اجتماعی**»[1] که متضمن به‌کارگیری نرم‌افزار یا سخت‌افزار رایانه‌ای نیست هم میسر است. از این‌رو، به‌جای این شرط، عبارت «**به‌وسیله تدابیر امنیتی حفاظت شده است**» آمده است. در اینجا فقط لازم است صاحب یا متصدی سیستم یا داده، آنها را با تدابیر امنیتی حفظ کرده باشد، فارغ از اینکه دسترسی به سیستم توأم با نقض آنها باشد یا با روش‌های دیگر. این ماده درواقع درصدد حمایت همه‌جانبه از اقدام اشخاص در اتخاذ تدابیر امنیتی برای سیستم یا داده‌های خود است. غیر از این، لفظ «**امنیتی**» که به‌طور دقیق به تدابیر مرتبط با سلامت سیستم‌ها و داده‌ها اشاره دارد، به‌جای لفظ «**حفاظتی**» که دقیق نیست و هم به تدابیر بیرون از فضای سایبر نیز اشاره دارد، انتخاب شده است.

د) مجازات: حبس یا جزای نقدی یا هر دو: در لایحه برای اکثریت قریب به اتفاق جرائم جزای نقدی پیش‌بینی شده است. اما این تک‌محوری مشکلاتی را به بار می‌آورد: اولاً بیشتر مرتکبان جرائم رایانه‌ای، به‌ویژه آنهایی که مرتکب جرائم خطرناک رایانه‌ای می‌شوند، افرادی خلاق، باهوش و دارای امکانات مادی و معنوی هستند و در غالب موارد، به راحتی توان پرداخت جزای نقدی را

1. Social Engineering

دارند و به‌نظر نمی‌رسد جزای نقدی نسبت به آنها «**بازدارندگی**»[1] مناسبی داشته باشد. ثانیاً مجازات‌های پیشنهادی همان مجازات‌های متداول مقررات کیفری کشورمان و سایر کشورهاست، یعنی جزای نقدی و حبس یا هر دو. حال دادرس با توجه به نوع جرم و سابقه مرتکب و میزان خسارت ناشی از جرم می‌تواند بین جرم و کیفر، تناسب لازم را برقرار کند. ثالثاً در مواردی که جرم اهمیت درخور توجه ندارد، سعی شده تا میزان حبس از حیث حداقل و حداکثر طوری تنظیم شود تا مرتکب مشمول مجازات‌های جایگزین مندرج در «**لایحه مجازات‌های اجتماعی**» که هم‌اکنون در قوه مقننه مطرح است قرار گیرد و مجازات جایگزین متناسب برای وی در نظر گرفته شود تا هم با اطمینان از محکومیت صرف به جزای نقدی گستاخ نگردد و هم با حبس، استعداد وی هدر نرود، بلکه با تعیین مجازات اجتماعی متناسب، مثل خدمات عام‌المنفعه یا ارائه خدمات به نهادهای دولتی، از یک‌سو حضور وی در اجتماع حفظ شود و از سوی دیگر، از استعداد و توانایی وی در راه خدمت به جامعه استفاده شود. رابعاً با عنایت به بین‌المللی و فرامرزی بودن بسیاری از جرائم رایانه‌ای، هم‌اکنون نیز محاکم ما به‌طور فعال با مصادیق «**استرداد**» مجرمان مواجهند و چنانچه از لحاظ مجازات سنخیت لازم وجود نداشته باشد، عملاً تعداد زیادی از مجرمان رایانه‌ای بدون مجازات و آزاد خواهند ماند.

هـ) متناسب کردن جزای نقدی و حبس: برخلاف اکثر مقررات کیفری و همچنین لایحه دولت، در متن پیشنهادی سعی شده بین دو کیفر حبس و جزای نقدی تناسب و توازن برقرار شود. در اینجا هر سه ماه حبس تقریباً معادل پنج میلیون ریال درنظر گرفته شده است. این میزان تقریباً یک سوم تا یک پنجم درآمد یک شخص عادی در کشور ماست و با پرداخت آن به عسروحرج نمی‌افتد. هرچند کیفرها انتخابی و متنوعند و چنانچه از نظر قاضی جزای نقدی قدرت تنبه مرتکب و بازدارندگی را نداشته باشد، می‌تواند حبس را انتخاب کند یا اینکه هر دو را انتخاب کند.

پیشنهاد مرکز ـ اصلاح ماده (۲) لایحه

ماده (۱)

هرکس به‌طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

1. Deterrence

مبحث دوم ـ شنود و دریافت بدون مجوز

عنوان مجرمانه «**شنود غیرمجاز**» در مبحث دوم از فصل یکم، جانشین عنوان «**شنود و دریافت بدون مجوز**» شده است. شنود مفهوم عامی است که «**دریافت**» را هم دربرمی‌گیرد و ذکر دریافت که جنبه فیزیکی آن نیز غالب است، در کنار «**شنود**» زاید می‌باشد. به‌ویژه آنکه برخلاف شنود که اقدامی «**فعالانه**» است، دریافت جنبه «**منفعلانه‌ای**» دارد، لذا صرف دریافت محتوای ارتباطات بدون نقش‌آفرینی فعالانه موجبی برای کیفر به‌شمار نمی‌آید.

پیشنهاد مرکز ـ اصلاح عنوان مبحث دوم به:
مبحث دوم ـ شنود غیرمجاز

ماده (۳) لایحه

هرکس به‌طور عمدی و بدون مجوز مرجع قانونی، داده‌های در حال انتقال در یک ارتباط خصوصی را در سیستم‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری شنود یا دریافت نماید به جزای نقدی از پنج میلیون (۵۰۰۰۰۰۰) ریال تا سی میلیون (۳۰۰۰۰۰۰۰) ریال محکوم خواهد شد.

تغییرات صورت گرفته در این ماده به‌شرح زیر است. لازم به ذکر است به مواردی که دلایل تغییر یا اصلاح آنها پیش از این بیان شد، مجدداً اشاره نمی‌شود:

الف) «**محتوای در حال انتقال ارتباطات غیرعمومی**» به‌جای «**داده‌های در حال انتقال در یک ارتباط خصوصی**» به‌کار رفته است. داده هر نمادی از واقعه، اطلاعات یا مفاهیم قابل پردازش در سیستم رایانه‌ای یا مخابراتی است و مصادیق آن به قدری گسترده است که شامل محتوا و داده ترافیک هم می‌شود. در بزه شنود، هر نوع داده‌ای دریافت نمی‌شود، بلکه محتواست که موضوع این جرم واقع می‌شود و آوردن لفظ «**محتوا**» به‌دلیل عام بودن «**داده**» بود که شامل داده ترافیک نیز می‌شد و اصولاً شنود برای چنین داده‌هایی مطرح نمی‌شود.

ب) تعبیر «**ارتباطات غیرعمومی**» از آن رو به‌جای «**ارتباط خصوصی**» انتخاب شده که **اولاً** مشخص نبود واژه خصوصی در برابر عمومی به‌کار رفته است یا «**دولتی**» یا «**گروهی**»، حال آنکه منظور از ارتباط خصوصی در جرم شنود این است که این ارتباط در مرعی و منظر عموم نباشد و همگان از محتوای داده‌های در حال انتقال اطلاع نیابند. به همین دلیل، «**ارتباط غیرعمومی**» این مفهوم را بهتر و سریع‌تر به ذهن می‌رساند. «**ارتباط غیرعمومی**» ارتباطی است که بین دو یا چند شخص به‌صورت هماهنگ با یکدیگر با مبدأ، مقصد و مسیر انتقال مشخص برقرار می‌شود و شنود محتوای چنین ارتباطی رفتار سرزنش‌آمیز علیه محرمانگی داده‌ها و مستوجب کیفر است.

پیشنهاد مرکز ـ اصلاح ماده (۳) لایحه

ماده (۲)

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

مبحث سوم ـ جرائم علیه امنیت

عنوان مجرمانه «**جاسوسی رایانه‌ای**» در مبحث سوم از فصل یکم به‌جای «**جرائم علیه امنیت**» انتخاب شده است. دلایل این جایگزینی به این شرح است:

الف) جرائم علیه امنیت، آن هم بدون آوردن دو قید «**داخلی**» و «**خارجی**» که در فصل اول باب تعزیرات قانون مجازات اسلامی، مصوب ۱۳۷۵، آمده است، به طیف گسترده‌ای از جرائم اشاره دارد که به‌گونه‌ای با مقوله امنیت مرتبطند. این طیف گسترده از جرائم مدنظر لایحه نبوده و به همین دلیل صرفاً به یک جرم اشاره کرده است. همچنانکه جرائم علیه امنیت ابهام دارند که آیا به دنبال بیان اَعمال قابل کیفر علیه امنیت داخلی یا خارجی کشور است یا امنیت رایانه و فضای سایبر. مهم‌تر اینکه جرائم علیه امنیت با توجه به گستردگی مصادیق آن، چنانچه در فضای سایبر یا از طریق رایانه ارتکاب یابند، لزوماً علیه «**محرمانگی داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی**» نیستند و از این مجرا نیز ذکر عنوان «**جرائم علیه امنیت**» در ذیل فصل یکم با عنوان «**جرائم علیه محرمانگی داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی**» با انتقاد پیش‌گفته مواجه است.

ب) عنوان «**جاسوسی رایانه‌ای**» که خود یکی از مصادیق جرائم علیه امنیت داخلی و خارجی است، عنوان مناسبی است که نه تنها با محتوای مواد (۳)، (٤) و (٥) پیشنهادی مرکز همخوانی دارد، بلکه در زمره برجسته‌ترین جرائم علیه محرمانگی داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی قرار دارد. شاید گفته شود که جرائم موضوع مواد (٤) و (٥) ارتباطی با جاسوسی رایانه‌ای ندارند و با عنوان جرائم علیه امنیت بیشتر مطابقت داشته باشند. اما چنین نیست و جرائم موضوع این دو ماده نیز مستقیماً با جاسوسی رایانه‌ای مرتبطند، زیرا بیشتر کشورها «**مقدمات جاسوسی**» را نیز جرم‌انگاری و این موضوعات را در ذیل جاسوسی رایانه‌ای بحث کرده‌اند. به همین دلیل، از آنجا که نقض تدبیرهای امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سری، از مقدمات قریبه جرم جاسوسی رایانه‌ای است، باید در ذیل همین عنوان مورد بررسی قرار گیرد. همچنانکه ماده (٥) بی‌احتیاطی مأموران را از آن رو جرم‌انگاری کرده که موجب تحقق جاسوسی رایانه‌ای شده‌اند.

پیشنهاد مرکز ـ اصلاح عنوان مبحث سوم به:
مبحث سوم ـ جاسوسی رایانه‌ای

ماده (۴) لایحه

هرکس به‌طور عمدی و بدون مجوز مرجع قانونی، به داده‌های رایانه‌ای به کلی سری و سری موجود در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده دسترسی یابد یا داده‌های رایانه‌ای به کلی سری و سری در حال انتقال را شنود یا دریافت نماید به جزای نقدی از ده میلیون (۱۰۰۰۰۰۰۰) ریال تا یک میلیارد (۱۰۰۰۰۰۰۰۰) ریال متناسب با جرم اتفاق افتاده محکوم خواهد شد.

***تبصره «۱»ـ** داده‌های رایانه‌ای به کل سری داده‌هایی هستند که افشای بدون مجوز آنها می‌تواند به اساس حکومت و مبانی نظام جمهوری اسلامی ایران و تمامیت ارضی آن ضرر جبران‌ناپذیری وارد نماید و منظور از داده‌های رایانه‌ای سری داده‌هایی است که افشای آنها بدون مجوز مرجع قانونی می‌تواند امنیت ملی و یا منافع ملی را دچار مخاطره کند.*

***تبصره «۲»ـ** آیین‌نامه شیوه حفاظت و انتقال داده‌های رایانه‌ای به کلی سری و سری ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت دادگستری و با همکاری وزارتخانه‌های کشور، اطلاعات، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه شده و به تصویب هیئت وزیران خواهد رسید.*

تغییرات به عمل آمده در این ماده به‌شرح زیر است:

الف) «**داده‌های سری**» به‌جای «**داده‌های رایانه‌ای به کلی سری و سری**» به‌کار رفته است. هرچند آیین‌نامه طرز نگاهداری اسناد سری و محرمانه دولتی و طبقه‌بندی و نحوه مشخص کردن نوع اسناد و اطلاعات، مصوب ۱۳۵۴/۱۰/۱ هیئت وزیران، بین اسناد سری و اسناد به کلی سری با توجه به طبقه‌بندی اسناد سری و محرمانه دولتی در ماده (۱) تفاوت قائل شده است؛ اما در قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی، مصوب ۱۳۵۳/۱۱/۲۹، اسناد دولتی به دوگونه است: سری و محرمانه و به همین دلیل در این قانون تنها داده‌های سری منظور شده که هر دو قسم را دربرمی‌گیرد. هرچند جهت تعیین تکلیف راجع به طبقه‌بندی آنها از حیث سری و محرمانه بودن، تنظیم آیین‌نامه‌ای در این زمینه لازم خواهد بود که به این مهم در تبصره «۲» ماده (۳) پیشنهادی اشاره شده است. ضمناً در این ماده «**داده‌های رایانه‌ای سری**» به «**داده‌های سری**» تبدیل شده است، زیرا صفت رایانه‌ای برای داده‌ها، با توجه به اینکه اصولاً این قانون در مورد رایانه و فضای سایبر است ضرورتی ندارد.

ب) تفکیک مراحل مختلف تحقق جاسوسی: در لایحه، برای جاسوسی رایانه‌ای (که البته صراحتاً به این عنوان اشاره‌ای نشده) دو رفتار فیزیکی مجرمانه پیش‌بینی شده است: ۱. *دسترسی به داده‌های سری موجود در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده*، ۲. *شنود یا دریافت آنها در*

حین *انتقال*. اما در ماده (۳) پیشنهادی، مراحل جاسوسی به‌طور جداگانه مورد توجه قرار گرفته‌اند و در ارتباط با هریک، مجازات متناسب پیش‌بینی شده است. این مراحل عبارتند از:

۱. *دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال:* هرچند دسترسی به داده‌ها یا تحصیل آنها یا شنود محتوای رایانه‌ای به‌موجب مواد (۱) و (۲) جرم‌انگاری شده‌اند، اما در این ماده به لحاظ اهمیتی که موضوع جرم (داده‌ها یا محتوای سری) دارد، دوباره مورد توجه قرار گرفته‌اند.

۲. *در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت.*

۳. *افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت، یا گروه بیگانه یا عاملان آنها:* دو قسم اخیر، به‌عنوان بندهای «ب» و «ج» به ماده (۳) اضافه شده‌اند که در اصل این دو بند به جاسوسی رایانه‌ای اشاره دارند که همان در دسترس قرار دادن داده‌های سری برای اشخاص فاقد صلاحیت یا دولت‌ها و گروه‌های بیگانه است.

ج) ارائه تعریف عام از داده‌های سری: در تبصره «۱» ماده (٤) لایحه، داده‌های سری و به‌کلی سری تعریف شده‌اند، اما از آنجا که در ماده پیشنهادی مرکز داده‌های سری شامل داده‌های به‌کلی سری نیز می‌شود، به ارائه یک تعریف کلی و جامع بسنده شده است.

د) اصلاح مجازات: تعیین صرف جزای نقدی برای مرتکب جرم جاسوسی تاکنون در قانون‌گذاری دنیا بی‌سابقه بوده است. حتی در بسیاری از مقررات کیفری، برای جاسوسی، به‌همراه حبس جزای نقدی نیز تعیین نمی‌شود، زیرا با حمایتی که از جاسوس به عمل می‌آید، پرداخت جزای نقدی به هر میزان که باشد، نه تنها امکان‌پذیر است، بلکه اصولاً «**بازدارندگی**» نسبت به جرم ندارد. در عوض، حبس طولانی‌مدت با جرم جاسوسی متناسب است و غیر از این، در اختیار داشتن جاسوس از حیث سیاسی و اطلاعاتی نیز می‌تواند مفید باشد.

ماده (۴) الحاقی مرکز

موضوع این ماده، نقض تدبیرهای امنیتی سیستم‌های رایانه‌ای و مخابراتی به قصد دسترسی به داده‌های سری است که نوعی جرم «**بازدارنده**» تلقی می‌شود تا حفاظت سیستم‌های رایانه‌ای یا مخابراتی حساس، تأمین و مقدمات تحقق جرم جاسوسی حذف شود. نقض تدابیر امنیتی در این ماده با دسترسی غیرمجاز در ماده (۱) متفاوت است. فارغ از اینکه در ماده (۱) لزوماً نقض تدابیر امنیتی شرط نیست، در آن به «**قصد خاص**» نیز اشاره نشده است. اما در ماده (٤) نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی باید به قصد دسترسی به داده‌های سری باشد.

ماده (۵) الحاقی مرکز

موضوع این ماده، بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی منجر به دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سیستم‌های رایانه‌ای و مخابراتی است. جرم موضوع این ماده، هم خاص است و هم غیرعمدی. خاص است به لحاظ اینکه مرتکب جرم فقط مأمور دولتی مسئول حفظ داده‌هاست یا مأموری است که به هر نحو داده‌های مذکور در اختیارش قرار گرفته و غیرعمدی است، زیرا از روی بی‌احتیاطی یا بی‌مبالاتی یا عدم رعایت تدابیر امنیتی باعث می‌شود اشخاص فاقد صلاحیت، به داده‌ها، حامل‌های داده یا سیستم‌های رایانه‌ای و مخابراتی دست یابند. البته در اینجا تصریح شده درصورتی مسئولند که آموزش لازم را دیده باشند تا مقامات مافوق موظف باشند افراد آموزش‌دیده و باتجربه‌ای را بر این امور بگمارند. وضع چنین ماده‌ای به لحاظ حساسیت داده‌های سری و جنبه امنیتی آنهاست که در این قبیل موضوعات و جرائم، قانون‌گذار بی‌احتیاطی یا بی‌مبالاتی اشخاص را هم برنمی‌تابد و پیش‌بینی چنین ماده‌ای ضروری است. به همین منظور، علاوه بر مجازات‌های مرسوم حبس و جزای نقدی، انفصال از خدمت دولتی نیز پیش‌بینی شده تا «**بازدارندگی**» آن تقویت شود.

پیشنهاد مرکز ـ اصلاح ماده (۴) لایحه و الحاق دو ماده

ماده (۳)

هرکس به‌طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب 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 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) افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

تبصره «۱» ـ داده‌های سری داده‌هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می‌زند.

تبصره «۲» ـ آیین‌نامهٔ نحوه تعیین و تشخیص داده‌های سری و نحوهٔ طبقه‌بندی و حفاظت 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 هیئت دولت خواهد رسید.

ماده (۴)

هرکس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۵)

چنانچه مأموران دولتی که مسئول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سیستم‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سیستم‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سیستم‌های مذکور شوند، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

فصل دوم ـ جرائم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

مبحث نخست ـ جعل

عنوان مبحث نخست از فصل دوم لایحه، از «**جعل**» به «**جعل رایانه‌ای**» تغییر یافته است، زیرا عنوان مجرمانه «**جعل**» جنبه سنتی دارد و به‌طور دقیق به ایجاد یا تغییر نوشته با قصد تقلب اشاره دارد که از ماده (۵۲۳) قانون مجازات اسلامی به بعد و در قوانین مختلف پیش‌بینی شده است. به‌کارگیری عنوان «**جعل**» در این لایحه، برخلاف عنوان مشهور و شناخته شده است، زیرا موضوع این جعل نوشته است و هر موضوع خارج از آن، یا در دایره جعل قرار نمی‌گیرد یا محل اختلاف است. پس جعل پیش‌بینی شده در لایحه باید نسبت به جعل مندرج در قانون مجازات اسلامی یا سایر مقررات، اخص باشد که این مهم با عنوان «**جعل رایانه‌ای**» تحقق می‌یابد.

پیشنهاد مرکز ـ اصلاح عنوان مبحث به:
مبحث یکم ـ جعل رایانه‌ای

ماده (۵) لایحه

هرکس با قصد تقلب، داده‌های رایانه‌ای قابل استناد یا داده‌های موجود در کارت‌های اعتباری یا مغناطیسی یا سایر علائم یا کدهای کارت‌های قابل پردازش و یا مورد استفاده در سیستم‌های رایانه‌ای یا مخابراتی را تغییر داده یا ایجاد یا حذف یا متوقف نماید جاعل محسوب شده و به مجازات قانونی مقرر برای جعل محکوم خواهد شد و همچنین هرکس با علم به جعل و تزویر از آنها استفاده کند، به مجازات قانونی مقرر برای استفاده‌کننده محکوم می‌گردد.

تغییرات به عمل آمده در این ماده که در متن پیشنهادی مرکز ذیل ماده (٦) آمده به‌شرح زیر است:

الف) تغییر شیوه نگارش ماده: در ماده پیشنهادی، جعل در قالب دو بند ذکر شده است. نخست *تغییر داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانه داده‌ها. دوم، تغییر داده‌ها یا علائم موجود*

در کارت‌های حافظه یا قابل پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علائم به آنها.

در بند نخست، دو قسم رفتار فیزیکی مدنظر قرار گرفته است: اول تغییر داده‌هایی که نزد مراجع قانونی «**استنادپذیر**»[1] اند، دوم ایجاد یا وارد کردن داده‌ها. از آنجا که داده‌های قسم اخیر برخلاف قسم نخست با قصد تقلب وارد می‌شوند، لازم نیست استنادپذیر باشند و شامل هر نوع داده‌ای می‌شوند.

در بند دوم، به تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن داده‌ها یا علائم به آنها اشاره شده است که نسبت به متن ماده (۵) لایحه کامل‌تر است. لازم به ذکر است، شرط «**متقلبانه بودن**» برای هر دو بند ضروری است.

ب) تعبیر «**قصد تقلب**» در صدر ماده به «**به‌طور غیرمجاز**» تغییر یافته است. با توجه به توضیحات فوق، قصد متقلبانه در قسمت انتهایی در بند پیشنهادی آمده تا مشمول اقدامات خاص مذکور شود. اما برای اینکه اقدامات «**مجاز**» از شمول ماده خارج شود، در ابتدای آن قید غیرمجاز اضافه شده است.

ج) پیش‌بینی مجازات مستقل، به‌جای ارجاع به قانون مجازات اسلامی: ارجاع به قوانینی چون قانون مجازات اسلامی در جرم‌انگاری‌های جدید، صحیح به نظر نمی‌رسد. اولاً ماهیت اعمال ارجاع یافته به آن جرائم متفاوت است و به همین دلیل مشمول جرم‌انگاری جدید شده است و شباهت عناوین دلیلی بر همانندی ارکان و شرایط هر دو جرم نیست. ثانیاً هم‌اکنون قانون مجازات اسلامی در شرف تغییر است و نمی‌توان به آن اتکا کرد.

د) شایان ذکر است در انتهای لایحه، ذیل ماده (۵۸) اصلاحی پیشنهاد شده ماده (٦٨) قانون تجارت الکترونیکی ناظر به جعل رایانه‌ای نسخ شود. این ماده به طرز عجیبی مشوش تنظیم شده و به‌نحوی مباحث سنتی و جدید را درهم‌آمیخته که امکان استناد به خود را سلب کرده است. برای مثال، این موارد قابل ذکرند:

۱. رفتار فیزیکی ارتکاب جعل در دو مرحله ذکر شده است، حال آنکه طبق اصل قانونی بودن جرائم باید رفتار فیزیکی به‌طور مشخص تبیین شود.

۲. جعل با استفاده از سند مجعول تفاوت دارد و با اخذ گواهی مجعول اقدام به جعل کردن معنا ندارد. لذا استفاده از سند مجعول نیز باید به‌طور مجزا قید شود.

---

1. Admissible

۳. جعل رایانه‌ای رفتار مجرمانه مطلق دارد و شروع به آن معنا ندارد.

٤. جالب آنکه در نهایت استفاده از سند مجعول را به‌طور مجزا پیش‌بینی نکرده است.[۱]

ماده (۷) الحاقی مرکز

موضوع این ماده استفاده از داده‌ها یا کارت‌ها یا تراشه‌های مجعول است که همانند مقررات جزایی پیشین که جعل و استفاده از سند مجعول را دو جرم مجزا دانسته‌اند، ضرورت انعکاس آن در اینجا احساس می‌شود. لازم به ذکر است به لحاظ اینکه در فضای سایبر جعل و استفاده از آن در کمترین زمان ممکن قابل تحقق است، چنانچه مرتکب آن یک نفر باشد، فقط باید مجازات جرم جعل را اعمال و کیفیت مشدده لحاظ کرد.

پیشنهاد مرکز ـ اصلاح ماده (۵) لایحه و الحاق یک ماده

ماده (۶)

هرکس به‌طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد:

الف) تغییر داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها.

ب) تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها یا علائم به آنها.

ماده (۷)

هرکس با علم به مجعول بودن داده‌ها یا کارت‌ها یا تراشه‌ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهد شد.

مبحث دوم ـ تخریب و ایجاد اختلال در داده‌ها

از آنجا که عنوان این مبحث با مبحث سوم، یعنی «**اختلال در سیستم**» همپوشانی دارد و همچنین، در سایر مواد، داده‌ها و سیستم‌ها به‌طور یکسان موضوع جرم‌انگاری قرار گرفته‌اند، عنوان مبحث دوم به ترتیب پیشنهادی اصلاح می‌شود.

همچنین، به «**ایجاد اختلال**» دو ایراد وارد است: اولاً «ایجاد» زائد است، ثانیاً «اختلال» بر وزن

---

۱. ماده (٦٨): *«هرکس در بستر مبادلات الکترونیکی از طریق ورود، تغییر، محو و توقف «داده‌پیام» و مداخله در پردازش «داده‌پیام» و سیستم‌های رایانه‌ای و یا استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضا ـ مثل کلید اختصاصی ـ بدون مجوز امضاکننده و یا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و یا عدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل «داده‌پیام‌های» ارزش مالی و اثباتی نماید تا با ارائه آن به مراجع اداری، قضایی و مالی و غیره به‌عنوان «داده‌پیام‌های» معتبر استفاده نماید، جاعل محسوب و به مجازات حبس از یک سال تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون ریال محکوم می‌شود.*

***تبصره ـ** مجازات شروع به این جرم حداقل مجازات در این ماده می‌باشد».*

«افتعال» معنای تأثیرپذیری دارد، حال آنکه چنین مفهومی در اینجا مدنظر نیست. لذا «اخلال» از باب متعدی به معنای اثرگذاری جایگزین آن شده است.

پیشنهاد مرکز ـ اصلاح و ادغام عناوین مباحث دوم و سوم به:
مبحث دوم ـ تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی

ماده (۶) لایحه

هرکس به‌طور عمدی داده‌های رایانه‌ای متعلق به دیگری را از حامل‌های داده یا سیستم‌های رایانه‌ای یا مخابراتی پاک نماید یا صدمه بزند یا غیرقابل استفاده کند یا به هر نحو به‌طور کلی یا جزئی تخریب یا مختل نماید به جزای نقدی از ده میلیون (۱۰۰۰۰۰۰۰) ریال تا یکصد میلیون (۱۰۰۰۰۰۰۰۰) ریال محکوم خواهد شد.

در این ماده یک تغییر اعمال شده و آن جایگزینی رفتارهای فیزیکی «**پاک کردن**» یا «**صدمه زدن**» با «**حذف**» یا «**مختل کردن**» است. زیرا این اصطلاحات سنتی‌اند و با واژگان رایج و فنی رایانه‌ای مأنوس نیستند.

پیشنهاد مرکز ـ اصلاح ماده (۶) لایحه

ماده (۸)

هرکس به‌طور غیرمجاز داده‌های دیگری را از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیرقابل پردازش کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

مبحث سوم ـ اختلال در سیستم

با توجه به توضیحات فوق، این عنوان حذف و در مبحث دوم ادغام شد.

ماده (۷) لایحه

هرکس به‌طور عمدی با انجام اعمالی از قبیل وارد کردن، انتقال دادن، ارسال، پخش، صدمه زدن، پاک کردن، ایجاد وقفه، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را از کار بیاندازد یا کارکرد آنها را مختل نماید به جزای نقدی از ده میلیون ریال تا یکصد میلیون ریال محکوم خواهد شد و چنان‌چه عمل وی به قصد اخلال در نظم و امنیت عمومی باشد و در قوانین دیگر مجازات شدیدتری پیش‌بینی شده باشد، به مجازات

مندرج در همان قانون محکوم خواهد شد.

در ماده (۹) پیشنهادی مرکز، صدر ماده (۷) با اندک تغییراتی حفظ شده است. سایر تغییرات عبارتند از:

الف) به‌جای رفتارهای «**پاک کردن**» و «**ایجاد وقفه**»، واژه‌های مناسب فنی «**حذف کردن**» و «**متوقف کردن**» آمده است.

ب) قسمت انتهایی ماده، به لحاظ اهمیت موضوع و همچنین ابهام در ارجاع مجازات آن، در ماده مستقلی آمده است.

پیشنهاد مرکز ـ اصلاح ماده (۷) لایحه
ماده (۹)
هرکس به‌طور غیرمجاز با انجام اعمالی از قبیل وارد کردن، انتقال دادن، ارسال، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری، سیستم‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آنها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۰) الحاقی مرکز

این ماده به متن پیشنهادی اضافه شده تا خلأ فعل سرزنش‌آمیز «**ممانعت از دستیابی**» را رفع کند. هدف از وضع این ماده، حمایت از حق دسترسی افراد به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی است که با ممانعت دیگری مواجه می‌شوند. البته در ظاهر ممکن است تصور شود که این ماده با مواد مربوط به تخریب و اخلال در داده‌ها یا سیستم‌ها تعارض دارد، اما در بسیاری موارد، ایجاد مانع در دستیابی به داده‌ها و سیستم‌ها ملازمه‌ای با تخریب و اخلال در آنها ندارد. برای مثال، کسی که برای سیستم رایانه‌ای دیگری گذرواژه قرار می‌دهد یا آن را تغییر می‌دهد و مانع دستیابی او به اطلاعات و رایانه‌اش می‌شود، بدون تخریب یا اخلال در داده‌ها یا سیستم‌ها مانع دستیابی شخص مجاز به داده‌ها یا سیستم خویش شده است.

ماده (۱۱) الحاقی مرکز

از آنجا که کلیه نهادهای دولتی و عمومی به تدریج از امکانات رایانه‌ای و اینترنتی استفاده می‌کنند و سعی در رایانه‌ای کردن امورشان دارند، امکان ایراد هرگونه خدشه، به‌ویژه اگر خدمات عمومی ارائه می‌دهند، وجود دارد و بنابراین، جرم‌انگاری اقداماتی که می‌تواند جلوه‌ای از «تروریسم

سایبری»[1] باشد، ضروری به نظر می‌رسد.

ممکن است ادعا شود بین این ماده و جرم موضوع ماده (۹) تعارض وجود دارد، اما باید گفت جرم موضوع ماده (۱۱) ابتدائاً یک جرم رایانه‌ای نیست، بلکه نتایج مورد نظر در این ماده از قبیل اخلال در روند ارائه خدمات یا ایراد صدمه به اموال دولتی یا عمومی، یک مرحله پس از جرم اخلال در سیستم‌ها یا داده‌های موضوع ماده (۹) تحقق می‌یابند. به‌عبارت دیگر، جرم‌انگاری ماده (۱۱) برای جلوگیری از به‌کارگیری سیستم‌های رایانه‌ای و مخابراتی با اعمالی از قبیل دسترسی غیرمجاز یا تخریب داده‌ها یا اخلال در سیستم‌ها برای به مخاطره انداختن رفاه و آسایش و امنیت عمومی است.

پیشنهاد مرکز ـ الحاق دو ماده

ماده (۱۰)

هرکس به‌طور غیرمجاز با انجام اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی شود، به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۱)

هرکس به قصد به خطر انداختن سلامت یا آسایش عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سیستم‌های رایانه‌ای و مخابراتی که برای ارائهٔ خدمات ضروری عمومی به‌کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل‌ونقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهد شد.

فصل سوم ـ کلاهبرداری

کلاهبرداری یک جرم شناخته‌شده در ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری، مصوب ۱۳۶۷ است که متشکل از اجزای توسل به وسایل متقلبانه، فریب قربانی و تحصیل یا بردن مال دیگری است و هر رفتاری که همه این اجزا را نداشته باشد، اما برخی از آن را داشته باشد یا شبیه رفتارها یا اجزای ذکر شده باشد، «**در حکم کلاهبردار**» خواهد بود و از آنجا که جرم موضوع ماده (۱۳) پیشنهادی اجزای و شرایط لازم برای تحقق کلاهبرداری سنتی را ندارد، باید به‌گونه‌ای از این عنوان متمایز می‌گردید که به همین دلیل از تعبیر «**کلاهبرداری مرتبط با رایانه**» استفاده شده است.

همچنین، یکی از نواقص بزرگ لایحه عدم پیش‌بینی ماده‌ای راجع به «**سرقت داده‌های رایانه‌ای**» است که سعی شده در ماده (۱۲) الحاقی مرکز این خلأ رفع شود. توضیحات راجع به آن در ذیل ماده پیشنهادی مرکز آمده است.

1. Cyber Terrorism

پیشنهاد مرکز ـ اصلاح عنوان فصل سوم به:
فصل سوم ـ سرقت و کلاهبرداری مرتبط با رایانه

ماده (۱۲) الحاقی مرکز

نکات اصلی راجع به این ماده با موضوع «**سرقت داده‌های رایانه‌ای**» عبارتند از:

الف) پیش از هر چیز تصریح می‌شود این مقرره هر داده‌ای را مورد حمایت قرار نمی‌دهد. برخی داده‌ها به‌طور خاص مشمول حمایت‌های قانونی هستند و نیازی به نسخ آنها و وضع قوانین جدید به شکل کلی نیست. برای مثال، ماده (٦٢) قانون تجارت الکترونیکی، مصوب ۱۳۸۲ و ماده (۱۳) قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای، مصوب ۱۳۷۹، از داده‌هایی که آثار مورد حمایت قانون در آنها تبلور یافته و همچنین نرم‌افزارهای رایانه‌ای که به‌نوبه خود «داده» به‌شمار می‌آیند، تحت شرایطی حمایت کیفری به عمل آورده‌اند. لذا در اینجا آن دسته از داده‌هایی هدف قرار گرفته‌اند که تحت حمایت هیچ قانونی قرار نگرفته‌اند.

ب) درصورت تصویب ماده پیشنهادی، می‌توان آن را تأیید دیگر قانون‌گذار ایرانی بر «**واجد ارزش مالی بودن**» داده‌ها دانست که در نوع خود یک اقدام ارزنده به‌شمار می‌آید و یک خلأ بزرگ در نظام قانونی ملی را برطرف می‌کند.

ج) در ماده پیشنهادی، از فعل «**ربودن**» برای انتقال داده‌ها استفاده شده است، زیرا نزدیک‌ترین تعبیری است که می‌تواند ماهیت سرقت داده‌ها را انعکاس دهد و تعابیری چون «تصاحب»، «برداشتن» و «انتقال دادن» بار معنایی مطلوب را ندارند.

د) یکی از وجوه تمایز اصلی سرقت داده‌های الکترونیکی با «**اشیای ملموس**» این است که امکان «ربایش» آنها در عین باقی ماندن «اصل داده‌ها» نزد صاحب آن امکان‌پذیر است. اما از آنجا که صرف ربودن و دستیابی به نسخه‌ای از آن داده‌ها، سلطه مالکانه صاحب داده‌ها را نقض می‌کند و قطعاً به وی زیان مادی وارد می‌آورد، می‌بایست تحت شمول ضمانت اجرای کیفری قرار گیرد. اما از آنجا که دو وضعیت ربودن عین داده‌ها یا تهیه نسخه‌ای از آنها با یکدیگر تفاوت دارد، نوع و میزان مجازات آنها متفاوت در نظر گرفته شده است.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۱۲)

هرکس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن

باشد، به جزای نقدی از یک تا بیست میلیون ریال و در غیر این صورت به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۸) لایحه

هرکس از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد، توقف داده‌ها یا اختلال در عملکرد سیستم، سوءاستفاده نماید و از این طریق وجه یا مال یا منفعت یا خدمات مالی و یا امتیازات مالی برای خود یا دیگری تحصیل کند، کلاهبردار محسوب شده و به مجازات قانونی مقرر برای کلاهبرداری محکوم خواهد شد.

مواردی که در ماده پیشنهادی اصلاح شده‌اند عبارتند از:

الف) اصطلاح «**سوءاستفاده**» از این ماده حذف شده است، زیرا افعال فیزیکی مندرج در ماده که به‌صورت غیرمجاز ارتکاب می‌یابند، همگی نوعی سوءاستفاده هستند و لزومی به ذکر این اصطلاح نیست، کما اینکه با آوردن سوءاستفاده در ماده، رابطه بین رفتارهایی مثل وارد کردن، تغییر، حذف و ... با سوءاستفاده از حیث اینکه کدام یک «**رکن مادی**» کلاهبرداری رایانه‌ای را تشکیل می‌دهند مشخص نیست.

ب) مجازات کلاهبرداری از یک تا هفت سال مندرج در ماده یک قانون تشدید، به یک تا پنج سال و جزای نقدی مقرر تغییر می‌یابد، چون مجازات سنگین ماده یک قانون تشدید به‌دلیل مرکب بودن جرم کلاهبرداری و دشوار بودن تحقق و احراز آن است، حال آنکه ماده (۱۳) عملاً نوعی تحصیل مال به‌صورت غیرمجاز را پیش‌بینی کرده که مصادیق آن بسیار است.

ج) درصورت تصویب نهایی این ماده از لایحه یا ماده پیشنهادی مرکز، ضروری است ماده (٦٧) قانون تجارت الکترونیکی با عنوان «**کلاهبرداری کامپیوتری**» نسخ شود، زیرا:

۱. این ماده جرم کلاهبرداری رایانه‌ای را به‌مثابه جرم کلاهبرداری مرسوم یا سنتی آورده که اشتباه است و این دو فعل مجرمانه با یکدیگر فرق دارند. مشخصه بارز آن آوردن شرط «**فریفتن**» است که در جرم کلاهبرداری رایانه‌ای تحقق آن شرط نیست.

۲. برخی ایرادات ماده (۱) قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری، مصوب ۱۳٦۷ در اینجا تکرار شده است. برای مثال، حداقل مجازات مقرر برای شروع به این جرم طبق آن قانون جزای نقدی خواهد بود که معلوم نیست چگونه در جایی که هنوز جرمی ارتکاب نیافته قابل محاسبه است.

۳. بر این ماده آشفتگی عجیبی حاکم است و معلوم نیست از چه سیاق ادبی تبعیت کرده است.

برای مثال، در کنار «سوءاستفاده»، «استفاده غیرمجاز» نیز آمده که هدف از آن مشخص نیست.[۱]

پیشنهاد مرکز ـ اصلاح ماده (۸) لایحه

ماده (۱۳)

هرکس به‌طور غیرمجاز از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم ـ جرائم مرتبط با محتوا

این عنوان به «**جرائم علیه عفت و اخلاق عمومی**» اصلاح شده است. زیرا از یک‌سو، جرائم مرتبط با محتوا نامأنوس و نارساست و مصادیق خود را به‌طور شفاف بیان نمی‌کند و در سایر کشورها و مخصوصاً در کنوانسیون جرائم سایبر نیز غالباً «**هرزه‌نگاری کودکان**»[۲] را دربرمی‌گیرد و مشخص نیست این عنوان منحصر در هرزه‌نگاری است یا شامل سایر جرائم نیز می‌شود. از سوی دیگر، محتوا مفهوم عامی دارد که عنوان «**جرائم مرتبط با محتوا**» نیز بر عمومیت و ابهام آن می‌افزاید، گویی اینکه به هر نوع جرمی که با محتوا مرتبط است اشاره دارد که اگر چنین باشد، اکثر جرائم رایانه‌ای در ذیل آن قرار می‌گیرد و حال آنکه منظور از جرائم مرتبط با محتوا جرائمی است که از طریق تولید یا انتشار تصاویر یا فیلم‌های مستهجن، به عفت عمومی خدشه وارد می‌شود.

پیشنهاد مرکز ـ تغییر عنوان فصل چهارم به:

فصل چهارم ـ جرائم علیه عفت و اخلاق عمومی

ماده (۹) لایحه

هرکس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی محتویات مستهجن را ارائه یا منتشر کند و یا مورد هر قسم معامله قرار دهد و یا به‌منظور انتشار یا تجارت تولید نماید به مجازات مقرر در ماده

---

۱. ماده (٦٧): «*هرکس در بستر مبادلات الکترونیکی، با سوءاستفاده و یا استفاده غیرمجاز از «داده‌پیام»ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف «داده‌پیام» مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره، دیگران را بفریبید و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد، مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از ۱ تا ۳ سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌شود.*

***تبصره ـ** شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده می‌باشد».*

2. Child Pornography

(٦٤٠) قانون مجازات اسلامی محکوم خواهد شد.

***تبصره ـ** محتویات مستهجن به محتویاتی گفته می‌شود که شامل نمایش برهنگی کامل زن یا مرد و یا اندام تناسلی یا نمایش آمیزش و یا عمل جنسی انسان باشد.*

اصلاحات به عمل آمده در این ماده عبارتند از:

الف) واژه «**ارائه**» حذف و به‌جای آن «**توزیع**» آمده است، زیرا مصادیق آن به قدری گسترده است که شامل هر نوع نمایش یا در دسترس قرار دادن یا حتی نشان دادن محتویات مستهجن نیز می‌شود.

ب) در کنار «**تولید**»، «**ذخیره**» به قصد «**انتشار**» یا «**تجارت**» نیز جرم‌انگاری شده است تا افراد از ذخیره این محتویات به قصد انتشار یا تجارت پرهیز کنند. کما اینکه شبیه همین مقرره در رأی وحدت رویه شماره (٦٤٥) هیئت عمومی دیوان عالی کشور، مصوب ۱۳۷۸ مورد تأکید قرار گرفته است. هرچند طبق تبصره «۲» ذیل بند «ب» ماده (۳) قانون اصلاح قانون مجازات اشخاصی که به‌نحوی در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند، مصوب دی‌ماه ۱۳۸٦، حالتی از این اقدام، یعنی «**نگهداری**» نوار، دیسکت و لوح فشرده به کلی ممنوع و برای آن مجازات پیش‌بینی شده است.

ج) تبصره ماده (۹) که به تعریف محتویات مستهجن اختصاص یافته، در راستای اصل شفافیت قوانین کیفری با دقت بیشتری تعریف شده است تا شامل تصویر، صوت یا متن هم بشود و تفاوتی نکند واقعی باشد یا نیمه‌واقعی (مثل تغییر عکس یا فیلم دیگری یا جان‌بخشی به تصویر ثابت دیگری) یا غیرواقعی (مثل کارتون یا پویانمایی). لفظ «**نمایش**» چون جنبه دیداری داشته و با صوت و متن همخوانی نداشت، حذف و به‌جای آن از لفظ «**بیانگر**» استفاده شده است. همچنین این تعریف، از تعریف ارائه شده راجع به آثار سمعی و بصری مستهجن در قانون مذکور، کامل‌تر و تقریباً تمامی مصادیق لازم‌الشمول را دربرمی‌گیرد. در تبصره «۵» ذیل بند «الف» ماده (۳) قانون مذکور آمده است: *«آثار سمعی و بصری مستهجن به آثاری گفته می‌شود که محتوای آنها نمایش برهنگی زن و مرد و یا اندام تناسلی و یا نمایش آمیزش جنسی باشد».*

د) در تبصره «۲» ماده پیشنهادی کیفیت مشدده‌ای لحاظ شده که چشم‌پوشی از آن می‌تواند به نفع سوداگران این حوزه تمام شود. چنانچه شخصی تولید یا توزیع یا انتشار یا معامله محتویات مستهجن را «**حرفه**» خود قرار دهد، شایسته نیست از کیفیات مخففه احتمالی بهره‌مند شود. لذا مقرر شده به حداکثر هر دو مجازات پیشنهادی محکوم شود.

هـ) در پایان، با توجه به انسجام و جامعیتی که بر مجموعه مواد این فصل از لایحه و مواد پیشنهادی آن حاکم است، پیشنهاد شده ماده (۱۰) قانون سمعی و بصری فوق‌الذکر نسخ شود. بالطبع سایر ضوابط راجع به سیستم‌های رایانه‌ای و مخابراتی در آن قانون نیز طبق مصوبه جدید قابل رسیدگی و مجازات خواهند بود.[۱]

پیشنهاد مرکز ـ اصلاح ماده (۹) لایحه

ماده (۱۴)

هرکس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی محتویات مستهجن را منتشر یا توزیع یا معامله کند یا به قصد انتشار یا تجارت تولید یا ذخیره کند، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره «۱» ـ محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی اطلاق می‌شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

تبصره «۲» ـ چنانچه مرتکب اعمال مذکور در این ماده را حرفهٔ خود قرار داده باشد به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

ماده (۱۰) لایحه

اشخاصی که به‌وسیله حامل‌های داده یا سیستم رایانه‌ای یا مخابراتی مرتکب یکی از اعمال زیر شوند به ترتیب زیر مجازات می‌گردند:

***الف)** هرکس محتویات مستهجن را به اشخاص زیر هجده سال تمام ارائه نماید یا محتویات مستهجن اشخاص زیر ۱۸ سال تمام را تولید یا ارائه یا منتشر نماید و یا مورد هر قسم معامله قرار دهد و یا آنها را تهیه یا نگهداری یا ذخیره کند، به حداکثر مجازات مقرر در ماده (٦٤٠) قانون مجازات اسلامی محکوم خواهد شد.*

***ب)** هرکس به‌منظور دستیابی اشخاص زیر هجده سال تمام به محتویات مستهجن یا به‌منظور ارتکاب جرائم مبادرت به تحریک یا ترغیب یا تهدید یا تطمیع یا فریب آنها نموده و یا شیوه دستیابی یا ارتکاب موارد ذکر شده را برای آنها تسهیل نموده یا آموزش دهد به مجازات مقرر در ماده (۶٤۰) قانون مجازات اسلامی محکوم خواهد شد.*

***ج)** هرکس محتویات مستهجن غیرواقعی (از قبیل پویانمایی یا طراحی یا نقاشی) را به قصد ارائه یا انتشار، تهیه یا تولید یا ذخیره یا نگهداری نماید به حداقل مجازات مقرر در ماده (۶٤۰) قانون*

---

۱. ماده (۱۰): «انتشار آثار مستهجن و مبتذل از طریق ارتباطات الکترونیکی و سایت‌های کامپیوتری یا وسیله و تکنیک مشابه دیگر از مصادیق تکثیر و انتشار محسوب و مرتکب حسب مورد به مجازات مقرر در این قانون محکوم خواهد شد».

مجازات اسلامی محکوم خواهد شد.

***تبصره ـ** مفاد مواد (۹) و (۱۰) شامل آن دسته از محتویاتی نخواهد بود که با رعایت موازین شرعی و برای مقاصد علمی یا هر مصلحت حلال عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا انتشار یا ذخیره شده یا مورد معامله قرار می‌گیرد.*

در این ماده، نحوه نگارش عبارات تغییر یافته است تا صراحت و شفافیت آنها بیشتر شود:

الف) در بند «**الف**» پیشنهادی این ماده که جانشین بند «الف» ماده (۱۰) شده است، ارجاع به مجازات ماده (٦٤٠) حذف و با توجه به اهمیت موضوع، مجازات جداگانه‌ای درنظر گرفته شده است.

ب) قید «**تمام**» از ۱۸ سال حذف شده تا این مقرره کیفری از این قشر شدیداً آسیب‌پذیر حمایت مؤثرتر و جامعی به عمل آورد.

ج) در عین حال، به اشخاص «**ظاهراً کمتر از ۱۸ سال**» نیز توجه شده است تا مشکلات تعیین سن در رایانه تا حدود زیادی رفع شود. این تعبیر در کنوانسیون جرائم سایبر نیز به‌کار رفته است، زیرا در اکثر موارد سن اشخاص مورد سوءاستفاده در رایانه درج نمی‌شود و نامشخص است.

د) بند «**ب**» لایحه به دو بند «**ب**» و «**ج**» تبدیل شده است. در بند «**ب**» پیشنهادی، به تحریک یا ترغیب یا تهدید یا اعمالی از این قبیل برای دستیابی اشخاص کمتر از ۱۸ سال به محتویات مستهجن اشاره شده که جنبه هرزه‌نگاری دارد، اما در بند «**ج**» اصولاً هرزه‌نگاری مدنظر نیست و به حمایت همه‌جانبه از اشخاص زیر ۱۸ سال در فضای سایبر در برابر تحریک یا ترغیب یا اعمالی از این قبیل برای ارتکاب جرائم یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز توجه شده است. تفکیک این دو بند، هم از حیث تفاوت موضوع و هم از حیث شکل نگارش ضروری به نظر می‌رسد.

هـ) بند «**ج**» ماده (۱۰) لایحه حذف می‌شود و بند «**ج**» اصلاحی با عباراتی کامل‌تر که از بند «**ب**» منفک شده است، جانشین آن می‌گردد. قابل ذکر است در هر سه بند تغییرات ماهوی صورت نگرفته و بیشتر شکل نگارش اصلاح شده است.

و) از تبصره لفظ «**حلال**» به لحاظ ابهام و همچنین تعارض با مفهوم «**مصلحت**» حذف می‌شود و همچنین عبارت «**موازین شرعی**» نیز به لحاظ اینکه اصولاً درخصوص فضای سایبر مقررات فقهی یا شرعی پیش‌بینی نشده حذف می‌شود. کما اینکه رعایت موازین شرعی به شکلی که در محیط بیرونی و خارجی مطرح است، در فضای سایبر امکان‌پذیر نیست.

پیشنهاد مرکز ـ اصلاح ماده (۱۰) لایحه

ماده (۱۵)

هرکس از طریق سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب مقرر مجازات خواهد شد:

الف) چنانچه محتویات مستهجن را به اشخاص کمتر از ۱۸ سال ارائه کند یا محتویات مستهجن اشخاص کمتر از ۱۸ سال یا ظاهراً کمتر از ۱۸ سال را تولید یا ارائه یا منتشر یا معامله کند یا تهیه یا نگهداری یا ذخیره کند، به حبس از شش ماه تا سه سال یا جزای نقدی از ده تا شصت میلیون ریال یا هر دو مجازات.

ب) چنانچه به‌منظور دستیابی اشخاص کمتر از ۱۸ سال به محتویات مستهجن، آنها را تحریک یا ترغیب یا تهدید یا تطمیع کند یا فریب دهد یا شیوه دستیابی به آنها را تسهیل کند یا آموزش دهد، به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات.

ج) چنانچه اشخاص کمتر از ۱۸ سال را به ارتکاب جرائم یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز تحریک یا ترغیب یا تهدید یا دعوت کند یا فریب دهد یا شیوه ارتکاب یا استعمال آنها را تسهیل کند یا آموزش دهد، به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات.

تبصره ـ مفاد این ماده و ماده (۱٤) شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می‌شود.

ماده (۱۱) لایحه

مضمون این ماده با عنوان فصل چهارم پیشنهادی، یعنی جرائم علیه عفت و اخلاق عمومی سازگاری ندارد. به همین دلیل، باید عنوان متناسب با آن درج شود. به‌ویژه آنکه به ماده (۱۲) لایحه نیز چنین ایرادی وارد است. لذا فصل جدیدی با عنوان «**هتک حیثیت و نشر اکاذیب**» پیش‌بینی شده و برای رعایت ترتیب منطقی مواد فصل جدید، اصلاحیه ماده (۱۱) لایحه به انتهای این فصل منتقل شده است. لذا توضیحات راجع به موارد اصلاحی این ماده پس از بررسی مواد (۱۲) و (۱۳) لایحه خواهد آمد.

پیشنهاد مرکز ـ الحاق فصل پنجم ـ هتک حیثیت و نشر اکاذیب و انتقال اصلاحیهٔ ماده (۱۱) لایحه به دو ماده بعد ذیل ماده (۱۸)

ماده (۱۲) لایحه

هرکس به‌وسیله سیستم رایانه‌ای یا مخابراتی فیلم یا صوت دیگری را تغییر دهد یا تحریف نماید و منتشر سازد یا با علم به تغییر یا تحریف، انتشار دهد به‌نحوی که منجر به هتک حرمت یا ضرر وی گردد، به مجازات مقرر در ماده (٦٤٠) قانون مجازات اسلامی محکوم خواهد شد.

***تبصره ـ** چنانچه عمل مرتکب از مصادیق تعرض به نوامیس مردم باشد به حداکثر هر سه*

مجازات مقرر در ماده (٦٤٠) قانون مجازات اسلامی محکوم خواهد شد.

این ماده با تغییر محتوایی خاصی مواجه نیست. تنها با عنایت به مسائل مطروحه، ارجاع مجازات آن به ماده (٦٤٠) قانون مجازات اسلامی حذف شده است. تبصره این ماده نیز حذف می‌شود، زیرا نه تنها «**تعرض به نوامیس مردم**» تعبیری مبهم است، بلکه چنین رفتاری در فضای سایبر قابل تحقق نیست.

پیشنهاد مرکز ـ اصلاح ماده (۱۲) لایحه و الحاق یک تبصره

ماده (۱۶)

هرکس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به‌نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ـ چنانچه تغییر یا تحریف به‌صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

فصل پنجم ـ افشای سر

این فصل حذف شده است. زیرا افشای سر در ذیل جرائم مرتبط با محتوا قرار نمی‌گیرد و اکنون که از عنوان «**هتک حیثیت و نشر اکاذیب**» استفاده شده، ذیل آن قرار می‌گیرد. کما اینکه اصولاً رفتار فیزیکی افشای سر با توجه به استدلال‌های بعدی در ماده حذف شده و نتیجتاً به‌کار بردن عنوان آن سالبه به انتفای موضوع است.

به‌علاوه، جرم پیش‌بینی شده در ماده (۱۷) پیشنهادی، انتشار صوت یا تصویر یا فیلم یا اسرار خصوصی یا خانوادگی دیگری یا در دسترس قرار دادن آنها بدون رضایت شخص است که جنبه حیثیتی دارد و با عنوان جدید سازگار است.

پیشنهاد مرکز ـ حذف عنوان فصل پنجم ـ افشای سر

ماده (۱۳) لایحه

هرکس به‌وسیله سیستم رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی و خانوادگی یا اسرار دیگری را، به‌جز موارد قانونی، بدون رضایت او منتشر نماید یا در دسترس دیگران قرار دهد به‌گونه‌ای که منجر به ضرر وی شود یا به‌طور عرفی موجب هتک حیثیت او تلقی شود به مجازات مقرر برای افشای سر محکوم خواهد شد.

در ماده اصلاحی مرکز، علاوه بر مجازات که مشخصاً نوع و میزان آن تعیین شده، دو تغییر دیگر نیز اعمال شده است:

الف) تعبیر «**اسرار دیگری**» حذف شده است. زیرا ماهیت سر مشخص نیست و این سؤال را متبادر می‌سازد که آیا همگان باید حافظ اسرار یکدیگر باشند؟ در حالت عادی حفظ سر نسبت به برخی اشخاص مصداق دارد که قانوناً با توجه به وظایف و شغل‌شان، افراد اسرارشان را نزد آنها بازگو می‌کنند، مثل پزشک یا وکیل، وگرنه اگر قرار بود حفظ سر به کلیه افراد سرایت یابد، مفهوم مبهم و مغشوشی پیدا می‌کرد.

ب) تعبیر «**جز در موارد قانونی**» نیز حذف شده است. زیرا اصولاً مقرره قانونی وجود ندارد که به این موضوع حکم دهد و انجام آن حتی از سوی مراجع قانونی نیز قابل تصور نیست.

ج) افشای سر در قوانین ملی مسبوق به سابقه عمومی نیست و تنها موارد و مشاغل خاصی را دربرمی‌گیرد. برای مثال، در قانون وکالت به آن اشاره شده یا ماده (٦٤٨) قانون مجازات اسلامی نیز به موارد خاصی اشاره دارد. لذا با عنایت به اینکه این اقدام به واقع سرزنش‌آمیز در فضای سایبر به‌راحتی قابل ارتکاب است و نبود یک مقرره جامع حمایتی کیفرمدار به‌خوبی احساس می‌شود، این ماده در لایحه پیش‌بینی شده است.

پیشنهاد مرکز ـ اصلاح ماده (۱۳) لایحه

ماده (۱۷)

هرکس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به‌نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

ماده (۱۱) لایحه

هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به‌وسیله سیستم رایانه یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا به‌عنوان نقل قول، به شخص حقیقی یا حقوقی یا مقام‌های رسمی به‌طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یاد شده به‌نحوی از انحا ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت درصورت امکان به مجازات قانونی مقرر برای جرم نشر اکاذیب محکوم خواهد شد.

با توجه به توضیحاتی که داده شد، این ماده به آخرین ماده از فصل پنجم انتقال یافته است.

تغییرات به عمل آمده عبارتند از:

الف) تعبیر «**مقامات رسمی**» از صدر ماده حذف شده است. زیرا نه اضرار به آنها مفهوم دارد، چون از این لحاظ در حکم سایر شهروندان هستند، و نه همانند عموم ذهنشان مشوش می‌شود. درواقع این جرم اساساً عموم مردم را هدف قرار می‌دهد تا ذهنیت آنها را نسبت به مقامات رسمی و حاکمیت تغییر دهد.

ب) تعبیر «**رأساً یا به‌عنوان نقل قول**» حذف شده است. زیرا این جرم قائم به شخص است و صحیح نیست که موارد نقل قول را هم دربرگیرد. مگر اینکه شخص با علم به کذب بودن آن را بازگو کند که در این صورت رأساً مشمول این ماده می‌شود و دیگر عنوان ناقل ندارد.

ج) تعبیر «**تلویحی**» حذف شده است. زیرا احراز آن دشوار و ممکن است تالی فاسد به دنبال داشته باشد و با اصل تفسیر مضیق قوانین جزایی نیز تعارض دارد.

د) تعبیر «**درصورت امکان**» نیز زائد تشخیص و حذف شده است. به‌ویژه آنکه معلوم نیست به اعاده حیثیت برمی‌گردد یا به مجازات مقرر برای آن.

هـ) مجازات نیز طبق روال معمول مشخصاً تعیین شده است.

و) در پایان، از آنجا که ممکن است تشکیک شود این ماده انعکاس صرف ماده (٦٩٨) قانون مجازات اسلامی است، گفتنی است در آن ماده ابزارهای ارتکاب این جرم به‌طور حصری بیان شده‌اند و سیستم‌های رایانه‌ای و مخابراتی را دربرنمی‌گیرند. لذا برای رفع این خلأ، این ماده پیشنهاد شده است. همچنین با توجه به رشد گرایش شهروندان ایرانی به استفاده از رسانه‌های خبررسان الکترونیکی گوناگون، به‌ویژه پایگاه‌های اطلاع‌رسانی اینترنتی، این جرم به سهولت قابل ارتکاب است و باید به‌طور خاص از سوی قانون‌گذار مورد توجه قرار گیرد.

پیشنهاد مرکز ـ اصلاح ماده (۱۱) لایحه

ماده (۱۸)

هرکس به قصد اضرار به غیر یا تشویش اذهان عمومی به‌وسیلهٔ سیستم‌های رایانه‌ای یا مخابراتی اکاذیبی را منتشر کند یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت به شخص حقیقی یا حقوقی به‌طور صریح نسبت دهد، اعم از اینکه به‌نحوی از انحا ضرر مادی یا معنوی وارد شود یا نشود، افزون بر اعادهٔ حیثیت، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

فصل ششم ـ مسئولیت کیفری ارائه‌دهندگان خدمات

گزافه نیست گفته شود که شاهرگ فضای سایبر در دستان ارائه‌دهندگان خدمات است. آنها با تأمین

دسترسی کاربران به شبکه‌های رایانه‌ای و مخابراتی و واگذاری فضای شبکه‌ای به اشخاصی که قصد دارند محتوای الکترونیکی‌شان را ذخیره یا ارائه کنند، نقشی حیاتی ایفا می‌کنند.

بنابراین، موضوع و دو ماده (۱٤) و (۱٥) ذیل این فصل پذیرفتنی هستند، اما شایسته است از یک‌سو گروه مهم دیگری که می‌توانند نقش مؤثری در تحقق اهداف مجرمانه سایبری به‌ویژه در سطح کلان و گسترده آن ایفا کنند، یعنی «**اشخاص حقوقی**» تحت شمول مقررات کیفری این قانون قرار گیرند و از سوی دیگر، نواقص و نارسایی‌های این دو ماده نیز رفع شود.

به این ترتیب، پیشنهاد می‌شود عنوان این فصل به ترتیب ذیل اصلاح شود. به‌ویژه آنکه اصولاً ارائه‌دهندگان خدمات تنها می‌توانند در قالب «**شخصیت حقوقی**» فعالیت کنند و چنانچه مرتکب سایر جرائم این قانون شوند نیز رأساً موضوع حکم قرار خواهند گرفت.

پیشنهاد مرکز ـ اصلاح عنوان فصل ششم به:
فصل ششم ـ مسئولیت کیفری اشخاص

ماده (۱۹) الحاقی مرکز

با توجه به توضیحات فوق، در این ماده، شرایط تحقق مسئولیت کیفری شخص حقوقی تبیین شده است:

الف) پیش از هر چیز این ماده «**کلیه**» جرائم رایانه‌ای را دربرمی‌گیرد. لذا چنانچه شخص حقوقی مرتکب جرم رایانه‌ای مندرج در قانون دیگری نیز شود، مشمول مقررات این ماده خواهد شد.

ب) جرم رایانه‌ای باید به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد. بنابراین اگر فرد مذکور در بندهای «**الف**» تا «**د**» ماده پیشنهادی مرتکب جرم رایانه‌ای شود، ولی به نام شرکت و در راستای منافع آن نباشد، مشمول این ماده نمی‌شود. منظور از منافع در این ماده نیز اعم از «منافع مادی و معنوی» است و عمل برمبنای نام شرکت نیز نیازی به تصریح ندارد، بلکه صرفاً کافی است احراز شود شخص عمل مجرمانه را برای خود انجام نداده و به‌عبارت دیگر، اراده‌اش در وجود شخص حقوقی مستغرق گشته و به نام آن و در راستای منافع آن مرتکب جرم شده است.

ج) اشخاص مندرج در بندهای چهارگانه این ماده احصا شده‌اند تا این ماده جلوه خاص و استثنایی خود را حفظ کند و تنها اشخاصی که در راستای منافع شخص حقوقی و به نام آن مرتکب جرم می‌شوند را دربرگیرد.

د) در بند «الف» مدیر شخص حقوقی هدف قرار گرفته است. از آنجا که احتمال می‌رود در معنای «**مدیر**» تشکیک شود، در تبصره «۱» تعریف شده است. مطابق این تبصره، مقام ذی‌صلاح قضایی

موظف است در مجموعه شخص حقوقی به دنبال کسی باشد که اختیار نمایندگی، تصمیم‌گیری یا نظارت بر شخص حقوقی را داراست. به‌عبارت دیگر، صرف شهره بودن یک شخص در یک مجموعه به نام مدیر کفایت نمی‌کند، بلکه باید سمت او براساس این تبصره احراز گردد و چه‌بسا اشخاصی که ظاهراً مدیر هستند، ولی هیچ‌گونه اختیار و سمتی را به عهده ندارند و از طرف دیگر، چه بسا اشخاصی که ظاهراً هیچ مسئولیتی به عهده ندارند، ولی عنان امور را در اختیار دارند. بنابراین، احراز سمت مدیریت از جانب دادگاه الزامی است. تکیه بیش از حد بر این موضوع به این دلیل است که سایر اشخاصی که مطابق این ماده مرتکب جرم می‌شوند و در بندهای بعدی از آنها نام برده شده، به‌نحوی با این شخصیت در ارتباطند. لذا تا او شناسایی نشود، امکان شناسایی سایرین وجود نخواهد داشت.

هـ) در بند «**ب**» به موردی اشاره شده که مدیر شخص حقوقی دستور ارتکاب جرم را صادر کند و جرم به وقوع پیوندد. لذا کسی که موظف است از دستور مدیر شخص حقوقی تبعیت کند، در راستای منافع آن و به نام آن مرتکب جرم رایانه‌ای می‌شود.

و) بند «**ج**» وضعیتی را دربرمی‌گیرد که یکی از کارمندان شخص حقوقی، در هر سمت و رده‌ای که قرار دارد، با آگاهی مدیر یا در اثر عدم نظارت وی، مرتکب جرم رایانه‌ای می‌شود. مدیر موظف است درصورت آگاهی از امکان وقوع جرم در راستای منافع و به نام شخص حقوقی، ممانعت لازم را به عمل آورد. همچنین، آگاهی وی از کردار کارکنان «**مفروض**» انگاشته می‌شود. بنابراین اگر اثبات شود که به‌طور متعارف نظارت خود را به عمل نیاورده و از این طریق موجبات وقوع جرم رایانه‌ای را فراهم آورده است، باز هم می‌توان بر مسئولیت کیفری شخص حقوقی تأکید کرد.

ز) بند «د» مواردی را دربرمی‌گیرد که تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم اختصاص یافته باشد. در اینجا میزان نقش‌آفرینی، آگاهی و دخالت مدیر شخص حقوقی هیچ تأثیری ندارد. بلکه حتی بدون آگاهی وی نیز می‌توان مسئولیت کیفری را اعمال کرد (البته بعید به نظر می‌رسد که در این‌گونه موارد مدیر مربوطه بی‌اطلاع بوده یا هیچ نقشی نداشته باشد).

ح) در مورد تبصره «۱» توضیحات لازم داده شد. اما چنانچه شخص حقوقی چند مدیر داشته و اراده جمعی آنها صورتگر اراده شخص حقوقی باشد، درصورت تحقق عنوان مدیریت بر هریک از آنها، حتی اگر بدون آگاهی دیگران مرتکب اعمال مندرج در این ماده شود، می‌توان مجموعه شخص حقوقی را نیز تحت تعقیب قرار داد.

ط) تبصره «۲» نیز تصریح دارد مرتکب جرم مبرای از مسئولیت کیفری نیست. زیرا او قانون‌شکن واقعی بوده و نباید از مجازات معاف شود.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۱۹)

در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به‌وقوع پیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد.

تبصره «۱» ـ منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد.

تبصره «۲» ـ مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود.

ماده (۲۰) الحاقی مرکز

پس از تعیین مسئولیت کیفری اشخاص حقوقی، نوبت به وضع مجازات برای آنها می‌رسد. ناگفته پیداست از آنجا که آنها «**شخصیت اعتباری**» دارند و با اشخاص حقیقی متفاوتند، باید ضمانت اجرای کیفری متناسب با آنها وضع شود.

الف) به‌طور کلی در تدوین این ماده سه نکته مهم رعایت شده است:

۱. جنبه‌های جرم‌شناسانه موضوع در کنار اعمال مسئولیت کیفری،

۲. سازگاری نوع و میزان مجازات با ماهیت اعتباری اشخاص حقوقی،

۳. پیش‌بینی نحوه جبران خسارات ناشی از جرم ارتکابی.

ب) طبق صدر این ماده، به هنگام تعیین مجازات باید سه نکته مهم را مدنظر داشت:

۱. **شرایط و اوضاع و احوال جرم ارتکابی**: علت و انگیزه ارتکاب جرم چه بوده و چه اهدافی از آن دنبال می‌شده است؟ طیف وسیعی از جرائم رایانه‌ای با اهداف و انگیزه‌های خاص ارتکاب می‌یابند. بنابراین، توجه به نوع و نحوه ارتکاب جرم و اینکه مدیر مربوطه چه نقشی ایفا کرده و تا چه اندازه اراده شخص حقوقی در وقوع این جرم تجلی یافته، می‌تواند نقش مهمی در تعیین نوع و میزان مجازات داشته باشد.

۲. **میزان درآمد شخص حقوقی**: این موضوع اخیراً توجه نظام‌های حقوقی را به خود جلب کرده و جلوه دیگری از فردی کردن مجازات‌هاست.

۳. **نتایج حاصله از ارتکاب جرم**: طیف وسیع جرائم رایانه‌ای نتایج گوناگونی دارند و یکی از راه‌های مجازات عادلانه و اثربخش به‌شمار می‌آید. نتیجه مجرمانه‌ای که به امنیت، اقتصاد و فرهنگ

یک جامعه لطمه وارد می‌آورد، با لطمه مالی صرف به یک فرد یا گروه خاص متفاوت است.

ج) با توجه به توضیحات فوق، سه نوع مجازات پیش‌بینی شده است:

۱. **جزای نقدی**: در اینجا «**حداکثر**» میزان جزای نقدی مدنظر قرار گرفته است. اگر به‌طور عام بیان می‌شد، «**حداقل**» میزان آن را هم دربرمی‌گرفت که حتی با سه یا شش برابر کردن هم مبلغی ناچیز می‌شد. فرض بر این است که اشخاص حقوقی وضعیت اقتصادی مطلوب‌تری دارند و رعایت جنبه «**بازدارندگی**» مجازات ایجاب می‌کند این نکته لحاظ شود.

۲. **تعطیلی موقت**: این اصطلاح برای قانون‌گذار کیفری ما ناآشنا نیست. اما برای تفکیک این نوع مجازات از مجازات بند بعد که سنگین‌تر به‌شمار می‌آید، سقف معینی تعیین شده است.

۳. **انحلال**: معدودی از جرائم شدید مشمول این حکم می‌شوند، مانند جاسوسی رایانه‌ای.

د) در تبصره «۱» به یک مجازات تکمیلی اشاره شده تا مدیران در زمان تصدی خود به وظیفه نظارتی‌شان عمل و علاوه بر صیانت نفس، از بروز تخلفات در مجموعه‌شان پیشگیری کنند. بنابراین، چنانچه طبق بند «ب» شخص حقوقی منحل شود، مدیر آن به مدت ۳ سال حق تأسیس، نمایندگی، تصمیم‌گیری یا نظارت بر شخص حقوقی دیگری را نخواهد داشت.

هـ) تبصره «۲» به نحوه جبران خسارت اشاره دارد. از آنجا که جرم رایانه‌ای به نام و در راستای منافع شخص حقوقی ارتکاب یافته است، اولین جبران‌کننده خسارات نیز باید خود آن باشد و از محل اموال آن جبران شود. اما اگر این اموال تکافوی خسارات وارده را نکند، از اموال مرتکب جرم جبران خواهد شد.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۲۰)

اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و درصورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و درصورت تکرار جرم شخص حقوقی منحل خواهد شد.

تبصره «۱» ـ مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می‌شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی دیگری را نخواهد داشت.

تبصره «۲» ـ خسارات شاکی خصوصی از اموال شخص حقوقی جبران خواهد شد. درصورتی که اموال شخص حقوقی به تنهایی تکافو نکند، مابه‌التفاوت از اموال مرتکب جبران خواهد شد.

ماده (۱۴) لایحه

ایجادکنندگان نقطه تماس بین‌المللی موظفند با به‌کارگیری تدبیرها و تجهیزات فنی متعارف محتویات مستهجن موضوع ماده (۹) و بند «الف» ماده (۱۰) این قانون را پالایش نمایند. در غیر این صورت فرد متخلف برای بار نخست به پرداخت جزای نقدی از مبلغ ده میلیون (۱۰۰۰۰۰۰۰) ریال تا یکصد میلیون (۱۰۰۰۰۰۰۰۰) ریال و درصورت تکرار به تعطیل موقت از یک هفته تا یک ماه و برای بار سوم به لغو دائم مجوز و محرومیت دائم از تصدی این حرفه محکوم خواهد شد. سایر ارائه‌کنندگان خدمات دسترسی نیز که با علم به تخلف ایجادکنندگان نقطه تماس بین‌المللی، محتویات مستهجن ذکر شده را به کاربران ارائه دهند به مجازات مقرر در این ماده محکوم خواهند شد.

نکات لحاظ شده در ماده پیشنهادی مرکز به‌شرح ذیل است:

الف) تعبیر «**ایجادکنندگان نقطه تماس بین‌المللی**» به «**ارائه‌دهندگان خدمات دسترسی**» تغییر یافته است. طبق مصوبه ٤٨٨ شورای عالی انقلاب فرهنگی در سال ۱۳۸۰ راجع به استفاده از شبکه‌های اطلاع‌رسانی رایانه‌ای، خدمات دسترسی به سه گروه ایجادکنندگان نقطه تماس بین‌المللی (آیین‌نامه (الف))، واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت (رساها) (آیین‌نامه (ب)) و دفاتر خدمات اینترنتی حضوری (کافی‌نت‌ها) (آیین‌نامه (ج)) تقسیم شده‌اند.[۱] درواقع، ایجادکنندگان نقطه تماس بین‌المللی، نوک هرم دسترسی و تنها پل ارتباطی قانونی میان شبکه داخل و خارج کشور به‌شمار می‌آیند. لذا طبیعی است آنها نسبت به لایه‌های زیرین خود امکانات و تجهیزات بیشتر و پیشرفته‌تری در اختیار داشته باشند. ولی اقدام مورد انتظار این ماده، یعنی «**پالایش**»[۲] محتوای مجرمانه، مستلزم تجهیزات سخت‌افزاری و نرم‌افزاری است که باید تمامی ارائه‌دهندگان خدمات داشته باشند، در غیر این صورت حق ندارند فعالیت کنند. هرچند نباید شائبه پالایش چندمرحله‌ای به ذهن متبادر شود و در این رابطه هماهنگی‌های لازم صورت گرفته است.

ب) نکته مهم‌تر این است که تعبیر «ارائه‌دهنده خدمات دسترسی» عام است و با مرور زمان مفهوم خود را از دست نمی‌دهد. حال آنکه اکنون تعابیری چون «ایجادکنندگان نقطه تماس کم‌ظرفیت و پرظرفیت» که چند سال گذشته رواج داشته، اکنون کارایی ندارند و تعابیر جدیدی چون تأمین، توزیع و عرضه اینترنت و اینترانت ملی به‌کار می‌رود.

ج) تعبیر «**تدبیرها و تجهیزات فنی متعارف**» با «**ضوابط فنی و فهرست مقرر از سوی ...**» جایگزین شده است. منظور از «**متعارف**» بودن تدبیرها و تجهیزات روشن نیست و این نوع

---

۱. مرکز پژوهش‌های مجلس شورای اسلامی، تأملی بر فیلترینگ: ۳. سالم‌سازی فضای سایبر و تعارضات موجود، شماره ۸۵۷٤، مهرماه ۱۳۸٦، ص ۱۸.

2. Filtering

ضابطه‌انگاری همواره مخاطبان این ماده را در معرض مسئولیت قرار می‌دهد. ممکن است بهترین تدابیر و تجهیزات روزآمد «**نامتعارف**» تلقی شود. در دنیای فناوری اطلاعات و ارتباطات که هر روز شگفتی‌های جدیدی پدید می‌آید و در دسترس همگان قرار می‌گیرد، احراز چنین ضابطه‌ای دشوار خواهد بود. لذا باید یک مرجع ذی‌صلاح قانونی تکلیف این مسئولیت را روشن کند و به همین دلیل به نظر رسید صراحتاً راجع به این موضوع در اینجا تعیین تکلیف شود.

د) پیش‌بینی کمیته تعیین مصادیق: شایان ذکر است در مصوبه مذکور شورای عالی انقلاب فرهنگی، کمیته‌ای برای تعیین محتوای غیرمجاز پیش‌بینی شده بود که صبغه قضایی نداشت.[۱] حال آنکه پالایش محتوا صبغه کیفری و تأمینی دارد و بنابراین باید زیر نظر مقام ذی‌صلاح قضایی نسبت به مصادیق موردنظر تعیین تکلیف شود. به همین منظور در تبصره ماده پیشنهادی آمده کمیته در «محل دادستانی کل کشور» و به ریاست ایشان تشکیل شود. هرچند به‌منظور جلب آرای کارشناسی کلیه مسئولان و دست‌اندرکاران امر، نمایندگان آنها به‌عنوان اعضای اصلی در کمیته حضور خواهند یافت.

هـ) پالایش محتوای مجرمانه به‌موجب «**شکایت خصوصی**»: همان‌طور که اکنون نیز این رویه اعمال می‌شود، برخی جرائم رایانه‌ای جنبه خصوصی داشته و ممکن است یکی از اقدامات قضایی ناظر به آن، پالایش محتوایی باشد که از طریق پایگاه‌های اطلاع‌رسانی رایانه‌ای در دسترس عموم قرار گرفته است، مانند هتک حیثیت و نشر اکاذیب. در چنین حالتی از آنجا که ارجاع پرونده کیفری به کمیته تعیین مصادیق خلاف قانون اساسی است،[۲] در تبصره «۲» ماده پیشنهادی آمده قاضی رسیدگی‌کننده به پرونده به پالایش یا عدم پالایش محتوا را صادر خواهد کرد.

و) تأکید بر «**محتوای مجرمانه**» به‌جای «**محتوای مستهجن**»: تردیدی نیست که محتوای مستهجن، مجرمانه است و حتی بخش اعظم امر پالایش را به خود اختصاص داده است؛ اما نباید از سایر محتویات مجرمانه غافل شد. در این لایحه به برخی از آنها اشاره شده، ولی به آنها محدود نیست و طبق نظر کمیته تعیین مصادیق، هر محتوایی که مجرمانه تلقی شود، مشمول پالایش خواهد شد.

ز) مجازات «**شخصیت حقوقی**» ارائه‌دهندگان خدمات در کنار مجازات «**فرد متخلف**»: طبق تبصره «۲» ماده (۱۹) پیشنهادی مرکز، مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود. لذا می‌توان گفت در رابطه با ارائه‌دهندگان خدمات نیز رویکرد جامعی نسبت به لایحه اتخاذ شده است.

---

۱. مرکز پژوهش‌های مجلس شورای اسلامی، تأملی بر فیلترینگ: ٤. مشترک گرامی دسترسی به این سایت امکان‌پذیر نمی‌باشد، شماره ۸۵۸۱، مهرماه ۱۳۸٦، ص ۲.

۲. طبق اصل ١٦٧ قانون اساسی قاضی شخصاً موظف است به موضوع رسیدگی و حکم آن را استخراج کند.

ح) تفکیک «**ترک فعل عمدی**» از «**بی‌احتیاطی و بی‌مبالاتی**»: رعایت این مسئله منطقی و حتی الزامی است. اگر ارائه‌دهندگان خدمات عمداً از اعمال ضوابط پالایش خودداری کنند، از آنجا که (یک یا چند) شاهراه کشور را در اختیار دارند، می‌توانند باعث آلودگی سیستم‌های رایانه‌ای بسیاری از کاربران به محتوای مجرمانه شوند. لذا با توجه به اینکه گناهی نابخشودنی مرتکب شده‌اند در همان مرتبه نخست «**منحل**» خواهند شد. هرچند این مسئله بعید است. اما اگر مرتکب بی‌احتیاطی و بی‌مبالاتی شوند، در مراتب اول و دوم به جزای نقدی و درصورت تکرار چاره‌ای جز تعطیلی موقت آنها نخواهد بود.

پیشنهاد مرکز ـ اصلاح ماده (۱۴) لایحه

ماده (۲۱)

ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کمیتهٔ تعیین مصادیق موضوع این ماده محتوای مجرمانه از قبیل محتویات مستهجن را پالایش کنند. درصورتی که عمداً از پالایش محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینهٔ دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبهٔ نخست به جزای نقدی از بیست تا یکصد میلیون ریال و در مرتبهٔ دوم به جزای نقدی از یکصد میلیون تا یک میلیارد ریال و در مرتبهٔ سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره «۱» ـ قوهٔ قضائیه موظف است ظرف یک ماه از تاریخ تصویب این قانون کمیتهٔ تعیین مصادیق محتوای مجرمانه را در محل دادستانی کل کشور تشکیل دهد. نمایندگان وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، بهداشت، درمان و آموزش پزشکی، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، سازمان تبلیغات اسلامی، سازمان صدا و سیما و نیروی انتظامی به‌همراه یک نفر نمایندهٔ مجلس شورای اسلامی به انتخاب مجلس و نمایندهٔ نظام صنفی رایانه‌ای کشور اعضای کمیته را تشکیل خواهند داد. ریاست کمیته به عهدهٔ دادستان کل کشور خواهد بود.

تبصره «۲» ـ پالایش محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام قضایی رسیدگی‌کننده به پرونده انجام خواهد شد.

ماده (۱۵) لایحه

ارائه‌کنندگان خدمات میزبانی موظفند پس از اطلاع از وجود محتویات مستهجن موضوع ماده (۹) و بند «الف» ماده (۱۰) این قانون در فضای واگذار شده توسط آنها، به‌سرعت محتویات ذکر شده را غیرقابل دسترس نموده و مراتب را به مراجع قضایی یا انتظامی محل اعلام نموده و براساس دستور مقام قضایی اقدام نمایند. در غیر این صورت فرد متخلف برای بار نخست به پرداخت جزای نقدی از مبلغ ده میلیون (۱۰۰۰۰۰۰۰) ریال تا پنجاه میلیون (۵۰۰۰۰۰۰۰) ریال و درصورت تکرار به پرداخت جزای نقدی از مبلغ پنجاه میلیون (۵۰۰۰۰۰۰۰) ریال تا یکصد میلیون (۱۰۰۰۰۰۰۰۰) ریال و

محرومیت دائم از حرفه ذکر شده محکوم خواهد شد.

این ماده ناظر به دسته مهم دیگری از ارائه‌دهندگان خدمات، موسوم به ارائـه‌دهنـدگان خـدمات میزبانی[1] است که فضای موردنیاز ارائه‌دهندگان محتوا را در فضای سایبر تأمین می‌کنند. اصلاحات اعمال شده در این ماده عبارتند از:

الف) تصریح به «**تابعیت**» ارائه‌دهندگان خدمات: به‌طور کلی، ارائه خدمات میزبانی یا از طریـق مراکز داده[2] احداث شده در داخل کشور امکان‌پذیر است یا باید از مراکز داده خارج از کشور تـأمین شود. تصریح به تابعیت این حسن را دارد که هر دو گروه فوق را دربرمی‌گیرد و دیگـر ایـن احتمـال از بین خواهد رفت که با سختگیری به مراکز داده داخلی، ارائه‌دهندگان خـدمات میزبـانی بـه مراکـز داده خارجی گرایش یابند. زیرا هر دو به یک اندازه در مقابل این قانون مسئولند.

ب) این ماده همانند ماده (۲۱) پیشنهادی فوق تنظیم و در آن مقرر شده ارائـه‌دهنـدگان خـدمات میزبانی به محض دریافت دستور از کمیته، اقدامات لازم را انجام دهند. در غیـر ایـن صـورت، طبـق این ماده مجازات خواهند شد.

پیشنهاد مرکز ـ اصلاح ماده (۱۵) لایحه

ماده (۲۲)

اتباع ایرانی ارائه‌دهنده خدمات میزبانی موظفند به محض دریافت دسـتور کمیتـه تعیـین مصـادیق مـذکور در ماده فوق یا مقام قضایی رسیدگی‌کننده به پرونده مبنی‌بر وجود محتوای مجرمانه در سیسـتم‌هـای رایانـه‌ای خود از ادامهٔ دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای دسـتور کمیتـه یـا مقـام قضـایی خودداری کنند، منحل خواهند شد. در غیـر ایـن صـورت، چنانچـه در اثـر بـی‌احتیـاطی و بـی‌مبـالاتی زمینـه دسترسی به محتوای مجرمانه مزبور را فراهم کنند، در مرتبه نخسـت بـه جـزای نقـدی از بیسـت تـا یکصـد میلیون ریال و در مرتبه دوم به یکصد میلیون تا یک میلیارد ریال و در مرتبه سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

ماده (۲۳) الحاقی مرکز

در ادوار مختلف، متناسب با پیشرفت و توسعه‌یافتگی جوامع، سرمایه‌های جدیدی پدید مـی‌آینـد کـه هرچند ممکن است مشهود نباشند و جلب توجه نکنند، اما بسیار ارزشـمندند و از آنجـا کـه بـه همـه آحاد جامعه تعلق دارند، حاکمیت ملی موظف است از آنها صیانت و با هرگونه سوءاسـتفاده از آنهـا مبارزه کند. حال چنانچه این سوءاستفاده جنبه «**امنیتی**» نیز بیابد، باید در مقابله با آن تعجیل کرد.

یکی از مزایای شگفت‌انگیز فناوری اطلاعات و ارتباطات، تسهیل برقـراری ارتباطـات مخـابراتی

1. Host
2. Data Center

در بستر فناوری نوینی به نام پروتکل اینترنتی (IP) است. ارتباط مخابراتی که به این شکل از خارج به داخل متصل می‌شود، در اصطلاح Termination و برعکس آن را Origination می‌گویند. در این روش، با توجه به توانمندی‌های اینترنت در انتقال صوت، هزینه‌ها به‌طور قابل ملاحظه‌ای کاهش می‌یابد. لکن این موضوع درآمدهای نامشروع و نیز مسائل ضد امنیت ملی را نیز به دنبال دارد. بخش اصلی سوءاستفاده مالی از این پدیده نوین که از آن به «قاچاق مخابراتی» نیز یاد می‌شود، به Termination تعلق دارد که سالیانه صدها میلیارد ریال سود نصیب متخلفان می‌کند. هرچند باید به خط مقابل آن، یعنی Origination نیز توجه داشت. لذا علاوه بر ضرورت ساماندهی این حوزه از سوی مراجع ذی‌صلاح قانونی، یعنی کمیسیون و سازمان تنظیم مقررات ارتباطات رادیویی، باید سزادهی کیفری متخلفان را نیز در دستور کار قرار داد. به‌ویژه آنکه امکان ارتکاب انواع جرائم و تخلفات بدون امکان اعمال نظارت لازم وجود دارد و حتی تهدیدهای امنیت ملی نیز جدی تلقی می‌شود.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۲۳)

هرکس بدون مجوز قانونی از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی مبتنی‌بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند، به حبس از یک تا سه سال یا جزای نقدی از یکصد میلیون تا یک میلیارد ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم ـ سایر جرائم

ماده (۱۶) لایحه

اشخاص زیر به جزای نقدی از پنج میلیون (۵۰۰۰۰۰۰) ریال تا بیست میلیون (۲۰۰۰۰۰۰۰) ریال محکوم خواهند شد:

***الف)** هرکس با علم و عمد اقدام به تولید یا انتشار یا توزیع یا معامله داده‌ها یا نرم‌افزارها و یا هر نوع وسایل الکترونیکی که صرفاً برای ارتکاب جرائم رایانه‌ای به‌کار می‌روند، نماید.*

***ب)** هرکس با علم و عمد رمز عبور یا کد دستیابی یا داده‌های رایانه‌ای را بدون مجوز مرجع قانونی به دیگران ارائه کرده یا مورد معامله قرار دهد یا منتشر نماید به‌گونه‌ای که امکان دسترسی بدون مجوز مرجع قانونی به داده یا سیستم‌های رایانه‌ای و یا مخابراتی دیگری را فراهم آورد.*

***تبصره** ـ درصورتی که مرتکب، اعمال یاد شده را حرفه خود قرار داده باشد، به حداکثر مجازات مذکور محکوم خواهد شد.*

علاوه‌بر پاره‌ای اصلاحات ویرایشی، به ماده پیشنهادی یک بند نیز الحاق شده که در ذیل می‌آید:

الف) از آنجا که مرتکب و تصریح به علم و عمد وی وجه مشترک تمامی بندهای این ماده است، باید به ابتدای ماده انتقال یابد.

ب) علاوه بر جزای نقدی، مجازات حبس نیز پیش‌بینی شده است.

ج) در بند «الف»، به‌جای «**وسایل**»، «**ابزارها**» به‌کار رفته است. اما اصلاح مهم‌تر این بند، تسری آن به «**تمامی جرائم**» و نه فقط جرائم رایانه‌ای است. زیرا این احتمال نفی نمی‌شود که از داده‌ها یا نرم‌افزارها یا ابزارهای الکترونیکی، صرفاً برای ارتکاب سایر جرائم استفاده شود.

د) توضیحات لازم راجع به اصلاحات به عمل آمده در بند «ب» در قسمت‌های پیشین آمده است. مانند جایگزینی «**بدون مجوز مرجع قانونی**» با «**غیرمجاز**».

هـ) یکی از ویژگی‌های متمایز جرائم رایانه‌ای نسبت به سایر جرائم، نیاز به درجات مختلف تبحر و تجربه است، به‌ویژه جرائم خطرناک رایانه‌ای که تنها توسط افرادی قابل ارتکاب است که تجربه و تخصص بالایی داشته باشند. لذا باید با اشخاصی که به آموزش نحوه ارتکاب این طیف از جرائم می‌پردازند برخورد کرد. کما اینکه متأسفانه ملاحظه می‌شود به‌دلیل نبود قانون کیفری مناسب، برخی آشکارا به این امر مبادرت می‌ورزند و برای مثال دوره‌های پیشرفته نفوذ غیرمجاز[1] را نیز آموزش می‌دهند که «مادر جرائم رایانه‌ای» لقب گرفته است.

و) نکته اصلاح شده در تبصره، تصریح به ضرورت اعمال حداکثر هر دو مجازات مقرر است که به نظر می‌رسد دیدگاه نویسندگان لایحه نیز همین است.

پیشنهاد مرکز ـ اصلاح ماده (۱۶) لایحه

ماده (۲۴)

هرکس مرتکب اعمال زیر شود، به حبس از نودویک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد:

الف) تولید یا انتشار یا توزیع یا معاملهٔ داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به‌منظور ارتکاب جرائم به‌کار می‌رود.

ب) فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند.

ج) آموزش نحوهٔ ارتکاب جرائم رایانه‌ای.

تبصره ـ چنانچه مرتکب اعمال یاد شده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

1. Hacking

فصل هشتم ـ تخفیف و تشدید مجازات و سایر مسائل

قسمت انتهایی این عنوان نه تنها عامیانه است و در لسان قانون‌گذار سابقه‌ای از آن دیده نمی‌شود، بلکه تنها ماده از لایحه که مشمول این قسم انتهایی می‌شود، ماده (۱۹) است. این ماده نیز صرف‌نظر از ابقا یا رد آن می‌تواند در انتهای لایحه در ذیل «**بخش پنجم ـ سایر مقررات**» بیاید که البته پیشنهاد مرکز حذف آن است که در جای خود توضیح داده خواهد شد.

پیشنهاد مرکز ـ اصلاح عنوان فصل هشتم به: **فصل هشتم ـ تخفیف و تشدید مجازات‌ها**

ماده (۱۷) لایحه

اشخاصی که مرتکب جرائم ذکر شده در مواد (۲)، (۳)، (٤) و (٥) این قانون شده‌اند هرگاه پیش از کشف جرم، مأموران تعقیب را از ارتکاب جرم مطلع نمایند یا به هنگام تعقیب موجبات تسهیل تعقیب سایر مرتکبان را فراهم آورند یا مأموران دولت را به‌گونه مؤثری در کشف جرم کمک و راهنمایی کنند و یا ضرر و زیان ناشی از جرم را در مرحله تحقیق جبران نمایند بنا به پیشنهاد دادستان مربوط و موافقت دادگاه و یا با تشخیص دادگاه در مجازات آنان تخفیف متناسب داده می‌شود و دادگاه می‌تواند مجازات مرتکب را معلق یا او را از مجازات معاف کند.

اصلاحات به عمل آمده در این ماده عبارتند از:

الف) به‌جای ٤ ماده‌ای که در لایحه تصریح شده، به تمامی جرائم موضوع این قانون تسری یافته است. شاید دلیل ارجاع به آن مواد، توجه به جنبه «**امنیتی**» آنها و داشتن سابقه در قانون مجازات اسلامی، باب جرائم علیه امنیت ملی باشد. اما جرائم سایبری وضعیت ویژه‌ای دارند و نباید این فرصت مغتنم را از سایر جرائم دریغ کرد.

ب) نکته مهم دیگر این است که فراهم آوردن موجبات تسهیل تعقیب سایر مرتکبان درصورتی مشمول کیفیات مخففه می‌شود که به‌موجب «**اقرار متهم**» باشد.

ج) با وجود اینکه عنوان این فصل و هدف این ماده تخفیف مجازات است؛ اما در انتهای آن آمده قاضی می‌تواند مجازات را معلق یا حتی مرتکب را از مجازات معاف کند. این مسئله می‌تواند تالی فاسدهایی داشته باشد. هرچند احکام تعلیق در کلیات قانون مجازات اسلامی (ماده (۲۵)) آمده و نیازی به تصریح نیست. لذا باید به تخفیف مجازات بسنده کرد.

پیشنهاد مرکز ـ اصلاح ماده (۱۷) لایحه

ماده (۲۵)

هرگاه مرتکبان جرائم این قانون پیش از کشف جرم، مأموران تعقیب را از ارتکاب جرم مطلع نمایند یا به هنگام تعقیب به‌واسطه اقرار خود موجبات تسهیل تعقیب سایر مرتکبان را فراهم آورند یا مأموران دولت را به‌گونه مؤثری در کشف جرم کمک و راهنمایی کنند یا ضرر و زیان ناشی از جرم را در مرحله تحقیق جبران نمایند بنا به پیشنهاد دادستان مربوط و موافقت دادگاه و یا با تشخیص دادگاه در مجازات آنان تخفیف مناسب داده می‌شود.

ماده (۱۸) لایحه

هریک از کارمندان و کارکنان اداره‌ها و سازمان‌ها یا شوراها و یا شهرداری‌ها و مؤسسه‌ها و شرکت‌های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه‌هایی که زیر نظر ولی فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه‌هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضایی و به‌طور کلی اعضا و کارکنان قوای سه‌گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرائم رایانه‌ای موضوع این قانون شوند، حسب مورد به بیش از دو سوم حداکثر مجازات مقرر محکوم خواهند شد.

***تبصره ـ** هرگاه عمل مرتکب مشمول عنوان معاونت در جرم باشد به نصف حداکثر مجازات قانونی محکوم خواهد شد.*

این ماده تنها به یک مورد از موارد لازم‌الشمول، اما به تفصیل اشاره کرده است. اصلاحات و الحاقات اعمال شده در ماده پیشنهادی عبارتند از:

الف) تفصیل سازمان‌های دولتی یا وابسته به دولت زائد تلقی می‌شود. زیرا سابقه آن در سایر قوانین نیز وجود دارد و نیازی نیست هر بار که قانون جدیدی برای مخاطب قرار دادن آنها به تصویب می‌رسد، به تفصیل به همگی آنها اشاره شود. لذا به‌جای آن، تعبیر مختصر «**کارمند دولت یا مأمور به خدمات عمومی**» آمده است.

ب) همچنین، برای اینکه کلیه جرائم رایانه‌ای، اعم از موضوع این قانون یا سایر قوانین مصوب را دربرگیرد، قید «**موضوع این قانون**» نیز حذف شده است.

ج) گروه مهم دیگری که باید مخاطب این کیفیت مشدده قرار گیرد، «**متصدیان و متصرفان شبکه‌های رایانه‌ای یا مخابراتی**» هستند. از آنجا که فرض می‌شود این گروه تخصص و امکانات بیشتری برای ارتکاب جرم در اختیار دارند و بدتر از آن می‌توانند پیامدهای ناگواری رقم بزنند، اگر به مناسبت شغل خود مرتکب جرم رایانه‌ای شدند، باید مستوجب تشدید مجازات باشند.

د) حالت سوم به آماج یا اهداف جرم رایانه‌ای مربوط می‌شود که اگر متعلق به دولت یـا خـدمات عمـومی باشد، باید مشمول تشدید مجازات قرار گیرد و به نظر نمی‌رسد توجیه آن نیازمند دلیل باشد.

هـ) یکی از مشکلات دنیای امروز، گرایش جرائم به سوی سازمان‌یافتگی است و جرائم رایانه‌ای نیز از این قاعده مستثنا نیست. به‌ویژه آنکه امکان سازمان‌یافتگی فرامرزی آن بدون مشکل فراهم است. لذا بند «د» ماده پیشنهادی، این گروه را هدف قرار داده است.

و) گسـتردگی جـرم بـه آمـاج و بـزه‌دیـدگان آن مربـوط مـی‌شـود. بـه نظـر نمـی‌رسـد در تفسـیر «**گستردگی**» ابهام خاصی وجود داشته باشد. زیرا قانون‌گذار و محـاکم مـا بـا آن بیگانـه نیسـتند و برای مثال، در قانون مجازات اخلالگران در نظام اقتصادی کشور، مصـوب ۱۳۶۹ از تعبیـر «**عمـده**» استفاده شده که مفهوم مشابهی دارد.

ز) به نظر نمی‌رسد تبصره لایحه مسئله خاصی را حل کرده باشد. زیرا اصل موضوع به‌موجب ایـن ماده تشدید شده و چنانچه فعل مرتکب در رابطه با آن جنبه معاونت بیابد، خودبه‌خـود مجـازات آن ارتقا می‌یابد.

پیشنهاد مرکز ـ اصلاح ماده (۱۸) لایحه

ماده (۲۶)

در موارد زیر، حسب مورد مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد:

الف) کارمند دولت یا مأمور به خدمات عمومی که به مناسبت شغل خود مرتکب جرم رایانه‌ای شده باشد.

ب) متصدی یا متصرف قانونی شبکه‌های رایانه‌ای یـا مخـابراتی کـه بـه مناسـبت شـغل خـود مرتکـب جـرم رایانه‌ای شده باشد.

ج) داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه‌دهنده خدمات عمومی باشد.

د) جرم به‌صورت سازمان‌یافته ارتکاب یافته باشد.

هـ) جرم در سطح گسترده‌ای ارتکاب یافته باشد.

ماده (۱۹) لایحه

چنانچه در اثر ارتکاب جرائم رایانه‌ای ضرر و زیانی متوجـه دیگـری گـردد، جبـران خسـارت وارده وفق قوانین و مقررات مربوط صورت خواهد پذیرفت.

کمتر جرمی یافت می‌شود که منجر به ضرر و زیان، اعم از مـادی و معنـوی نشـود. بـه همـین دلیل، در کنار بیشتر پرونده‌های کیفری، دادخواست جبـران خسـارت نیـز تقـدیم مـی‌شـود و بـدون مشکل و خلأ قانونی مورد رسیدگی قرار می‌گیرد. جرائم رایانه‌ای نیز از این قاعده مستثنا نیسـتند و ضرورتی به تصریح ندارد.

پیشنهاد مرکز ـ حذف ماده (۱۹) لایحه

ماده (۲۷) الحاقی مرکز

یکی از تدابیر کیفری که می‌تواند اثربخشی مطلوبی از لحاظ «**بازدارندگی**» داشته باشد، محروم کردن مرتکبان جرائم رایانه‌ای تحت شرایط خاصی از خدمات اجتماعی است. در مرتبه نخست، مرتکب مجازات مقرر را متحمل می‌شود. چنانچه پس از تحمل کیفر دوباره مرتکب جرم شود، مشمول ضوابط تکرار جرم (ماده (۴۶) قانون مجازات اسلامی) می‌شود. چنانچه در مرتبه سوم به قانون‌شکنی خود ادامه دهد، شایستگی بهره‌مندی از خدمات اجتماعی را از دست می‌دهد و محروم کردن وی منطقی و به مصلحت جامعه خواهد بود. زیرا خطرناکی خود را نشان داده و باید با اتخاذ اقدامات تأمینی از قرار گرفتن چندباره وی در بستر ارتکاب جرم خودداری کرد.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۲۷)

درصورت تکرار جرم برای بیش از دو بار، دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنهٔ مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم نودویک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال.

ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال.

ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.

بخش سوم ـ آیین دادرسی

با اینکه این گزارش در مقام توجیه بخش‌ها یا مواد لایحه نیست، اما لازم به یادآوری است دلیل اصلی پیش‌بینی مجموعه مقررات شکلی کیفری برای جرائم رایانه‌ای، ماهیت متمایز داده‌ها و سیستم‌های رایانه‌ای و مخابراتی به‌عنوان موضوعات اصلی دادرسی کیفری است. به‌طور کلی، دو حوزه اصلی دادرسی، یعنی صلاحیت کیفری و اقدامات ضابطان قضایی جهت گردآوری، تفتیش و توقیف داده‌ها و سیستم‌ها، به‌ویژه در پرتو قواعد ادله اثبات دعوا، با شرایط جدیدی مواجه شده‌اند که لزوم وضع قواعد و مقررات کیفری جدید را محرز می‌گردانند.

همچنین، به هنگام تدوین پیش‌نویس لایحه جدید قانون آیین دادرسی کیفری، ۳ حوزه مشمول تدوین مقررات آیین دادرسی کیفری افتراقی (متمایز) شدند که عبارتند از: دادرسی اطفال، جرائم رایانه‌ای و جرائم سازمان‌یافته. در ذیل به مجموعه مقررات آیین دادرسی جرائم رایانه‌ای اشاره

می‌شود. اما پیش از آن تصریح می‌شود از آنجا که بخش نخست لایحه راجع به تعاریف حذف شده، شمارگان این بخش کاهش می‌یابد.

پیشنهاد مرکز ـ اصلاح عنوان بخش سوم به:
بخش دوم ـ آیین دادرسی

فصل یکم ـ صلاحیت

ماده (۲۸) الحاقی مرکز

یکی از ویژگی‌های برجسته و منحصربه‌فرد فضای سایبر، عدم وابستگی «**مکانی**» آن است. به‌عبارت دیگر، این فضا یک دنیای فرامرزی است که هیچ تعلق خاطری به مرزهای جغرافیایی و سیاسی یا موانع فیزیکی ندارد و هیچ‌کس با اتصال به آن نیز احساس نیاز نمی‌کند که موقعیت مکانی خود را در فضای سایبر شناسایی کند. زیرا امور بدون وابستگی مکانی و با بالاترین بازدهی انجام می‌شود.

با این حال، این مزیت بزرگ مشکلاتی را برای حاکمیت ملی کشورها پدید آورده است. در دنیای فیزیکی، کشورها براساس اصل احترام متقابل به قلمرو حاکمیتی یکدیگر، از تعرض به آن پرهیز می‌کنند. یکی از نمادهای بارز عدم مداخله یا عدم تعرض، متوقف کردن اقدام قضایی ـ پلیسی در فراسوی مرزهاست و از اینجا طبق قواعد حقوق کیفری بین‌المللی و با موافقت کشور درخواست‌شونده عمل می‌شود.

اما در فضای سایبر، این تفکیک قلمرو برای اعمال صلاحیت نظام حقوق کیفری ملی به آسانی امکان‌پذیر نیست و بدتر از آن تعارض‌های گسترده صلاحیتی میان کشورها رخ داده و پیش‌بینی می‌شود اگر نظام حقوق کیفری بین‌المللی چاره‌ای اساسی نیندیشد، تدابیر کیفری اتخاذ شده از سوی کشورها، یعنی قوانین کیفری، با بن‌بست مواجه خواهند شد و بلااجرا خواهند ماند.

لایحه جرائم رایانه‌ای، راجع به صلاحیت نظام حقوق کیفری ایران مقرره‌ای پیش‌بینی نکرده و آن را مسکوت گذاشته و تنها به دو ماده تشریفاتی راجع به صلاحیت محاکم داخلی بسنده کرده است. ولی به نظر می‌رسد می‌توان به معیارهای حداقلی اتکا و راه را برای ارتقای این حوزه حیاتی در حقوق کیفری سایبری هموار کرد. به همین منظور، ماده (۲۸) ذیل پیشنهاد شده است.

الف) در صدر ماده، سایر قوانینی که به‌نحوی صلاحیت نظام حقوق کیفری ایران را تعریف و ترسیم می‌کنند، به‌ویژه مواد نخستین قانون مجازات اسلامی، به رسمیت شناخته شده و درواقع بندهای پیشنهادی، مکمل و مؤید قوانین موجود هستند و می‌کوشند علاوه بر رفع نارسایی‌ها و خلأهای احتمالی، نظام حقوق کیفری سایبری کشورمان را تثبیت کنند.

ب) در بند «الف»، بر موقعیت فیزیکی «**داده‌های مجرمانه**»، مانند محتوای مستهجن یا داده‌هایی که برای ارتکاب جرم به‌کار رفته‌اند، مانند گذرواژه‌ای که به‌طور غیرمجاز به‌دست آمده، تأکید شده است. در سایر قوانین، قلمرو حاکمیتی ایران در سه حوزه زمینی، هوایی و دریایی ترسیم شده و ابهامی ندارد. لذا چنانچه این‌گونه داده‌ها در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده‌ای که در خاک ایران مستقرند یا وجود دارند، ذخیره شده باشند، فرض می‌شود که جرم رایانه‌ای ناشی از آنها در داخل قلمرو حاکمیت ایران ارتکاب یافته است، چه مرتکب یا بزه‌دیده آن در داخل خاک ایران حضور داشته باشد و چه نداشته باشد.

ج) پیش از ورود به بند «ب» ماده پیشنهادی، لازم به ذکر است به‌طور کلی دو نوع دامنه مرتبه بالا وجود دارد: دامنه مرتبه بالای عمومی،[1] مانند net.،.com. و دامنه مرتبه بالای کد کشوری[2] مانند ir.، متعلق به ایران، ru. متعلق به روسیه، fr. متعلق به فرانسه. همان‌طور که ملاحظه می‌شود، گروه دوم نمادهای حاکمیت ملی در فضای سایبر به‌شمار می‌آیند. این دیدگاه با این واقعیت نیز تقویت می‌شود که شرکت آمریکایی ICANN این نمادها را تنها به نمایندگان حاکمیت ملی واگذار می‌کند، حال آنکه دامنه‌های مرتبه بالای عمومی توسط شرکای تجاری آن در سراسر جهان واگذار می‌شوند. بنابراین، به نظر می‌رسد این حق هر کشور است که نسبت به جرائم ارتکابی در وب‌سایتی که نام دامنه ملی را دارد ادعای صلاحیت کند، فارغ از اینکه مرتکب یا بزه‌دیده آن تابعیت کدام کشور را داشته باشد یا از خدمات میزبانی یا دسترسی کدام کشور استفاده کند. این نماد در حکم قلمرو حاکمیتی[3] است و جرم ارتکابی در آن در حکم جرم ارتکابی در قلمرو سرزمینی کشور خواهد بود.

د) در بند «ج» ماده پیشنهادی، رویکرد حمایتی در صلاحیت کیفری[4] لحاظ شده که در قوانین کیفری سنتی نیز سابقه دارد. در اینجا تفاوتی نمی‌کند که مرتکب، ایرانی یا غیرایرانی باشد و سیستم‌ها یا داده‌ها در داخل یا خارج از ایران مستقر یا ذخیره شده باشند. بلکه آنچه هدف قرار گرفته مهم است که سه گروه را شامل می‌شود:

۱. داده‌ها و سیستم‌ها و وب‌سایت‌های مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت: حاکمیت ملی، هم به لحاظ قرار داشتن در معرض تهدیدهای خاصی مثل اقدامات ضد حاکمیتی و تروریستی و هم به‌دلیل ضرورت اداره بلانقطاع امور کشور نیازمند حمایت کیفری ویژه است.

۲. هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد: با توجه به روند پرشتاب

1. Generic Top Level Domain Name
2. Country Code Top Level Domain Name
3. Territoriality
4. Protective Jurisdiction

خصوصی‌سازی و آزادسازی امور تصدی‌گری دولتی، به‌ویژه پس از ابلاغیه مقام معظم رهبری راجع به اصل ٤٤ قانون اساسی، به نظر می‌رسد قانون‌گذار کیفری باید آمادگی لازم را برای حمایت از نهادها و مؤسساتی که خدمات عمومی ارائه می‌دهند به‌دست آورد.

۳. وب‌سایت‌های دارای دامنه ملی ایران در سطح گسترده: دلیل آوردن قید «گسترده»، گرفتار نکردن محاکم ایران به موارد غیرضرور است. ممکن است یک نفر از گوشه‌ای از جهان از نام دامنه ملی ایران استفاده کند و بزه‌دیده جرمی هم واقع شود. لزومی ندارد محاکم ایران درگیر رسیدگی به آن شوند، به‌ویژه آنکه صلاحیت تابعیتی بزه‌دیده‌محور[1] در موضع اقلیتی نظام حقوق کیفری بین‌المللی قرار دارد و چندان مورد استناد قرار نمی‌گیرد. اما هنگامی که این دامنه‌ها به‌طور گسترده هدف قرار می‌گیرند، احتمال بیشتر، هدف قرار دادن نظام حاکمیت ملی است و جرم از جنبه فردی خود خارج می‌شود.

هـ) مورد آخر، به صلاحیت جهانی نظام حقوق کیفری ایران در فضای سایبر اشاره دارد. با توجه به الحاق ایران به کنوانسیون‌های حمایتی از کودکان و همچنین اجماع بین‌المللی در مبارزه با جرائم رایانه‌ای متضمن سوءاستفاده از کودکان، به‌ویژه هرزه‌نگاری کودکان، محاکم ایران صلاحیت کیفری مطلق خواهند داشت و تنها کافی است طبق مقررات آیین دادرسی کیفری، مرتکب در خاک ایران یافت شود تا امکان محاکمه و مجازات آن به‌وجود آید.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۲۸)

علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به‌کار رفته‌اند به هر نحو در سیستم‌های رایانه‌ای و مخابراتی یا حامل‌های دادهٔ موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

ب) جرم از طریق وب‌سایت‌های دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یافته باشد.

ج) جرم توسط هر ایرانی یا غیرایرانی در خارج از ایران علیه سیستم‌های رایانه‌ای و مخابراتی و وب‌سایت‌های مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه وب‌سایت‌های دارای دامنهٔ مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد.

د) جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از ۱۸ سال، اعم از آنکه مرتکب یا بزه‌دیده ایرانی یا غیرایرانی باشد.

1. Victim - Based Nationality Jurisdiction

ماده (۲۹) الحاقی مرکز

این ماده که انعکاس تقریباً کاملی از ماده (۵۳) آیین دادرسی کیفری، مصوب ۱۳۷۸ است، با هدف تعیین تکلیف راجع به پرونده‌های جرائم رایانه‌ای و نجات بزه‌دیدگان و شاکیان از بلاتکلیفی آمده است. اصل در تعیین صلاحیت مراجع کیفری، «**محل وقوع جرم یا رفتار فیزیکی**» است؛ اما با توجه به ماهیت جرائم رایانه‌ای و امکان ارتکاب آنها با وجود فرسنگ‌ها فاصله و همچنین زمان‌بر بودن تعیین محل دقیق ارتکاب جرم و به تبع آن مجرم، در مقام تعیین تکلیف، دادسراهای محل کشف یا گزارش این جرائم مکلف شده‌اند تا زمان مشخص شدن محل وقوع جرم، تحقیقات مقدماتی را انجام دهند تا علاوه بر رسیدگی به حال بزه‌دیدگان و شاکیان، از آسیب‌دیدن یا تخریب ادله در سیستم‌های موجود جلوگیری شود. حال اگر محل وقوع جرم مشخص و طبق قوانین موجود مقام ذی‌صلاح قضایی تعیین شد، دادسرا پرونده را به آن عودت خواهد داد. در غیر این صورت، به تحقیقات خود ادامه و سپس قرار مربوط را صادر خواهد کرد. دادگاه ذی‌صلاح مربوط نیز پس از رسیدگی، حکم مقتضی را صادر خواهد کرد.

پیشنهاد مرکز ـ الحاق یک ماده
ماده (۲۹)
چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.

ماده (۲۰) لایحه

در هر حوزه قضایی، درصورت ضرورت به تشخیص رئیس قوه قضائیه به تعداد مورد نیاز شعبی از دادسراها و دادگاه‌های عمومی و انقلاب و تجدیدنظر برای رسیدگی به جرائم رایانه‌ای اختصاص می‌یابد.

***تبصره ـ** قضات دادسراها و دادگاه‌های ذکر شده از میان قضاتی که آشنایی لازم به امور رایانه دارند، انتخاب خواهند شد.*

نکات مورد توجه در رابطه با این لایحه عبارتند از:

الف) این ماده از لایحه دو قید را در زمینه اختصاص شعبی از مراجع قضایی آورده است که عبارتند از:

۱. درصورت ضرورت،

۲. به تشخیص رئیس قوه قضائیه. اما از آنجا که این موضوع صراحتاً در تبصره ذیل بند «ط» ماده (۳۳) قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران،

مصوب ۱۳۸۳/٦/۱۱ صراحتاً به ترتیب مقرر در ماده (۳۰) پیشنهادی آمده، به نظر رسید در راستای عمل به این قانون اصلاح شود.

ب) در این ماده به «**دادگاه‌های نظامی**» اشاره‌ای نشده، این در حالی است که دادگاه‌های نظامی به لحاظ اختیارات و مسئولیت‌هایی که قوانین خاص برای آنها تعیین کرده‌اند، نسبت به این قانون نیز صلاحیت دارند. برای مثال، در ماده (۱۳۱) قانون مجازات جرائم نیروهای مسلح، مصوب ۱۳۸۲/۱۰/۹ به مصادیقی از جرائم رایانه‌ای اشاره شده است.

پیشنهاد مرکز ـ اصلاح ماده (۲۰) لایحه
ماده (۳۰)
قوه قضائیه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه‌های عمومی و انقلاب، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد.

تبصره ـ قضات دادسراها و دادگاه‌های مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب خواهند شد.

ماده (۲۱) لایحه

درصورت بروز اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی خواهد بود.

این ماده با ایرادی مواجه نیست و عیناً تأیید می‌شود.

پیشنهاد مرکز ـ ابقای ماده (۲۱) لایحه در ماده (۳۱) پیشنهادی مرکز

فصل دوم ـ جمع‌آوری ادله الکترونیکی

مبحث یکم ـ نگهداری داده‌ها

ماده (۲۲) لایحه

کلیه ایجادکنندگان نقاط تماس بین‌المللی و ارائه‌دهندگان خدمات دسترسی موظفند داده‌های حاصل از مبادله داده محتوا را حداقل تا سه ماه پس از ایجاد و اطلاعات کاربران را حداقل تا سه ماه پس از خاتمه اشتراک نگهداری نمایند.

***تبصره ـ** مراجع ذکر شده موظفند آدرس‌های IP خود را به وزارت ارتباطات و فناوری اطلاعات اعلام کنند.*

الف) با توجه به توضیحاتی که ذیل ماده (۲۱) پیشنهادی مرکز راجع به ارائه‌دهندگان خدمات دسترسی داده شد، در اینجا نیز پیشنهاد می‌شود از همین تعبیر عام، یعنی «**ارائه‌دهندگان خدمات دسترسی**» استفاده شود. کما اینکه اکنون چنین رویه‌ای برقرار است و در هریک از لایه‌های دسترسی، داده‌های مربوط نگهداری می‌شود.

ب) با توجه به پیشرفت فناوری از یک‌سو و کاهش هزینه تأمین آن نسبت به زمان تدوین لایحه و اینکه در آینده سهل‌تر نیز خواهد شد و همچنین ضرورت دسترسی طولانی‌تر ضابطان قضایی به داده‌های مورد نیاز، مدت زمان سه ماه مندرج در لایحه به شش ماه افزایش یافت.

ج) با توجه به توضیحاتی که در ابتدای گزارش ذیل مبحث تعاریف داده شد، تعاریف مربوط به «داده‌های ترافیک» و «اطلاعات کاربران» در قالب دو تبصره به این ماده انتقال یافته است.

د) در نهایت، تبصره این ماده حذف شده است. زیرا هدف ارائه آدرس‌های IP توسط مراجع مذکور به وزارت ارتباطات و فناوری اطلاعات احراز نشد. مضافاً اینکه چرا فقط این آدرس‌ها و کدام نوع از آنها و چرا فقط به وزارت مذکور؟

پیشنهاد مرکز ـ اصلاح ماده (۲۲) لایحه و الحاق دو تبصره به آن

ماده (۳۲)

ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره «۱» ـ داده ترافیک هرگونه داده‌ای است که سیستم‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود.

تبصره «۲» ـ اطلاعات کاربر هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، آدرس جغرافیایی یا پستی یا IP، شماره تلفن و سایر مشخصات فردی اوست.

ماده (۳۳) الحاقی مرکز

در کنار ارائه‌دهندگان خدمات دسترسی، خدمات میزبانی نیز از داده‌های مشابه و همچنین سایر داده‌هایی برخوردارند که نگهداری آنها برای پیشبرد امور کیفری ضروری است. به همین منظور، در این ماده این گروه مخاطب قرار گرفته‌اند.

الف) تفاوت اصلی این ماده با ماده (۲۲) پیشنهادی در بخش ماهوی، نوع میزبانانی است که مخاطب قرار گرفته‌اند. در اینجا تنها میزبانان «**داخلی**» موظفند اطلاعات مربوط را نگهداری کنند. زیرا اعمال این مسئولیت بر میزبانانی که در خارج از ایران مستقرند، دخالت در امور حاکمیتی کشور متبوع

است و با اصول حقوق کیفری در تعارض است. همچنین دستیابی به آن اطلاعات مستلزم برقراری مناسبات همکاری دوجانبه پلیسی ـ قضایی است.

ب) در این ماده (۳) نوع داده و اطلاعات هدف قرار گرفته است:

۱. اطلاعات کاربران میزبانی: درواقع آنهایی که از خدمات میزبانی، فضای مورد نیاز برای ارائه یا ذخیره اطلاعات دریافت کرده‌اند،

۲. محتوای ذخیره شده توسط کاربران که می‌تواند متن، صوت، تصویر یا نظایر آن باشد.

۳. داده ترافیک حاصل از تغییرات ایجاد شده: هر بار که کاربر به فضای متعلق به خودش مراجعه و پردازش‌هایی را اعم از تغییر، حذف یا اضافه بر روی داده‌هایش انجام می‌دهد، با داده‌های ترافیک به ثبت می‌رسد.

ج) همان‌طور که ملاحظه می‌شود، پیشنهاد شده اطلاعات کاربران، مانند ماده فوق حداقل تا شش ماه پس از خاتمه اشتراک نگهداری شود. اما از آنجا که نگهداری محتوا نیازمند ابررایانه‌هایی با حافظه بسیار بالاست و عملاً حتی از عهده میزبانان بزرگ نیز خارج است، به مدت زمان حداقل پانزده روز اکتفا شده است.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۳۳)

ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمهٔ اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند.

مبحث دوم ـ حفظ فوری داده‌ها

از آنجا که این مبحث فقط به داده‌های رایانه‌ای ذخیره شده اشاره دارد و سایر اقسام مندرج در مباحث قبل و بعد را دربرنمی‌گیرد، پیشنهاد می‌شود صراحتاً در خود عنوان به نوع داده‌ها اشاره شود.

پیشنهاد مرکز ـ تغییر عنوان مبحث دوم به:
مبحث دوم ـ حفظ فوری داده‌های رایانه‌ای ذخیره شده

ماده (۲۳) لایحه

هرگاه حفظ داده‌های ذخیره شده برای تحقیق یا دادرسی لازم باشد مقام قضایی می‌تواند دستور حفاظت از داده‌های ذخیره شده را برای اشخاصی که داده‌های ذکر شده به‌گونه‌ای تحت تصرف یا

کنترل آنها قرار دارد صادر نماید و در موارد فوری ضابطان دادگستری می‌توانند دستور حفاظت را صادر نموده مراتب را حداکثر تا بیست‌وچهار ساعت به اطلاع مقام قضایی برسانند. چنانچه هریک از کارکنان دولت یا سایر اشخاص از اجرای دستور ذکر شده خودداری نمایند کارکنان دولت به مجازات امتناع از اجرای دستور مقام قضایی و سایر اشخاص به جزای نقدی از سه میلیون (۳۰۰۰۰۰۰) ریال تا ده میلیون (۱۰۰۰۰۰۰۰) ریال محکوم خواهند شد.

***تبصره ـ** مدت زمان حفاظت حداکثر سه ماه می‌باشد و با نظر مقام قضایی قابل تمدید است.*

این ماده به تغییرات ماهوی نیازی ندارد. در کنار اعمال یک‌سری اصلاحات ویرایشی، مطالب تکمیلی آمده است:

الف) در بحث شرایط فوری، مثال‌هایی آورده شده تا علاوه بر روشن شدن مطلب، از تمسک به موارد غیرضرور پرهیز شود و ضابطان قضایی نتوانند هر مسئله‌ای را مستمسک قرار دهند.

ب) مجازات وضع شده برای کسانی که از اجرای دستور حفاظت خودداری می‌کنند، به دو حالت دیگر نیز تسری یافته است:

۱. اشخاص مزبور داده‌های حفاظت شده را افشا کنند.

۲. اشخاصی که داده‌های مزبور به آنها مربوط می‌شود را از مفاد دستور صادره آگاه کنند.

این موضوع از چنان اهمیتی برخوردار است که کنوانسیون جرائم سایبر در بند «۳» ماده (۱۶) راجع به حفظ فوری داده‌های رایانه‌ای ذخیره شده، صراحتاً به محرمانه ماندن این داده‌ها تأکید کرده است.

ج) علاوه بر کارکنان دولت و اشخاص، «**ضابطان قضایی**» نیز رأساً مخاطب قرار گرفته‌اند. زیرا احتمال تخلف از سوی آنها نیز وجود دارد.

د) مجازات اصلاح شده است.

هـ) در تبصره «۱» الحاقی به نکته بسیار مهمی اشاره شده است. حفظ داده‌ها به‌منزله افشا یا ارائه آنها نیست و مستلزم مقررات مربوط است که منظور رعایت ماده بعدی است.

و) تبصره ماده (۲۳) نیز تکرار شده و فقط «**نظر**» مقام قضایی به «**دستور**» مقام قضایی تغییر یافته که دلیل آن رعایت دقیق‌تر مقررات رسیدگی است و به جهت حفظ ترتیب، در تبصره دو آورده شده است.

پیشنهاد مرکز ـ اصلاح ماده (۲۳) لایحه و الحاق یک تبصره به آن

ماده (۳۴)

هرگاه حفظ داده‌های رایانه‌ای ذخیره شده برای تحقیق یا دادرسی لازم باشد، مقام قضایی می‌تواند دستور حفاظت از آنها را برای اشخاصی که به‌نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضایی می‌توانند رأساً دستور حفاظت را صادر

کنند و مراتب را حداکثر تا ٢٤ ساعت به اطلاع مقام قضایی برسانند. چنانچه هریک از کارکنان دولت یا ضابطان قضایی یا سایر اشخاص از اجرای این دستور خودداری یا داده‌های حفاظت شده را افشا کنند یا اشخاصی که داده‌های مزبور به آنها مربوط می‌شود را از مفاد دستور صادره آگاه کنند، ضابطان قضایی و کارکنان دولت به مجازات امتناع از دستور مقام قضایی و سایر اشخاص به حبس از نودویک روز تا شش ماه یا جزای نقدی از پنج تا ده میلیون ریال یا هر دو مجازات محکوم خواهند شد.

تبصره «١» ـ حفظ داده‌ها به‌منزله ارائه یا افشای آنها نبوده و مستلزم مقررات مربوط است.

تبصره «٢» ـ مدت زمان حفاظت از داده‌ها حداکثر سه ماه است و درصورت لزوم با دستور مقام قضایی قابل تمدید است.

مبحث سوم ـ افشای داده‌ها

با توجه به این که عنوان «**ارائه**» برای این مبحث بار معنایی دقیق‌تری دارد، جایگزین «**افشا**» می‌شود.

پیشنهاد مرکز ـ اصلاح عنوان مبحث سوم به:
مبحث سوم ـ ارائه داده‌ها

ماده (٢۴) لایحه

مقام‌های قضایی می‌توانند دستور افشای داده‌های حفاظت شده مذکور در موارد (٢٢) و (٢٣) را به اشخاصی که داده‌های یاد شده را در تصرف و یا کنترل دارند صادر نموده تا در اختیار ضابطان قرار گیرد. مستنکف از اجرای دستور به مجازات مقرر در ماده (٢٣) این قانون محکوم خواهد شد.

تنها نکته اصلاح شده در این ماده، تغییر واژه «**افشا**» به «**ارائه**» است. همچنین لاجرم شماره مواد ارجاع یافته نیز اصلاح شده است.

پیشنهاد مرکز ـ اصلاح ماده (٢۴) لایحه
ماده (٣۵)
مقام قضایی می‌تواند دستور ارائه داده‌های حفاظت شده مذکور در مواد (٣٢)، (٣٣) و (٣٤) فوق را به اشخاص یاد شده بدهد تا در اختیار ضابطان قضایی قرار گیرد. مستنکف از اجرای این دستور به مجازات مقرر در ماده (٣٤) محکوم خواهد شد.

مبحث چهارم ـ تفتیش و توقیف داده‌ها و سیستم‌ها

با توجه به اینکه در تمامی عناوین و مفاد لایحه از عبارت دقیق «**داده‌ها و سیستم‌های رایانه‌ای و مخابراتی**» استفاده شده، در اینجا نیز اعمال می‌گردد.

پیشنهاد مرکز ـ اصلاح عنوان مبحث چهارم به:
مبحث چهارم ـ تفتیش و توقیف داده‌ها و سیستم‌های رایانه‌ای و مخابراتی

ماده (۲۵) لایحه

تفتیش و توقیف داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی در مواردی به عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم در آنها وجود داشته باشد.

در ماده پیشنهادی مرکز فقط یک نکته اضافه شده است. این اقدام باید به‌موجب «**دستور قضایی**» باشد. این تأکید از آن جهت بود که از ماده (۲۵) لایحه چنین برداشت می‌شد که در چنین مواردی ضابطان می‌توانند بدون اخذ «دستور قضایی» اقدام به تفتیش و توقیف کنند.

پیشنهاد مرکز ـ اصلاح ماده (۲۵) لایحه
ماده (۳۶)
تفتیش و توقیف داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی به‌موجب دستور قضایی و در مواردی به عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود داشته باشد.

ماده (۳۷) الحاقی مرکز

یکی از مسائل حساس در امر تفتیش و توقیف، «**حضور**» متصرف یا متصدی قانونی است و در قوانین سنتی هم سابقه دارد. ماده (۹۸) آیین دادرسی کیفری صراحتاً به آن پرداخته است. با اینکه احتمال عدم حضور متصرف یا متصدی قانونی داده‌ها یا سیستم‌ها نسبت به تفتیش اماکن و اشیای فیزیکی بیشتر است؛ اما به نظر رسید باز هم این عدم حضور باید به‌عنوان یک استثنا مد نظر قرار گیرد و همچنان بر اصل لزوم حضور این اشخاص به هنگام تفتیش و توقیف داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی تأکید شود. هرچند در انتها به این نکته اشاره شده که قاضی می‌تواند با ذکر دلایل، دستور تفتیش و توقیف بدون حضور اشخاص مذکور را هم صادر کند که البته بدیهی است با رعایت سایر مقررات، نظیر ماده فوق خواهد بود.

پیشنهاد مرکز ـ الحاق یک ماده
ماده (۳۷)
تفتیش و توقیف داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به‌نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سیستم‌ها انجام خواهد شد. در غیر این صورت، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر خواهد کرد.

ماده (۲۶) لایحه

دستور مقام قضایی به‌منظور تفتیش و توقیف درصورت امکان باید شامل اجرای دستور در داخل یا خارج از محل و اطلاعاتی نظیر مکان و محدوده تفتیش و توقیف، نوع داده‌های مورد نظر، مشخصات احتمالی فایل‌ها و سخت‌افزارها و نرم‌افزارها، تعداد آنها، مدت زمان مورد نیاز، نحوه دستیابی به فایل‌های رمزگذاری شده باشد. تفتیش مشتمل بر موارد زیر خواهد بود:

الف) تفتیش تمام یا بخشی از سیستم رایانه یا مخابراتی،

ب) تفتیش داده‌های رایانه‌ای ذخیره شده،

ج) تفتیش حامل‌های داده از قبیل: دیسک و لوح فشرده،

د) دستیابی به فایل‌های حذف شده یا رمزگذاری شده.

این ماده با ایراد ماهوی مواجه نیست. تغییرات اعمال شده عبارتند از:

الف) ماده (۲۶) لایحه علاوه بر «**تفتیش**»، ناظر به «**توقیف**» هم می‌باشد، در حالی که قسمت آخر تنها راجع به «**انواع تفتیش**» است و به همین دلیل باید به یک ماده مستقل انتقال یابد.

ب) در ماده جدید، واژه «**فایل**» به «**داده**» تغییر یافته که ناگفته پیداست تغییری در مفهوم آن ایجاد نمی‌شود. زیرا فایل نیز مجموعه‌ای از داده‌هاست که معنا و مفهومی را تبیین می‌کند.

ج) «**داده‌های حذف شده**» به هر دو ماده اضافه شده است. بازیابی این داده‌ها به اندازه رمزگشایی داده‌های رمزگذاری شده حائز اهمیت است.

د) «**کارت‌های حافظه**» به مصادیق حامل‌های داده اضافه شد. با توجه به عمومیت یافتن کاربرد انواع کارت‌های حافظه در قالب حافظه تلفن همراه، دوربین‌ها و به اصطلاح cool diskها، لازم است به آن اشاره شود.

هـ) با توجه به اینکه در ماده الحاقی، معرف، یعنی «تفتیش» و موضوع تعریف، یعنی «تفتیش» یکی هستند و این نوع نگارش صحیح نیست، در بندهای «الف» و «ب»، «دسترسی» و در بند «ج» «دستیابی» آمده که مفهوم لازم را منعکس می‌سازند.

و) بند «ب» لایحه نیز به‌دلیل زائد بودن حذف شد. زیرا دسترسی به داده‌های ذخیره شده یا از طریق بند «الف» یا «ب» متن پیشنهادی میسر است و حالت دیگری متصور نیست که داده‌ای ذخیره شده باشد، ولی در سیستم رایانه‌ای یا مخابراتی یا حامل داده نباشد.

پیشنهاد مرکز ـ اصلاح ماده (۲۶) لایحه و انتقال بخش انتهایی آن به یک ماده مستقل

ماده (۳۸)

دستور تفتیش و توقیف باید شامل اطلاعاتی باشد که به اجرای صحیح آن کمک می‌کند، از جمله اجرای دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده‌های مورد نظر، نوع و تعداد سخت‌افزارها و نرم‌افزارها، نحوه دستیابی به داده‌های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف.

ماده (۳۹)

تفتیش داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی شامل اقدامات ذیل می‌شود:

الف) دسترسی به تمام یا بخشی از سیستم‌های رایانه‌ای یا مخابراتی.

ب) دسترسی به حامل‌های داده از قبیل دیسکت‌ها یا لوح‌های فشرده یا کارت‌های حافظه.

ج) دستیابی به داده‌های حذف یا رمزنگاری شده.

ماده (۲۷) لایحه

داده‌ها، حامل‌های داده و سیستم‌های رایانه‌ای یا مخابراتی که دلیل یا وسیله ارتکاب جرم بوده و یا از جرم تحصیل شده‌اند، قابل توقیف می‌باشند.

پیشنهاد می‌شود این ماده حذف شود. زیرا:

الف) با توجه به مواد (۲۵) و (۳۰) لایحه محرز می‌شود تمامی حالات و توجیهات مدنظر قرار گرفته و ضرورتی بر ابقای آن نیست.

ب) ماده (۱۰) قانون مجازات اسلامی به تفصیل به این موارد اشاره کرده و نیازی به تأکید مجدد نیست.

ج) در مواد پایانی پیشنهادی، راجع به اموال ضبط شده ناشی از جرائم رایانه‌ای تعیین تکلیف شده است.

پیشنهاد مرکز ـ حذف ماده (۲۷) لایحه

ماده (۲۸) لایحه

در جمع‌آوری داده‌ها با رعایت تناسب، نوع، اهمیت و نقش داده‌ها در ارتکاب جرم، به روش‌هایی از قبیل موارد زیر عمل می‌شود:

الف) غیرقابل دسترس نمودن داده‌ها با روش‌هایی چون تغییر گذرواژه و رمزنگاری،

ب) تهیه پرینت از فایل‌ها،

ج) تهیه کپی یا تصویر از تمام یا بخشی از داده‌ها،

د) ضبط حامل‌های داده‌ها.

در رابطه با این ماده توجه به دو نکته ضروری است:

الف) به‌جای «**جمع‌آوری**»، «**توقیف**» بیاید. زیرا عنوان اختصاصی مبحث چهارم تفتیش و توقیف داده‌هاست که نسبت به‌عنوان کلی فصل دوم خود، یعنی جمع‌آوری ادله الکترونیکی اخص به‌شمار می‌آید.

ب) به‌جای «**پرینت**» که واژه‌ای لاتین است، «**چاپ**» و به‌جای «**فایل**»، «**داده**» بیاید.

ج) از آنجا که شیوه‌های توقیف داده‌ها به‌صورت تمثیلی آمده‌اند، ذکر آنها به‌صورت ترتیبی اشکال دارد. لذا این مصادیق در خود ماده آمده‌اند.

پیشنهاد مرکز ـ اصلاح ماده (۲۸) لایحه

ماده (۴۰)

در توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، کپی‌برداری یا تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود.

مواد (۲۹) و (۳۰) لایحه

ماده (۲۹)

توقیف سیستم‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش‌هایی از قبیل موارد زیر صورت می‌گیرد:

الف) تغییر گذرواژه به‌منظور عدم دسترسی به سیستم،

ب) خاموش نمودن سیستم،

ج) پلمپ سیستم در محل استقرار،

د) ضبط سیستم.

ماده (۳۰)

در موارد زیر سیستم‌های رایانه‌ای یا مخابراتی توقیف خواهند شد:

الف) داده‌های ذخیره شده به سهولت قابل دسترسی نبوده یا حجم زیادی داشته باشد.

ب) بهره‌برداری و تجزیه و تحلیل داده‌ها بدون وجود سیستم سخت‌افزاری امکان‌پذیر نباشد.

ج) مالک یا مسئول یا متصرف قانونی سیستم به توقیف رضایت داده باشد.

د) تهیه (تصویر) کپی از داده‌ها به لحاظ فنی امکان‌پذیر نباشد.

هـ) تفتیش در محل سبب ایراد صدمه به داده‌ها گردد.

و) سایر موارد با تصمیم مقام قضایی.

پیشنهاد اصلی مرکز در رابطه با این دو ماده جابه‌جایی آنهاست. زیرا رعایت ترتیب مفهومی مواد ایجاب می‌کند. ماده (۳۰) عملاً «**داده‌ها**» را هدف قرار داده و نه «**سیستم‌های رایانه‌ای و مخابراتی**» را. درواقع، این ماده شرایطی را تبیین می‌کند که به دلایلی امکان تفتیش داده‌ها وجود ندارد و باید سیستم توقیف شود. لذا باید بلافاصله بعد از ماده قبلی که ناظر به توقیف داده‌هاست بیاید. در عوض، ماده (۲۹) «**شیوه‌های**» توقیف سیستم‌های رایانه‌ای را مطرح می‌کند که می‌تواند پس از مواد مربوط به داده‌ها بیاید.

اصلاحات به عمل آمده عبارتند از:

الف) در بند «ب» ماده (۳۰)، به‌جای «**بهره‌برداری**»، «**تفتیش**» آمده است.

ب) بند «و» ماده (۳۰) از لحاظ ادبی با سایر بندها سازگار شده است.

ج) بند «ب» ماده (۲۹) که ناظر به «**خاموش کردن سیستم**» است، حذف می‌شود. زیرا هدف خاصی از آن استنباط نمی‌شود. اگر منظور عدم دسترسی است که تمامی بندها آن را دنبال می‌کنند و اگر مستلزم جابه‌جایی است که «**ضبط**» سیستم آن را پوشش می‌دهد. در مواردی که سیستم «**پلمپ**» می‌شود نیز هدف اصلی جلوگیری از ادامه کارکرد سیستم است و مقدمه واجب آن خاموش کردن است.

پیشنهاد مرکز ـ جابه‌جایی مواد (۲۹) و (۳۰) لایحه با یکدیگر و اصلاح آنها

ماده (۴۱)

در شرایط زیر سیستم‌های رایانه‌ای و مخابراتی توقیف خواهند شد:

الف) داده‌های ذخیره شده به سهولت در دسترس نبوده یا حجم زیادی داشته باشد،

ب) تفتیش و تجزیه و تحلیل داده‌ها بدون سیستم سخت‌افزاری امکان‌پذیر نباشد،

ج) متصرف قانونی سیستم رضایت داده باشد،

د) کپی‌برداری از داده‌ها به لحاظ فنی امکان‌پذیر نباشد،

هـ) تفتیش در محل باعث آسیب داده‌ها شود،

و) سایر شرایطی که قاضی تشخیص دهد.

ماده (۴۲)

توقیف سیستم‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش‌هایی از قبیل تغییر گذرواژه به‌منظور عدم دسترسی به سیستم، پلمپ سیستم در محل استقرار و ضبط سیستم صورت می‌گیرد.

ماده (۳۱) لایحه

توقیف حامل‌های داده غیرمتصل به سیستم رایانه‌ای یا مخابراتی، مانند ضبط آلات و ادوات جرم خواهد بود.

در بند «د» ماده (۲۸) لایحه به این مسئله اشاره شده و شیوه توقیف آنها نیز باید در آیین‌نامه بیاید. هرچند در اینجا نکته خاصی بیان نشده است. لذا پیشنهاد می‌شود حذف شود.

پیشنهاد مرکز ـ حذف ماده (۳۱) لایحه

ماده (۳۲) لایحه

چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سیستم‌های رایانه‌ای یا مخابراتی که تحت کنترل و یا تصرف متهم قرار دارند ضروری باشد، ضابطان با دستور مقام قضایی دامنه تفتیش و توقیف را به سیستم‌های دیگر گسترش داده و داده‌های مورد نظر را تفتیش یا توقیف خواهند نمود.

این ماده با ایرادی مواجه نیست و پیشنهاد می‌شود ابقا گردد.

پیشنهاد مرکز ـ ابقای ماده (۳۲) لایحه ذیل ماده (۴۳) پیشنهادی مرکز

مواد (۳۳) و (۳۴) لایحه

ماده (۳۳)

در موارد توقیف داده‌ها، چنانچه به روند تحقیقات لطمه‌ای وارد نیاید با تقاضا و هزینه مالک یا دارنده حق دسترسی به داده‌ها و دستور مقام قضایی، تصویر (کپی) داده‌های توقیف شده به ایشان تحویل می‌شود، مگر آنکه داده‌ها مجرمانه باشد.

ماده (۳۴)

در مواردی که با تشخیص مقام قضایی توقیف سیستم یا داده‌ها سبب ایراد لطمه‌های جانی یا مالی شدید به افراد یا اخلال در برنامه‌های خدمات عمومی گشته و یا مخل امنیت کشور باشد از روش‌های مناسب‌تری به‌جای توقیف استفاده خواهد شد.

در اینجا نیز ضروری است این دو ماده با یکدیگر جابه‌جا شوند. زیرا ماده (۳٤) هنوز دنباله مباحث توقیف است؛ اما موضوع ماده (۳۳) جزء مقررات پایانی این مبحث است که بر فرض ابقای

ماده (۳۵) لایحه با آن همخوانی دارد. لذا به دنبال این جابه‌جایی، پیشنهادهای اصلاحی ذیل مطرح می‌شود:

الف) در ماده (۳٤) لایحه آمده تحت شرایط مقرر به‌جای «**توقیف**» از «**روش‌های مناسب‌تری**» استفاده شود. به نظر می‌رسد این نوع ضابطه‌انگاری تالی فاسد دارد و همان‌طور که در عمومات آیین دادرسی کیفری نیز مشاهده می‌شود، تا حد امکان نباید به ضابطان قضایی ابتکار عمل بی‌حدوحصر داد و حداقل باید رئوس وظایف آنها مشخص شود. ضمن آنکه در این قانون شیوه‌های جایگزین دسترسی به داده‌ها و سیستم‌ها پیش‌بینی شده است. لذا در اینجا باید صراحتاً این اقدام منع گردد.

ب) در مورد ماده (۳۳) لایحه، صرف‌نظر از ایرادات نگارشی، نظیر آوردن «ایشان»، **اولاً** به‌جای «مالک یا دارنده حق دسترسی»، «ذی‌نفع» بار معنایی حقوقی بیشتری دارد و پیشنهاد می‌شود جایگزین شود. **ثانیاً** اخذ کپی از داده‌ها «حق» ذی‌نفع تلقی می‌شود و جنبه «استدعایی» یا «درخواست» ندارد. زیرا اگر شرایط این ماده ایجاب می‌کند، ضرورتی ندارد که وی را از دسترسی به داده‌هایش محروم کنیم. **ثالثاً** علاوه بر دو شرط مقرر در ماده (۳٤) لایحه که یکی در ابتدا و دیگری در انتها آمده، شرط مهم دیگر، عدم مغایرت با «محرمانه بودن تحقیقات» است که صراحتاً در ماده (۷۳) آیین دادرسی کیفری نیز به آن اشاره شده است.

پیشنهاد مرکز ـ اصلاح و جابه‌جایی مواد (۳۳) و (۳۴) لایحه

ماده (۴۴)

توقیف داده‌ها و سیستم‌های رایانه‌ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی می‌شود ممنوع است.

ماده (۴۵)

در جایی که اصل داده‌ها توقیف می‌شود، ذی‌نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به اینکه ارائه داده‌های توقیف شده منافی با محرمانه بودن تحقیقات نباشد و به روند تحقیقات لطمه‌ای وارد نسازد و داده‌ها مجرمانه نباشند.

ماده (۴۶) الحاقی مرکز

در این ماده بر این موضوع تأکید شده که توقیف اصل داده‌ها و سیستم‌های رایانه‌ای یا مخابراتی «**موقتی**» است و نباید بلاتکلیف رها شوند. هرچند نمی‌توان زمان خاصی را برای این کار مشخص کرد، زیرا روز به روز بر تنوع و میزان داده‌های رایانه‌ای افزوده می‌شود و دقیقاً نمی‌توان پیش‌بینی کرد طی چه مدت بررسی آنها اتمام می‌یابد. همچنین، ممکن است سخت‌افزارها و نرم‌افزارهایی

توقیف شوند که نمونه آنها تاکنون مشاهده نشده و نیاز به تخصص و مهارت جدیدی برای بررسی آنها باشد. لذا در این ماده به مهلت «**متناسب و متعارف**» اشاره شده تا قاضی با جلب نظر کارشناسان و ضابطان، بهترین زمان را که در آن می‌توان دلایل و مدارک مورد نیاز را تحصیل کرد تعیین کند.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۴۶)

در مواردی که اصل داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی توقیف می‌شود، قاضی موظف است با لحاظ نوع و میزان داده‌ها و نوع و تعداد سخت‌افزارها و نرم‌افزارها و نقش آنها در جرم ارتکابی، در مهلت متناسب و متعارف نسبت به آنها تعیین تکلیف کند.

ماده (۳۵) لایحه

متضرر می‌تواند در مورد عملیات و اقدام‌های مأموران در توقیف داده‌ها و سیستم‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضایی دستوردهنده تسلیم نماید. به درخواست یاد شده خارج از نوبت رسیدگی گردیده و تصمیم اتخاذ شده قابل اعتراض است.

به این مسئله باید طبق عمومات عمل کرد و پیش‌بینی مقرره خاص برای این طیف جرائم خاص توجیهی ندارد. به‌ویژه آنکه تصریح شده خارج از نوبت رسیدگی شود که توجیه‌بردار نیست و باید تشریفات خاص خود را طی کند. هرچند از آنجا که محاکم خاصی برای رسیدگی به این جرائم اختصاص یافته و خواهند یافت، این خلأ خودبه‌خود برطرف خواهد شد.

پیشنهاد مرکز ـ حذف ماده (۳۵) لایحه

مبحث پنجم ـ شنود داده‌ها

عنوان این مبحث، مانند برخی عناوین پیشین مبهم و نارساست، زیرا تمامی داده‌ها را دربرمی‌گیرد، حال آنکه شنود قسم خاصی از داده‌ها را هدف قرار می‌دهد.

عنوان پیشنهادی مرکز، «**شنود محتوای ارتباطات رایانه‌ای**» است تا **اولاً** سایر داده‌هایی که محتوا تلقی نمی‌شوند، به‌ویژه داده‌های ترافیک، از شمول آن خارج شوند، **ثانیاً** قید «رایانه‌ای» آورده شده تا از ارتباطات سنتی مخابراتی، به‌ویژه تلفن ثابت که از طریق خطوط «آنالوگ» فعال می‌شود متمایز گردد و با عنوان و موضوع این قانون سازگاری داشته باشد. هرچند اذعان می‌شود

به تدریج ارتباطات آنالوگ جای خود را بـه ارتباطـات «دیجیتـالی» مـی‌دهنـد. البتـه در اینجـا مقـرره جدیدی وضع نشده و تابع ضوابط موجود قرار گرفته است.

پیشنهاد مرکز ـ تغییر عنوان مبحث پنجم به:
مبحث پنجم ـ شنود محتوای ارتباطات رایانه‌ای

ماده (۳۶) لایحه

شنود داده محتوا ممنوع است، مگر با رعایت قوانین مربوط.

در این ماده اصلاحاتی به‌شرح ذیل اعمال شده است:

الف) با توجه به توضیحاتی که در ابتدای گزارش راجع به تعاریف بخش نخست داده شـد، اصـطلاح «داده محتوا»، مانند سایر اصطلاحات، نظیر «داده رایانـه‌ای» و «اطلاعـات» حـذف شـد. زیـرا بیشـتر موجبات ابهام و سردرگمی مسئولان را فراهم می‌کند و به‌جای آن «محتوای در حال انتقال ارتباطات غیرعمومی در سیستم‌های رایانه‌ای و مخابراتی» آورده شد که با توجـه بـه توضـیحات ارائـه شـده ذیل ماده (۲) پیشنهادی مرکز، به نظر می‌رسد معادل دقیق‌تر و منطقی‌تری باشد. بـرای مثـال، پسـت الکترونیکی یا ارتباطات برقرار شده در محیط‌های گپ[1] یا حتی پیامک از طریـق تلفـن‌هـای همـراه یـا پیجرها نیز مشمول این ضابطه می‌شوند.

ب) در تمامی نظام‌های حقوقی، شنود محتوای ارتباطات به‌عنوان آخرین گزینه مدنظر قـرار گرفتـه و مجریان قانون به راحتی نمی‌توانند بـه آن تمسـک جوینـد. حتـی کنوانسـیون جـرائم سـایبر نیـز در آخرین ماده بخش دوم خود (مـاده (۲۲)) بـه آن پرداختـه اسـت و در مـواد پیشـین، اقـدامات کمتـر تعرض‌آمیز دیگری را برشمرده است. لذا با توجه به حساسیت و اهمیت فوق‌العاده «شنود»،[2] به نظـر رسید برخلاف ماده (۳۶) لایحه که به‌طور مبهم به قوانین مربوط ارجاع داده اسـت، شـنود محتـوای در حال انتقال ارتباطات غیرعمومی در سیسـتم‌هـای رایانـه‌ای یـا مخـابراتی کـه تفـاوت چنـدانی بـا مقررات راجع به «شنود مکالمات تلفنی» نـدارد، تحـت شـمول آن قـرار گیـرد تـا کلیـه اقـدامات ایـن مجموعه با شفافیت و دقت هرچه بیشتر به اجرا درآید.

ج) در تبصره پیشنهادی به نکته‌ای اشاره شده که بیشتر در ارتباطات رایانـه‌ای و شـبکه‌ای مصـداق می‌یابد و اتفاقاً برخی مسائل حقوقی را در سایر کشورها پدید آورده که به نظر رسید پیشـاپیش در این قانون به آن اشاره و نسبت به آن تعیین تکلیـف شـود. طبـق ایـن تبصـره، صـرف دسـتیابی بـه داده‌های «در حال انتقال»، «شنود» تلقی نمی‌شود. بلکه ارتباطات «ذخیره شده» نیز در حکم آن است.

1. Chat Room
2. Interception

زیرا آنچه مورد حمایت قرار گرفته، در حال انتقال بودن محتوا نیست، بلکه خود محتواست. لذا ضروری است این مسئله مهم مورد توجه قرار گیرد.

پیشنهاد مرکز ـ اصلاح ماده (۳۶) لایحه و الحاق یک تبصره به آن

ماده (۴۷)

شنود محتوای در حال انتقال ارتباطات غیرعمومی در سیستم‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود.

تبصره ـ دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است.

مبحث ششم ـ سایر موارد

در ذیل این مبحث، دو ماده آمده که از مضامین آنها در مباحث شکلی حقوق کیفری سایبری به «**استنادپذیری ادله الکترونیکی**»[1] یاد می‌شود. با اینکه این عنوان عیناً در لسان قانون‌گذار مسبوق به سابقه نیست، اما نه تنها تعبیر دیگری از آن را به رسمیت شناخته (در فصل دوم از مبحث سوم از باب اول قانون تجارت الکترونیکی «پذیرش، ارزش اثباتی و ...» آمده که برگردان دیگری از این عبارت است)، بلکه محتوا و ضوابط آن را در مقررات مختلف آیین دادرسی کیفری اتخاذ کرده است، به‌ویژه آنکه مفهوم رسا و قابل درکی دارد و به وضوح قابلیت استناد ادله الکترونیکی در فرایند دادرسی کیفری را تبیین می‌کند.

اما از آنجا که بحث مستقلی در باب ادله الکترونیکی مطرح می‌شود و درواقع ضروری است به مقررات و ضوابط آن فراتر از فصل دوم راجع به تفتیش و توقیف توجه شود، به‌ویژه آنکه تنها ضابطان قضایی را مخاطب قرار نمی‌دهد و طرفین دعوا نیز مشمول آن می‌شوند، پیشنهاد مرکز این است که فصل مجزایی به آن اختصاص یابد.

پیشنهاد مرکز ـ تغییر عنوان مبحث ششم به:

فصل سوم ـ استنادپذیری ادله الکترونیکی

ماده (۳۷) لایحه

داده‌های رایانه‌ای و مخابراتی درصورتی که مطابق این قانون جمع‌آوری و نگهداری شده باشد می‌تواند در اثبات جرم مورد استفاده قرار گیرد.

1. Admissibility of Electronic Evidence

این ماده از لایحه به «استنادپذیری ادله الکترونیکی» از سوی مجریان قانون اشاره دارد. از آنجا که مجریان قانون به دستور مقام قضایی یا در شرایطی رأساً اقدام به جمع‌آوری ادله جرم می‌کنند، باید از مقررات خاصی تبعیت کنند. این موضوع، به‌ویژه در مورد ادله الکترونیکی حساسیت زیادی دارد و نحوه رویارویی و جمع‌آوری آنها نظم خاصی می‌طلبد و از آنجا که به راحتی آسیب‌پذیرند، باید بااحتیاط و در عین حال با سرعت عمل در دستور کار قرار گیرند. در غیر این صورت، ممکن است حقوق اشخاص پایمال شود یا حتی در اثر بی‌احتیاطی مجریان قانون، یک بی‌گناه محکوم شود. لذا جمع‌آوری ادله الکترونیکی و به تبع آن مستندسازی آنها باید تابع اصول و ضوابطی باشد که به‌دلیل مفصل بودن قواعد مربوط و همچنین نیاز مستمر به روزآمد کردن آنها، این موضوع به کلی به آیین‌نامه محول شده است.

در اینجا ضروری است به تعبیر «**مستندسازی**»[1] نیز توجه شود. با اینکه در آیین دادرسی کیفری صراحتاً نیامده است، اما به وضوح به نمونه‌هایی از آن تصریح شده است. برای مثال، آنچه در ماده (۱۰۸) آیین دادرسی کیفری راجع به شماره‌گذاری و ممهور و حفظ کردن آلات و ادوات جرم آمده یا ضوابطی که در مواد بعد به صراحت آمده، چیزی جز مستندسازی ادله نیست و به نظر می‌رسد وقت آن رسیده که این تعبیر دقیق در مجموعه قوانین وارد شود. اما همان‌طور که گفته شد، اقداماتی که لازم است در زمینه مستندسازی ادله الکترونیکی انجام شود را نمی‌توان به قانونی واگذار کرد که تغییر و اصلاح آن با تشریفات بسیار و طولانی‌مدت همراه است.

پیشنهاد مرکز ـ اصلاح ماده (۳۷) لایحه

ماده (۴۸)

گزارش و تحقیقات ضابطان قضایی در زمینه جمع‌آوری و مستندسازی ادله الکترونیکی مطابق آیین‌نامه مربوط خواهد بود.

ماده (۳۸) لایحه

به‌منظور جلوگیری از بروز هرگونه تغییر، تحریف یا آسیب و حفظ وضعیت اصلی داده‌های رایانه‌ای یا مخابراتی جمع‌آوری شده، لازم است تا زمانی که مرجع قضایی مربوط ضروری می‌داند، از آنها نگهداری و مراقبت به عمل آید.

تبصره *ـ آیین‌نامه شیوه جمع‌آوری، نگهداری و مراقبت از داده‌های رایانه‌ای و مخابراتی توسط وزارت دادگستری با همکاری نیروی انتظامی جمهوری اسلامی ایران و وزارت ارتباطات و فناوری اطلاعات ظرف سه ماه از تاریخ تصویب این قانون تهیه شده به تصویب رئیس قوه قضائیه خواهد رسید.*

1. Documentation

این ماده شق دوم فرایند استنادپذیری ادله الکترونیکی از سوی مجریان قانون را بیان می‌کند. پس از جمع‌آوری و مستندسازی ادله الکترونیکی، مجریان قانون موظفند طبق ضوابط مربوط از آنها «**نگهداری و مراقبت**»[1] به عمل آورند. این موضوع از آن جهت مورد تأکید قرار گرفته که ادله الکترونیکی به لحاظ ماهیتشان به راحتی در معرض تغییر یا تحریف یا آسیب قرار دارند و بنابراین باید جهت حفظ استنادپذیری آنها براساس اصول و ضوابط علمی، از آنها نگهداری و مراقبت کنند. اما از آنجا که این اقدامات، همانند جمع‌آوری و مستندسازی همواره در معرض تغییر و تحولند، باید به‌راحتی بتوان آنها را اصلاح کرد و از شیوه‌های جدیدتری بهره برد. به همین دلیل، نحوه نگهداری و مراقبت از ادله الکترونیکی نیز به آیین‌نامه مربوط واگذار شده است.

در رابطه با این موضوع، سه اصل کلیدی مورد توجه قرار گرفته است. چنانچه این اصول رعایت شوند، می‌توان گفت ادله الکترونیکی به‌دست آمده استنادپذیرند. این اصول عبارتند از:

۱. **صحت و تمامیت داده‌ها**:[2] به جرائم علیه این اصل در بخش جرائم و مجازات‌ها اشاره شد که به این ترتیب جایگاه مهم این اصل در عرصه فناوری اطلاعات و ارتباطات محرز می‌شود. هدف این اصل، حفظ شاکله اصلی و ماهیت داده‌ها و دور نگه‌داشتن آنها از هرگونه تغییر و تحریف است.

۲. **اعتبار**:[3] این اصل با نگاهی فراتر از شاکله داده‌ها، بستر تبادل، ذخیره یا پردازش و همچنین هویت پدیدآورندگان یا دست‌اندرکاران را مدنظر قرار می‌دهد.

۳. **انکارناپذیری**:[4] در اینجا رابطه میان داده‌ها با پدیده موردنظر و همچنین پدیدآورنده تبیین می‌شود، به‌گونه‌ای که امکان انکار یا نفی آن از سوی وی وجود نداشته باشد.

در پایان، راجع به تبصره این ماده از لایحه یادآور می‌شود از آنجا که بخش شکلی این قانون نیازمند آیین‌نامه‌های عدیده‌ای است که پیوستگی موضوعی با یکدیگر دارند و مراجع تدوین‌کننده و تصویب‌کننده آن نیز یکی هستند، در یک ماده مستقل (۵۶ پیشنهادی) پیش‌بینی شده‌اند و به بخش پایانی لایحه انتقال یافته‌اند.

پیشنهاد مرکز ـ اصلاح ماده (۳۸) لایحه و انتقال تبصره آن به یک ماده مستقل در بخش پایانی

ماده (۴۹)

به‌منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع‌آوری شده، لازم است مطابق آیین‌نامه مربوط از آنها نگهداری و مراقبت به عمل آید.

1. Preservation
2. Integrity
3. Authenticity
4. Non-Repudiation

ماده (۵۰) الحاقی مرکز

این ماده به شرایط لازم‌الاتباع جهت استنادپذیری ادله الکترونیکی ارائه شده از سوی عواملی جز ضابطان قضایی، مانند طرفین دعوا اشاره دارد. به‌طور کلی، در نظام‌های حقوقی مختلف که بر مبنای اصول خود ادله اثبات کیفری را تعریف می‌کنند، توجه به داده‌های رایانه‌ای به‌عنوان دلیل قابل استناد در محکمه هنوز مراحل اولیه خود را سپری می‌کند. دلیل اصلی این امر هم حساسیت محاکم به داده‌های رایانه‌ای است، زیرا یقیناً نمی‌توانند به آنها استناد کنند.

از سوی دیگر، گسترش بهره‌برداری از سیستم‌های رایانه‌ای و مخابراتی در تمامی شئون زندگی فردی و اجتماعی به حدی رسیده که نمی‌توان وجود داده‌های رایانه‌ای را در اثبات مسائل مختلف نفی کرد و حتی مسائل بسیاری پدید آمده که اثبات آنها جز با استناد به داده‌های رایانه‌ای میسر نیست. لذا به نظر رسید بهتر است در ابتدای این راه، به قواعد حداقلی بسنده شود تا از یک‌سو محاکم ما به تدریج با این‌گونه مدارک و دلایل بیشتر آشنا شوند و از سوی دیگر به‌راحتی نتوان با استناد به داده‌های رایانه‌ای آسیب‌پذیر، حقوق افراد را پایمال کرد.

طبق ماده پیشنهادی مرکز، برای اینکه عوامل ذی‌ربط بتوانند به داده‌های رایانه‌ای استناد کنند، باید دو شرط مهم و اساسی را اثبات کنند:

۱. داده‌های مورد استناد توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد. این قاعده که در قوانین دیگر، به‌ویژه قانون تجارت در زمینه استناد به دفاتر سابقه دارد، از آن جهت مد نظر قرار گرفته که احتمال خدشه وارد کردن به داده‌ها به حداقل می‌رسد. زیرا کسی این اعمال را بر روی داده‌ها انجام می‌دهد که هدفی جهت بهره‌برداری از آنها در دعوای مطروحه دنبال نمی‌کند و به همین دلیل، بعید است در تمامیت و صحت آنها خدشه‌ای وارد کند.

۲. سیستم رایانه‌ای یا مخابراتی مربوط به‌نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه‌ای وارد نشود.

به نظر می‌رسد به‌دلیل مشکل بودن اثبات این دو ضابطه، تنها داده‌های رایانه‌ای که واقعاً ارزش استناد در دعاوی را دارند از سوی طرفین دعوا ارائه خواهند شد. زیرا به‌راحتی نمی‌توان صحت عملکرد یک سیستم رایانه‌ای یا مخابراتی را اثبات کرد، به‌ویژه اگر شخصی هم باشد و قاعدتاً سیستم‌هایی را دربرمی‌گیرد که به‌طور معمول و متداول صحیح عمل می‌کنند، مانند سیستم‌های رایانه‌ای یا مخابراتی بانک‌ها یا مؤسسات عمومی.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۵۰)

چنانچه داده‌های رایانه‌ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد و سیستم رایانه‌ای یا مخابراتی مربوط به‌نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشده باشد، قابل استناد خواهند بود.

ماده (۵۱) الحاقی مرکز

یکی از ویژگی‌های متمایز مقررات آیین دادرسی کیفری سایبری نسبت به حقوق جزای ماهوی سایبری این است که نه تنها جرائم صرفاً رایانه‌ای ـ سایبری را دربرمی‌گیرد، بلکه بر سایر جرائمی که به هر نحو امکان استناد به ادله الکترونیکی برای اثبات یا رد دعوای کیفری وجود داشته باشد نیز حکومت دارند. برای مثال، چنانچه قاچاقچیان مواد مخدر در محاسبات و سایر اقدامات خود از سیستم‌های رایانه‌ای و مخابراتی استفاده کرده باشند و ضابطان قضایی بخواهند به ادله الکترونیکی برای اثبات جرم آنها استناد کنند، لازم است مقررات این قانون را رعایت کنند. گفتنی است این مقرره علاوه بر قوانین کیفری کشورها، در اسناد بین‌المللی، به‌ویژه کنوانسیون جرائم سایبر نیز مستند و لازم‌الاتباع شده است.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۵۱)

کلیه مقررات مندرج در فصل‌های دوم و سوم این بخش، علاوه بر جرائم رایانه‌ای شامل سایر جرائمی که ادله الکترونیکی در آنها مورد استناد قرار می‌گیرند نیز می‌شود.

بخش چهارم ـ همکاری‌های بین‌المللی

همان‌طور که ملاحظه می‌شود، در ذیل این بخش تنها به یک ماده اشاره شده که توجه به محتوای آن آشکار می‌سازد موضوع مستقلی را مطرح نکرده و در نهایت به تدوین لایحه یا آیین‌نامه ختم شده است. لذا محملی برای تخصیص یک بخش به آن وجود ندارد و پیشنهاد می‌شود این عنوان حذف شود و بخش نهایی به «**سایر مقررات**» اختصاص یابد.

پیشنهاد مرکز ـ تغییر عنوان بخش چهارم به:
بخش سوم ـ سایر مقررات

ماده (۳۹) لایحه

همکاری‌های بین‌المللی، هرگونه مبادله اطلاعات و انجام امور اداری و پلیسی و قضایی که دولت ایران و سایر دولت‌ها را قادر به کشف، پیگیری، تعقیب، رسیدگی و اجرای حکم نماید دربرخواهد گرفت.

***تبصره ـ** چگونگی پیگیری و انجام امور ذکر شده در این ماده و تشکیلات سازمانی مورد نیاز برای اجرای آن به‌موجب آیین‌نامه‌ای خواهد بود که ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت دادگستری با کسب نظر از مراجع مربوط تهیه گشته، به تصویب رئیس قوه قضائیه خواهد رسید.*

در این رابطه نکات ذیل قابل توجه است:

الف) این ماده به تعریف انواع و شیوه‌های همکاری بین‌المللی کیفری ایران اختصاص یافته که به نظر نمی‌رسد برای قانون‌گذار و مسئولان ذی‌ربط نامفهوم باشد تا ضرورت ایجاب کند دوباره در اینجا تعریف شود.

ب) مقدمه همکاری‌های بین‌المللی، پیوستن به معاهدات بین‌المللی و منطقه‌ای یا انعقاد معاهدات دوجانبه یا چندجانبه است که از نظر نویسندگان لایحه مغفول مانده است.

ج) تبصره این ماده با یک ایراد اساسی مواجه است. این اقدام مهم نیاز به آیین‌نامه ندارد. بلکه باید وزارت مربوط، یعنی وزارت دادگستری شود با همکاری وزارت ارتباطات و فناوری اطلاعات علاوه بر پیگیری امور، لوایح مربوط را تهیه کند و پس از تصویب در هیئت دولت، به مجلس شورای اسلامی تقدیم کند. کما اینکه چنین رویه‌ای در رابطه با سایر امور کیفری اتخاذ می‌شود.

پیشنهاد مرکز ـ اصلاح ماده (۳۹) لایحه

ماده (۵۲)

به‌منظور ارتقای همکاری‌های بین‌المللی در زمینه جرائم رایانه‌ای، وزارت دادگستری موظف است با همکاری وزارت ارتباطات و فناوری اطلاعات اقدامات لازم را در زمینه تدوین لوایح و پیگیری امور مربوط جهت پیوستن ایران به اسناد بین‌المللی و منطقه‌ای و معاهدات راجع به همکاری و معاضدت دوجانبه یا چندجانبه قضایی انجام دهد.

بخش پنجم ـ سایر مقررات

با توجه به توضیحات فوق راجع به تغییر عنوان بخش چهارم لایحه به «**بخش سوم ـ سایر مقررات**»، این بخش نیز خودبه‌خود حذف می‌شود.

ماده (۴۰) لایحه

در مواردی که سیستم رایانه‌ای یا مخابراتی به‌عنوان وسیله یا ابزار ارتکاب جرم مورد استفاده قرار گیرد و در این قانون مجازاتی تعیین نشده باشد مرتکب مطابق مقررات قانون مربوط مجازات خواهد شد.

الف) این ماده با ایرادی مواجه نیست و با قدری اصلاحات نگارشی انعکاس می‌یابد.

ب) در رابطه با تبصره الحاقی لازم به یادآوری است در مجموعه شکلی لایحه، چه در مقام تدوین و چه به هنگام اصلاح آن در مرکز سعی شده به تمامی مسائل راجع به نحوه رسیدگی کیفری جرائم رایانه‌ای اشاره شود. با این حال، ممکن است باز هم ضوابطی مغفول مانده باشد. لذا شایسته است تصریح شود که در این حالت به مقررات عام آیین دادرسی کیفری مراجعه شود.

همچنین، اشاره به قانون آیین دادرسی کیفری به‌جای قانون تشکیل دادگاه‌های عمومی و انقلاب در امور کیفری مصوب ۱۳۷۸ به دو دلیل بود:

۱. این قانون در شرف اصلاح است و از لحاظ اصول حقوقی نیز ارجاع به یک قانون صحیح نیست.

۲. با توجه به ماده (۲۰) لایحه که در اصلاح آن به مراجع قضایی دیگری نظیر «مراجع قضایی نظامی» اشاره شده، ضرورت ایجاب می‌کند امکان مراجعه به قوانین دادرسی کیفری آنها نیز وجود داشته باشد. لذا این عنوان عام، اما جامع انتخاب شده است.

پیشنهاد مرکز ـ اصلاح ماده (۴۰) لایحه و الحاق یک تبصره

ماده (۵۳)

در مواردی که سیستم رایانه‌ای یا مخابراتی به‌عنوان وسیله ارتکاب جرم به‌کار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده است، مطابق قوانین جزایی مربوط عمل خواهد شد.

تبصره ـ در مواردی که در بخش دوم این قانون برای رسیدگی به جرائم رایانه‌ای مقررات خاصی از جهت آیین دادرسی پیش‌بینی نشده است طبق مقررات قانون آیین دادرسی کیفری اقدام خواهد شد.

ماده (۵۴) الحاقی مرکز

همان‌طور که در سایر قوانین جزایی تفکیک جرائم عمومی از خصوصی مسبوق به سابقه است، شایسته است در اینجا نیز این موضوع مورد توجه قرار گیرد. به همین منظور موادی که به نظر می‌رسد امکان توقف تعقیب و اجرای حکم کیفری متعاقب گذشت شاکی خصوصی وجود دارد در ماده پیشنهادی آمده است.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۵۴)

جرائم موضوع مواد (۱)، (۲)، (۸)، (۹)، (۱۰)، (۱۲)، (۱۶) و (۱۷) جز با شکایت شاکی خصوصی تعقیب نمی‌شود و درصورتی که شاکی یا مدعی خصوصی در هر مرحله از دادرسی گذشت کند تعقیب و اجرا موقوف می‌شود.

ماده (۴۱) لایحه

میزان جزاهای نقدی موضوع این قانون، متناسب با شرایط اقتصادی هر سه سال یک بار براساس پیشنهاد قوه قضائیه و تأیید هیئت وزیران قابل اصلاح می‌باشد.

این ماده با قدری اصلاحات انعکاس یافته است.

پیشنهاد مرکز ـ اصلاح ماده (۴۱) لایحه

ماده (۵۵)

میزان جزاهای نقدی این قانون، براساس نرخ رسمی تورم حسب اعلام بانک مرکزی هر سه سال یک بار با پیشنهاد رئیس قوه قضائیه و تصویب هیئت وزیران قابل تغییر است.

ماده (۵۶) پیشنهادی مرکز

با توجه به توضیحاتی که راجع به ضرورت تخصیص یک ماده به آیین‌نامه‌های مورد نیاز این قانون داده شد، این ماده به ترتیب ذیل پیشنهاد می‌شود.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۵۶)

وزارت دادگستری موظف است ظرف شش ماه از تاریخ تصویب این قانون با همکاری وزارت ارتباطات و فناوری اطلاعات آیین‌نامه‌های مربوط به جمع‌آوری و استنادپذیری ادله الکترونیکی را تهیه کند و به تصویب هیئت دولت برساند. این وزارتخانه موظف است بر حسب ضرورت آیین‌نامه‌های مذکور را براساس آخرین دستاوردهای علمی روزآمد کند.

ماده (۵۷) الحاقی مرکز

در این ماده راجع به تجهیزات سخت‌افزاری و نرم‌افزاری که صرفاً به ارتکاب جرائم رایانه‌ای اختصاص یافته‌اند، تعیین تکلیف شده است. در این رابطه توجه به چند نکته ضروری است:

الف) قید «صرفاً» تصریح دارد که باید از ضبط افزارهای رایانه‌ای که کارکرد دوگانه خود را حفظ کرده‌اند، صرف‌نظر شود. کما اینکه این مسئله در جرائم مرسوم نیز قابل مشاهده است و

محاکم از صدور حکم ضبط تجهیزاتی که صرفاً به ارتکاب یک جرم اختصاص نیافته‌اند، پرهیز می‌کنند.

ب) این ماده ناظر به «**تمامی**» جرائم رایانه‌ای است و منحصر به جرائم موضوع این قانون نیست.

ج) تعیین تکلیف راجع به افزارهای ضبط شده با خود دولت است. از آنجا که گوناگونی این ابزارها با توجه به طیف جرائم رایانه‌ای بسیار بالاست، بهتر است مسئولان امر نسبت به هر قضیه تصمیم متناسب و شایسته‌ای اتخاذ کنند.

پیشنهاد مرکز ـ الحاق یک ماده

ماده (۵۷)

کلیه نرم‌افزارها و تجهیزات رایانه‌ای و مخابراتی که صرفاً به ارتکاب جرائم رایانه‌ای اختصاص یافته‌اند به نفع دولت ضبط خواهند شد.

ماده (۴۲) لایحه

قوانین و مقررات مغایر با این قانون ملغی است.

با توجه به اهمیت نسخ صریح برخی قوانین که با این لایحه در تعارض قرار دارند، پیشنهاد می‌شود در کنار تأکید عام بر قوانین مغایر، صراحتاً به آنها اشاره شود که ۲ قانون را شامل می‌شود: مواد (٦٧) و (٦٨) قانون تجارت الکترونیکی مصوب ۱۳۸۲ و ماده (۱۰) قانون اصلاح قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند، مصوب دی‌ماه ۱۳۸٦.

پیشنهاد مرکز ـ اصلاح ماده (۴۲) لایحه

ماده (۵۸)

قوانین مغایر با این قانون، از جمله مواد (۶۷) و (۶۸) قانون تجارت الکترونیکی، مصوب ۱۳۸۲ و ماده (۱۰) قانون اصلاح قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز می‌نمایند مصوب ۱۳۸٦ ملغی است.

منابع و مآخذ

۱. مجموعه قوانین و مقررات فناوری اطلاعات و ارتباطات ایران، دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۳.

۲. مرکز پژوهش‌های مجلس شورای اسلامی، گزارش کارشناسی درباره لایحه جرائم رایانه‌ای، شماره ۷۵۵۲، آبان‌ماه ۱۳۸۴.

۳. مرکز پژوهش‌های مجلس شورای اسلامی، تأملی بر فیلترینگ: ۳. سالم‌سازی فضای سایبر و تعارضات موجود، شماره ۸۵۷٤، مهرماه ۱۳۸٦.

۴. مرکز پژوهش‌های مجلس شورای اسلامی، تأملی بر فیلترینگ: ٤. مشترک گرامی دسترسی به این سایت امکان‌پذیر نمی‌باشد، شماره ۸۵۸۱، مهرماه ۱۳۸٦.

شناسنامه گزارش	شماره مسلسل: ۹۱۳۸

عنوان گزارش: اظهارنظر کارشناسی درباره: «لایحه جرائم رایانه‌ای» (گزارش ۱)

Report Title : Crime Cyber(1)

نام دفتر: مطالعات ارتباطات و فناوری‌های نوین

تهیه و تدوین: گروه کارشناسان

مدیر مطالعه: رضا باقری اصل

ناظر علمی: ـــــ

همکاران: جلیل امیدی (مطالعات حقوقی)، مهدی ادیبان (مطالعات فرهنگی)

همکاران و اظهارنظرکنندگان خارج از مرکز: سیامک قاجار قیونلو (شورای عالی اطلاع‌رسانی)، سیدهادی سجادی (وزارت ارتباطات و فناوری اطلاعات - مرکز تحقیقات مخابرات)، صمد مؤمن بالله (معاونت پارلمانی وزارت ارتباطات و فناوری اطلاعات)، حسین مهدیزاده (وزارت فرهنگ و ارشاد اسلامی)، علیرضا طوسی و علی نجفی (دفتر اینترنت دادستانی)، سرهنگ امجدنیا (معاونت امنیت عمومی ناجا)

ویراستار ادبی: ـــــ

ویراستار تخصصی: ـــــ

متقاضی: کمیسیون قضایی و حقوقی

واژه‌های کلیدی (فارسی / انگلیسی): ـــــ

تاریخ شروع مطالعه: ۱۳۸۷/۴/۱۲

تاریخ خاتمه مطالعه: ۱۳۸۷/۷/۳

تاریخ انتشار: ۱۳۸۷/۸/۵